TLP - GREEN

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EU MANAGED SECURITY SERVICES (EUMSS) CANDIDATE CERTIFICATION SCHEME DRAFT V1.1

JULY 2026

DOCUMENT HISTORY

//DRAFT ONLY - DELETE THIS SECTION AND PAGE UPON FINAL PUBLICATION

Date	Version	Modification	Author's comments
16/03/2026	Draft 0.1	Creation	For internal review
19/03/2026	Draft 0.3	Updated	For AHWG review
07/04/2026	Draft 0.4	Updated with AHWG comments	For AHWG validation
05/06/2026	Draft 1.0	Added HoLa and VeLa. Update with Cyprus AHWG Discussion	For AHWG Validation.
24/07/2026	Draft 1.1	Review of AHWG Comments	For Public Consultation.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity Certification Schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For enquiries or comments about this document, please contact ENISA via the certification webpage Ask questions, find answers - European Union Cybersecurity Certification.

ACKNOWLEDGEMENTS

ENISA AHWG ON EUMSS

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN Number, DOI Number (IF APPLICABLE)

Table of Contents

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

INTRODUCTION AND MAIN PRINCIPLES

0 INTRODUCTION AND MAIN PRINCIPLES

0.1 INTRODUCTION

On 25 April 2025, the European Commission requested ENISA to prepare a candidate European Cybersecurity Certification Scheme for Managed Security Services (MSS) pursuant to Article 48(1) of Regulation (EU) 2019/881 (Cybersecurity Act). ENISA replied positively to the request on 23 June 2025.

As a next step, ENISA established an Ad Hoc Working Group on Managed Security Services Certification[1] (EUMSS AHWG) to support the preparation of the candidate Scheme. The 13th of October the virtual Kick off meeting of the AHWG was held, on the 18th and 19th of November the first physical meeting took place.

This document is the result of the work of ENISA with the support the EUMSS AHWG and proposes a candidate European Cybersecurity Certification Scheme for Managed Security Services, hereinafter referred to as the EUMSS Scheme, in accordance with Regulation (EU) 2019/881. This version will be subject to a public review.

0.2 MAIN PRINCIPLES

0.2.1 SUBJECT MATTER AND MANDATE

This European Cybersecurity Certification Scheme for Managed Security Services (EUMSS) is developed by ENISA pursuant to Article 48(1) of Regulation (EU) 2019/881 (Cybersecurity Act), following a formal request from the European Commission.

The Scheme establishes a European cybersecurity certification structure for specific Managed Security Services, in accordance with the mandate conferred on ENISA.

The Scheme is designed in order to provide a harmonised and proportionate framework that supports cross-border service provision and Union-level crisis response capabilities, cover the incident management lifecycle (as per current request) and other relevant MSS (as per future requests). It builds, where appropriate, on existing European cybersecurity certification practices and assessment methodologies, while introducing EUMSS-specific elements necessary to address the operational and security characteristics of Managed Security Services. It does not however cover the certification of organisations (i.e. the providers of the services).

0.2.2 STRUCTURE AND SCOPE OF THE SCHEME: HORIZONTAL AND VERTICAL LAYERS

The EUMSS Scheme follows a layered approach, consisting of a horizontal set of common requirements hereinafter referred to as Horizonal Layer (HoLa) and a series of verticals, hereinafter

[1] https://certification.enisa.europa.eu/browse-topic/eumss_en

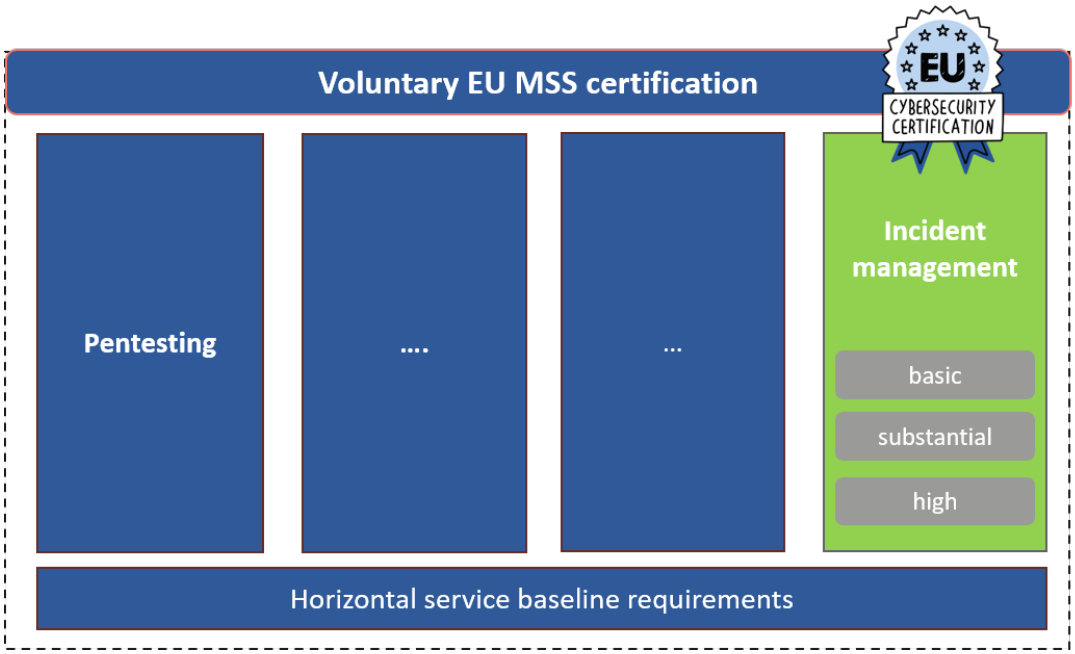
referred to as Vertical Layers (VeLa). These verticals define specific technical and operational requirements, some of which may be shared across multiple verticals.

Principally in line with the Commission request and the priorities linked to the Cyber Solidarity Act, the present version of the Scheme focuses on the Incident Management Lifecycle vertical and more specifically to the Incident Response service profile. A candidate cybersecurity Certification Scheme for managed security services in the areas covered by the Cybersecurity Emergency Mechanism would support the establishment of the EU Cybersecurity Reserve. Once EUMSS is in place, the provider delivering services under the umbrella of the EU Cybersecurity Reserve shall be certified in accordance with that Scheme within 2 years from the date of application thereof.

Future iterations of the EUMSS Scheme may extend its scope to additional service profiles within the incident management lifecycle, such as threat detection, incident qualification and escalation, recovery and post-incident analysis, and to additional Vertical Layers covering other Managed Security Services. Such extensions may be introduced through the update of the Scheme, in accordance with CHAPTER IX: UPDATE OF THE SCHEME, where they fall within the MSS scope and mandate of this Scheme and where the corresponding requirements, evaluation approach and transition arrangements are defined.

In accordance with the mandate conferred by Article 2(14a) of Regulation (EU) 2019/881 (Cybersecurity Act), future additional Vertical Layers may cover in particular penetration testing, security audits, consulting related to technical support, cyber threat intelligence provision, and risk assessment related to technical support.

The following image represents the structure of the certification, the pentesting Vertical Layer is a proposal that need to be requested by the commission.



0.2.3 HORIZONTAL LAYER

The Horizontal Layer provides one common set of baseline requirements applicable to all Managed Security Services certified under this Scheme. The Horizontal Layer does not constitute a stand-alone basis for certification. These baseline requirements apply as a mandatory prerequisite for each certified service profile and are the same for all assurance levels (See ASSURANCE LEVELS for details on assurance levels). However, the evaluation depth and rigour applied to those requirements shall correspond to the assurance level requested for the relevant service profile, in accordance with the evaluation methodology defined in this Scheme.

The Horizontal Layer is designed to ensure the security, reliability and operational resilience of Managed Security Services throughout their lifecycle, it defines baseline requirements in the following domains:

- Secure service and platform design, ensuring that Managed Security Services are designed with security by design and by default principles;
- Deployment and transition management, ensuring that services are securely integrated into customer environments and that transitions are managed in a controlled and secure manner;
- Availability and continuity management, ensuring resilience against disruptions and the continuity of service delivery;
- Operational service management, ensuring that services are effectively operated, monitored and managed on an ongoing basis; and
- Continuous improvement and technology maintenance, ensuring that technologies supporting Managed Security Services remain secure, up to date and fit for purpose over time.

Furthermore, to reflect the service-oriented nature of Managed Security Services and to ensure structural consistency, the Horizontal Layer establishes generic operational requirements aligned with the three core phases of service delivery (adapted from ISO 20700:2017):

- Setup Phase: Establishes the foundational baseline service delivery framework applicable to all MSS types before execution activities commence, including generic requirements for service definition, contract management, client onboarding, and the establishment of a service agreement
- Execution Phase: Establishes the framework for the operational delivery of the MSS, ensuring that the core activities operate securely within the horizontal requirements for continuity management, quality assurance, and secure design
- Closure Phase: Establishes general frameworks for the proper completion of service activities, including generic requirements for service review, knowledge retention, and continuous improvement cycles applicable to all MSS types

The Horizontal Layer is further specified, both in terms of security controls and means to assess their implementation, through Annex II to the Scheme.

0.2.4 VERTICAL LAYER

The Vertical Layer defines service-specific requirements applicable to particular Managed Security Services and services profiles included in these services.

Each service profile represents a distinct object of certification and may define specific technical, operational and assurance requirements, including reinforcements of the baseline controls defined in the Horizontal Layer that are necessary for the specific service profile.

The Vertical Layer and related reinforcements of the baseline controls defined in the Horizontal Layer that are necessary for the specific service profile are further specified, both in terms of security controls and means to assess their implementation, through Annex III to the Scheme.

0.2.5 RELATIONSHIP WITH NIS2

The Horizontal Layer of the Scheme includes baseline security controls that tailor specific requirements from the NIS2 Implementing Regulation (EU) 2024/2690 that are relevant for managed security services.

EUMSS certification may provide evidence relevant to selected cybersecurity risk-management requirements where the EUMSS requirements are aligned with requirements of Commission Implementing Regulation (EU) 2024/2690. However, EUMSS certification does not constitute, replace or predetermine compliance with Directive (EU) 2022/2555 or supervision by competent national authorities under that Directive.

0.2.6 DISTINCTION BETWEEN “WHAT” IS CERTIFIED AND “HOW” CONFORMITY IT IS ASSESSED

Given that the Scheme is designed to cover multiple service profiles within one or more Vertical Layers, which may be developed and updated progressively over time, it is essential to distinction the scope of the certification ("what") from the method of conformity assessment ("how"):

- what is the scope of the certification**,** and;
- how conformity is assessed**.**

This distinction is essential given that the Scheme is designed to cover multiple service profiles within one or more Vertical Layers, which may be developed and updated progressively over time.

0.2.7 "WHAT" IS CERTIFIED: SCOPE AND SUBJECT MATTER OF CERTIFICATION

The scope of certification (the "what") includes:

- the object of certification,
- the assurance level,
- the elements of the service subject to assessment,
- the requirements applicable to each service profile, and
- the baseline requirements defined in the Horizontal Layer.

A certified MSS service shall be considered as the capability of the provider to deliver this service under the conditions of this Scheme to all clients, and certificates shall not be issued for each instance of the service offered for each individual client.

0.2.8 "HOW" CONFORMITY IS ASSESSED: CONFORMITY ASSESSMENT APPROACH

Conformity assessment will be performed by accredited and where necessary authorised Conformity Assessment Bodies (CABs), and the EUMSS Certification Scheme establishes a common assessment approach for the evaluation of all Managed Security Services under to Article 60 of Regulation (EU) 2019/881 (Cybersecurity Act).

The Scheme relies on ISO/IEC 17065 and CEN/CENELEC TS 18072 — "Requirements for conformity assessment bodies certifying ICT services" — as the reference standard defining the organisational, competence and procedural requirements applicable to CABs certifying ICT services.

To ensure consistency throughout the Scheme, the following terminology convention is applied:

- Certification Requirements: Refers to the mandatory normative obligations and rules according to this Scheme (including its horizontal and Vertical Layers) that the service and the provider must fulfil to obtain and maintain the certification.
- Cybersecurity Controls: Refers to the specific technical, operational, methodological, or organisational measures that the Managed Security Service Provider designs, implements, and operates to mitigate cybersecurity risks and fulfil the certification requirements.

Therefore, within EUMSS:

- The horizontal and vertical certification requirements are set out in the Annexes. Supporting evaluation guidelines, based on evaluation activities aligned with CEN/CENELEC TS 18072, shall be developed to support the harmonised assessment of whether those requirements are fulfilled. Such guidelines should be made available before the date of application of the Scheme.
- the detailed evaluation techniques, sampling depth, technical verification activities and evidence review mechanisms will be determined by the CAB in accordance with:
    - the Scheme requirements,
    - the applicable assurance level,
    - and the characteristics of the service under evaluation.

0.2.9 ASSURANCE LEVELS

In accordance with Regulation (EU) 2019/881 (Cybersecurity Act), the EUMSS Certification Scheme refers to the three established assurance levels: 'basic', 'substantial', and 'high'.

The chosen assurance level must be commensurate with the level of risk associated with the intended use of the Managed Security Service, considering the probability and impact of a cyber incident.

For the initial version of the EUMSS Certification Scheme, the differentiation between these three assurance levels is reflected primarily in how the certification requirements are assessed, rather than in the definition of additional security controls. This might change in further updates to the Scheme.

Assurance levels under the EUMSS Certification Scheme are granted at the level of the certified service profile. The Horizontal Layer does not constitute a stand-alone object of certification and no separate assurance level shall be granted for the Horizontal Layer alone. Nevertheless, where the Horizontal Layer requirements are evaluated as part of a service-profile certification, the depth and rigour of their assessment shall correspond to the assurance level requested for that service profile.

For the Incident Response service profile, the Scheme defines three assurance levels. The requirements applicable to the service profile consist of:

- the Horizontal Layer baseline requirements, which apply across all service profiles at all levels; and
- any service-profile-specific requirements, including reinforcements of the Horizontal Layer, defined for the Incident Response service profile, for each assurance level.

0.3 REFERENCES

1. The EU Cybersecurity Act (CSA): Regulation - 2019/881 - EN - EUR-Lex
2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2): Directive - 2022/2555 - EN - EUR-Lex
3. Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive - 2022/2555 - EN - EUR-Lex as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers
4. Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act): Regulation - EU - 2025/38 - EN - EUR-Lex
5. Amendment to CSA mentioning MSS: Regulation - EU - 2025/37 - EN - EUR-Lex
6. European Commission Request for the preparation of a candidate Managed Security Services : https://certification.enisa.europa.eu/document/download/ebf34ee5-8d9d-4e0f-9407-8f87385de6b9_en?filename=MSS%20certification%20scheme%20-%20Request%20to%20ENISA.pdf
7. ENISA response to the request of 23 June 2025
8. Ad Hoc Working Group on EUMSS: EUMSS - European Union Cybersecurity Certification - European Union

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SCHEME CORE PART

1 CHAPTER I: GENERAL REQUIREMENTS

1.1 SUBJECT MATTER AND SCOPE

Explanatory note: This section establishes the scope and modular architecture of the Scheme, defining the interplay between the horizontal and Vertical Layers, and clearly sets the boundaries of the current scope while providing for future extensions as requested by the Commission.

1. This document establishes the candidate European Cybersecurity Certification Scheme for Managed Security Services ('EUMSS').

2. This Scheme applies to managed security services as defined in Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services (Text with EEA relevance).

3. This Scheme may apply to Managed Security Services provided for IT, OT or mixed IT/OT environments. Where the certified service relates to operational technology, industrial control systems, cyber-physical systems or safety-related operational environments, the certified scope and Service Agreement shall identify the relevant OT-specific constraints, including safety, environmental, operational, approval and change-management requirements. These constraints shall be taken into account when applying the horizontal and vertical requirements of this Scheme.

4. To accommodate the diverse nature of Managed Security Services, the EUMSS Scheme adopts a modular architecture consisting of:

   (a) A Horizontal Layer, which establishes a common, mandatory set of baseline security, reliability, and operational resilience requirements applicable to all Managed Security Services, regardless of their specific operational domain.

   (b) Vertical Layers, which define service-specific cybersecurity requirements tailored to particular Managed Security Service domains. Each Vertical Layer is further divided into specific service profiles that represent distinct objects of certification.

5. This first version of the Scheme covers the Incident Management lifecycle Vertical Layer, focusing on the Incident Response service profile.

6. To ensure that the framework remains adaptable to the evolving cybersecurity threat landscape and market needs, the EUMSS Scheme may be progressively extended through its update, in accordance with CHAPTER IX: UPDATE OF THE SCHEME, to include additional service profiles and additional Vertical Layers falling within the MSS scope and mandate of this Scheme. Such extensions may include:

(a) Additional service profiles within the Incident Management lifecycle Vertical Layer, from identification and detection through to recovery, and post-incident review.

(b) Additional Vertical Layers and service profiles covering other managed security services, such as penetration testing, security audits and consulting, including expert advice, related to technical support.

1.2 DEFINITIONS

Explanatory note: Within the context of the EUMSS Scheme, "Conformity Assessment Body" (CAB) is used as the overarching legal term for entities accredited to evaluate Managed Security Services under Regulation (EU) 2019/881 (Cybersecurity Act). A "Conformity Assessment Body" specifically refers to a CAB in its capacity to review evaluation results and formally issue, suspend, or withdraw an EUMSS certificate. While the terms may appear interchangeably, any Conformity Assessment Body operating under this Scheme is, by definition, a legally accredited Conformity Assessment Body.

For the purposes of this Scheme, the following definitions shall apply:

(1) managed security service: a service provided to a third party consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, such as incident handling, penetration testing, security audits and consulting, including expert advice, related to technical support;[2]

(2) scope of certification: unambiguous identification of the Managed Security Service and the specific Service Profile for which the certification is granted, and the specific technical, physical, and functional boundaries of the service evaluated by the Conformity Assessment Body. A certified MSS service shall be considered as the capability of the provider to deliver this service under the conditions of this Scheme to all clients, and certificates shall not be issued for each instance of the service offered for each individual client.[3]

(3) service profile: a defined Managed Security Service, or a defined subset of such service, that constitutes an object of certification under this Scheme. In this version of the Scheme, the certifiable service profile is the Incident Response service profile within the Incident Management lifecycle Vertical Layer.

(4) Horizontal Layer: the common, mandatory set of security, reliability and operational resilience requirements applicable to all Managed Security Services certified under this Scheme.

(5) Vertical Layer: a Managed Security Service domain that groups one or more service profiles and defines service-specific cybersecurity requirements tailored to that domain.

(6) Conformity Assessment Body: conformity assessment body as defined in Article 2, point (13), of Regulation (EC) No 765/2008, which performs certification activities.

(7) material change: modification of the service that impacts its certificate and is significant to intended users
Note 1 to entry: Materiality is the concept that misstatements, individually or aggregated, can influence the reliability of the claim or decisions made by the intended user.
Note 2 to entry: Materiality can be qualitative or quantitative.

(8) service agreement: a document covering characteristics and properties of the service to be delivered.
Note 1 to entry: the service agreement contains elements prescribed both in the Horizontal Layer and the Vertical Layer.
[SOURCE: ISO/IEC 17029:2019, 3.16, modified]

(9) subservice: a service, function or process used by the applicant to design, operate, manage or deliver the Managed Security Service submitted for certification, where that service, function, process or capability is provided by an internal or external subservice organisation itself.

[2] Article 2(14a) of Regulation (EU) 2019/881 (Cybersecurity Act)
[3] Article 54(1) of Regulation (EU) 2019/881 (Cybersecurity Act)

(10) subservice organisation: an internal or external organisation that provides a subservice used by the applicant for the design, operation, management or delivery of the Managed Security Service submitted for certification.

(11) inclusive method: an evaluation method under which the controls implemented by a subservice organisation that are necessary to meet the requirements of this Scheme are included within the scope of the evaluation.

(12) carve-out method: an evaluation method under which the controls implemented by a subservice organisation are not directly included within the scope of the evaluation, and the evaluation relies on assumptions regarding those controls and on assurance documentation or other evidence supporting those assumptions.

1.3 EVALUATION STANDARDS

Explanatory note: This section defines the hierarchy of standards used to evaluate Managed Security Services. CEN/CENELEC TS 18072 extends the ISO/IEC 17065 conformity assessment framework by providing specific methodology for the certification of ICT services, including advanced concepts such as operating effectiveness. Therefore, CABs shall comply with ISO/IEC 17065 for their certification activities and apply TS 18072 as the service-specific evaluation methodology. Established auditing guidelines, such as ISO 19011 and ISO/IEC 27007, may be used when assessing management system components of the service's Horizontal Layer.

1. The conformity assessment body shall apply the following primary standards and methodologies to evaluations performed under the EUMSS Scheme:

    a) EN ISO/IEC 17065 (Conformity assessment — Requirements for bodies certifying products, processes and services), which establishes the general requirements for the competence, consistent operation, and impartiality of the Conformity Assessment Body.

    b) CEN/CENELEC TS 18072 (Requirements for conformity assessment bodies certifying ICT services), which builds upon EN ISO/IEC 17065 by extending its conformity assessment principles to the certification of ICT services and by defining service-specific assessment activities, evidence types and evaluation approaches, including concepts such as operating effectiveness.

2. In addition, the conformity assessment body shall apply the evaluation methodologies and criteria laid down in Chapter II of this Scheme.

3. Assessment of the provider's management system shall be limited to those controls and processes that directly affect conformity of the service with this Scheme. Where useful for audit planning or competence considerations, the conformity assessment body may use relevant principles of EN ISO/IEC 17021-1 and EN ISO/IEC 27006 as supplementary guidance. Certification decisions shall remain based on the service requirements of this Scheme and shall be governed by EN ISO/IEC 17065, complemented by CEN/CENELEC TS 18072 for the certification of ICT services.

1.4 ASSURANCE LEVELS

Explanatory note: Assurance levels under the EUMSS Certification Scheme are defined exclusively at the level of the service profile (Vertical Layer). Once defined at the Vertical Layer, an assurance level may require additions (reinforcements) to the Horizontal Layer. There is only one assurance level per service profile possible and that one is dictated by the Vertical Layer. This means that it is not possible to have separate Horizontal Layer assurance level.
For the Incident Response service profile, the Scheme defines three assurance levels. The requirements applicable to the service profile consist of:

- *the Horizontal Layer baseline requirements, which apply across all service profiles at all levels; and*
- *any service profile-specific requirements, including reinforcements of the Horizontal Layer, defined for the Incident Response service profile, for each assurance level.*

1. Certification bodies shall issue EUMSS certificates at assurance level ‘basic’, ‘substantial’ or ‘high’.

2. The choice of the appropriate certification and its corresponding assurance level is a voluntary decision of the applicant. However, in accordance with Article 52(1) of Regulation (EU) 2019/881 (Cybersecurity Act), the chosen assurance level shall be based on an analysis of the risks and be commensurate with the level of risk associated with the intended use of the specific Managed Security Service profile being certified, its operational environment, and the specific needs of the clients.

3. Assurance levels under the EUMSS Certification Scheme are granted at the level of the specific service profile. Each EUMSS certificate shall refer to only one assurance level ('basic', 'substantial', or 'high') corresponding to the specific Managed Security Service profile being certified.

4. Where a MSSP delivers multiple service profiles or a combined service package to the same customer, the provider may hold and present distinct EUMSS certificates at different assurance levels for each respective service profile. In such cases, the provider shall ensure clear transparency to the customer regarding which specific components of the packaged service are certified and at which corresponding assurance level. The MSSP shall communicate and make available to the customer the certified MSS scope and assurance levels, using as a reference the certification website hosted by ENISA where the certificates will be published.[4]

5. Where different service profiles of the same provider are certified by different conformity assessment bodies, the recognition between bodies of a Horizontal Layer evaluation already performed for that provider is not defined in this version of the Scheme and is identified as an open item to be addressed in a future revision.

6. The distinction between assurance levels shall be reflected in the requirements applicable to the certified service profile and in the rigour, depth and confidence of the conformity assessment activities carried out by the Conformity Assessment Body in accordance with CEN/CENELEC TS 18072. Such activities may include, as applicable to the requested assurance level, increased sampling, verification of operating effectiveness over a defined

[4] in accordance with Article 50(1) of Regulation (EU) 2019/881

period, vulnerability identification, penetration testing where relevant, or substitute evaluation activities with equivalent effect.

7. The Horizontal Layer requirements set out in Annex II shall apply to all assurance levels. They shall not be certified separately. Where they are assessed as part of a service-profile certification, their evaluation shall be performed with the depth and rigour corresponding to the assurance level requested for that service profile.

8. The EUMSS Scheme follows a cumulative assurance model. Consequently, compliance with the Vertical Layer requirements of a higher assurance level inherently requires and implies compliance with all requirements applicable to the lower assurance level(s) for the same service profile. A service evaluated at assurance level ‘substantial’ shall also fulfil all requirements applicable to the ‘basic’ level, and a service evaluated at assurance level ‘high’ shall also fulfil all requirements applicable to both the ‘basic’ and ‘substantial’ levels.

1.5 CONFORMITY SELF-ASSESSMENT

Explanatory note: Article 53 of Regulation (EU) 2019/881 (Cybersecurity Act) allows European Schemes to permit conformity self-assessment for the 'basic' assurance level under the sole responsibility of the provider. However, to guarantee a consistent baseline of trust and independent verification for Managed Security Services across the Union, the EUMSS Scheme does not permit pure conformity self-assessment. All EUMSS certificates, including those at the 'basic' level, must be issued by an independent Conformity Assessment Body. For the 'basic' level, the conformity assessment body's evaluation activities will heavily rely on the CAB's reviewing the self-assessment or internal audit documentation provided by the applicant.

1. Conformity self-assessment under the sole responsibility of the Managed Security Service Provider, within the meaning of Article 53 of Regulation (EU) 2019/881 (Cybersecurity Act), shall not be permitted for any EUMSS certificate, regardless of the assurance level.

2 CHAPTER II: CERTIFICATION OF MSS

SECTION I: SPECIFIC STANDARDS AND REQUIREMENTS FOR EVALUATION

2.1 CRITERIA FOR CERTIFYING EUMSS

Explanatory note: This section codifies the modular architecture of the Scheme. It explicitly establishes a 1:1:1 mapping: one certificate corresponds to one specific Service Profile at one specific assurance level. A certificate is only issued when the service demonstrates conformity with both the foundational baseline (Horizontal Layer) and the operational specificities of the chosen service (Vertical Layer). It also introduces the requirement for a defined "scope of certification" and explicitly links to the evidence reuse mechanism for providers seeking multiple certificates.

1. Certification of a Managed Security Service shall be carried out against a clearly defined scope of certification, which shall unambiguously identify the technical, physical, and functional boundaries of the service submitted for evaluation.
2. An EUMSS certificate shall be issued for a single, specific service profile and for one selected assurance level. A provider may hold multiple EUMSS certifications for different service profiles, at different assurance levels, or for different scopes within the same service profile. In cases where the assurance of the service profiles is not hierarchical, each profile shall constitute a separate and distinct EUMSS certificate.
3. To obtain an EUMSS certificate, the specific Managed Security Service shall be evaluated and demonstrate conformity with all the following elements:
   a) a baseline security, reliability and operational resilience requirements defined in the Horizontal Layer set out in Annex II, which apply as a mandatory prerequisite and shall be assessed with the depth and rigour corresponding to the assurance level requested for the relevant service profile; and[5]
   b) the specific technical, operational and competence requirements defined in the applicable Vertical Layer and service profile set out in ANNEX III: VERTICAL LAYER, including any requirements or reinforcements applicable to the corresponding assurance level.
4. Where a provider applies for multiple distinct EUMSS certificates, the Conformity Assessment Body shall consider existing evidence already obtained or provided for previous EUMSS evaluations, following the rules of ISO/IEC 17065 where it determines that such evidence remains relevant, valid, sufficient and appropriate for the requested service profile, assurance level and scope of certification.

[5] Including a generic ISMS standard which forms the foundation for the EUMSS specific control set. The possible ISMS standards are numbered in the ANNEX XI: ACCEPTABLE ISMS STANDARDS FOR HOLA.

2.2 EVALUATION CRITERIA AND METHODS FOR MSS

Explanatory note: This section establishes the foundational criteria and methodological framework for evaluating Managed Security Services (MSS). It clarifies the distinction between the assessment methodology (the "how"), governed by CEN/CENELEC TS 18072, and the actual security requirements (the "what"), which are defined in the Horizontal and Vertical Layers of this Scheme. It explicitly integrates relevant international standards (such as ISO/IEC 27001 for baseline security management, ISO/IEC 27035 for incident response, ISO/IEC 20000-1 for service management and ISO 22301 for business continuity management) and mandatory legal requirements into the evaluation criteria. Although specific state-of-the-art and supporting documents are not yet available for this initial version of the Scheme, this section establishes the necessary legal requirements to seamlessly incorporate them once they are developed by ENISA and endorsed by the European Cybersecurity Certification Group (ECCG). Finally, it details the specific evaluation activities required for the 'substantial' and 'high' assurance levels in accordance with the Cybersecurity Act.

1. A Managed Security Service submitted for certification shall, as a minimum, be evaluated in accordance with the following criteria and methods:

   (a) the standards defined in section EVALUATION STANDARDS;

   (b) the baseline security, reliability and operational resilience requirements defined in the Horizontal Layer set out in Annex II, assessed with the depth and rigour corresponding to the assurance level requested for the relevant service profile;

   c) the specific technical, operational and competence requirements defined in the applicable Vertical Layer and service profile set out in Annex III, including any requirements or reinforcements applicable to the corresponding assurance level;

   d) the assurance level associated with the intended use of the Managed Security Service concerned pursuant to Article 52 of Regulation (EU) 2019/881 (Cybersecurity Act), and its security functions that support the security objectives set out in Article 51 of Regulation (EU) 2019/881 (Cybersecurity Act);

   e) where applicable, any state-of-the-art documents or guidance listed in Annex I and published by ENISA to support the consistent application of the Scheme, once they are available.

The evaluation shall be performed in accordance with the Conformity Assessment Bodies internal procedures, accredited by a national accreditation body against EN ISO/IEC 17065 and CEN/CENELEC TS 18072. These evaluation activities shall include at least a review of the technical documentation of the Managed Security Service and at least one on-site visit, which may be conducted at the premises of the applicant or at another location where the Managed Security Service is designed, operated, managed or delivered. If this is not reasonable the used method shall be augmented and mitigating measures should be in place to ensure that the use assessment method provides a sufficient level of confidence whether the documented controls are implemented and used. The objective is to provide assurance that the service is suitably designed and implemented to minimise the known basic risks of incidents and cyberattacks. Where a documentation review alone is not sufficient or appropriate to the nature of the service, the Conformity Assessment Body shall perform complementary evaluation activities with equivalent effect, such as structured interviews with service personnel, observation of service processes, inspection of service environments, or other activities consistent with CEN/CENELEC TS 18072.

2. As part of the evaluation methods for the ‘basic’ assurance level, the applicant shall conduct a comprehensive internal audit and self-evaluation against the requirements of the Scheme. The Conformity Assessment Body shall evaluate the conformity of the Managed Security Service by reviewing the applicant’s self-evaluation report, supporting technical documentation and other relevant evidence.

3. As part of the evaluation methods for the 'substantial' assurance level, the conformity assessment body shall undertake evaluation activities that include at least a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the Managed Security Service correctly implements and operates the necessary security controls.

4. As part of the evaluation methods for the 'high' assurance level, the conformity assessment body shall undertake evaluation activities that include at least a review to demonstrate the absence of publicly known vulnerabilities, testing to demonstrate that the Managed Security Service correctly implements and operates the necessary security controls at the state of the art, and an assessment of the resistance of the service to skilled attackers. Where vulnerability assessment and/or penetration testing activities are considered necessary by the conformity assessment body, the MSSP shall provide the conformity assessment body with the results of such activities, including the scope, methodology, identified findings, and remediation status where applicable. The conformity assessment body shall evaluate such evidence as part of the certification assessment.

5. Where any of the evaluation activities referred to in previous paragraphs, such as penetration testing, are not relevant or appropriate due to the specific nature of the Managed Security Service—such as services relying exclusively on physical, manual, or procedural activities without a dedicated IT delivery platform—substitute evaluation activities with equivalent effect shall be undertaken by the conformity assessment body as described in the ADDITIONAL OR SPECIFIC REQUIREMENTS FOR A chapter.

6. Where state-of-the-art documents have been established and are applicable, in exceptional and duly justified cases, a conformity assessment body may request to refrain from applying a state-of-the-art document. In such cases, the conformity assessment body shall inform the national cybersecurity certification authority with a duly reasoned justification for its request and propose an alternative evaluation methodology. The national cybersecurity certification authority shall assess the justification for an exception and, where justified, approve or amend the alternative evaluation methodology to be applied. Pending the decision of the national cybersecurity certification authority, the conformity assessment body shall not issue any certificate. The national cybersecurity certification authority shall notify the approved exception, without undue delay, to the European Cybersecurity Certification Group, which may issue an opinion, which may issue an opinion within 30 days. If no opinion is provided from the ECCG in 30 days, the exception is automatically approved. The national cybersecurity certification authority shall take utmost account of the opinion of the European Cybersecurity Certification Group.

2.3 EVALUATION OF SUBSERVICES AND DEPENDENCY ANALYSIS

Explanatory note: This section is needed as TS 18072 treats subservices as part of the evaluation method and dependency analysis, not only as supplier controls. TS 18072 requires the evaluator to determine, for each subservice, whether the inclusive or carve-out method is used, and only one method shall be defined per subservice; it also requires identification of subservice organisations whose assurance documentation may be reused in dependency analysis. TS 18072 Annex B then requires dependency analysis to verify whether assurance documentation for internal or external subservice organisations is adequate for the targeted assurance level.

1. Where the Managed Security Service submitted for certification relies on subservices, including subservices provided by internal or external subservice organisations, the applicant shall identify those subservices and describe their role in the design, operation, management or delivery of the certified service.

2. For each relevant subservice, the CAB shall identify whether the subservice is treated according to the inclusive method or the carve-out method, in accordance with CEN/CENELEC TS 18072. Only one method shall be defined for each subservice.

3. Under the inclusive method, the requirements implemented by the subservice organisation shall be included within the scope of the evaluation to the extent necessary to determine conformity of the Managed Security Service with this Scheme.

4. Under the carve-out method, the controls implemented by the subservice organisation shall not be directly included within the scope of the evaluation. In such cases, the applicant shall identify the assumptions made regarding the controls implemented by the subservice organisation and shall provide assurance documentation sufficient to support those assumptions.

5. Where the carve-out method is used, the Conformity Assessment Body shall perform a dependency analysis in accordance with CEN/CENELEC TS 18072. The dependency analysis shall determine whether the assurance documentation available for the relevant subservice is sufficient and appropriate to support the conformity assessment of the Managed Security Service at the requested assurance level.

6. The dependency analysis shall be performed for each relevant subservice and for each requirement of this Scheme for which the applicant relies, in whole or in part, on controls implemented by the subservice organisation.

7. Assurance documentation used for dependency analysis may include, where relevant, certificates, certification reports, audit reports, assurance reports, statements of applicability, bridge letters, or other documentation demonstrating the design, implementation or operating effectiveness of controls implemented by the subservice organisation.

8. The Conformity Assessment Body may rely on assurance documentation related to a subservice only where it has determined that the documentation is relevant to the certified service scope, covers the relevant requirements or assumptions, corresponds to the requested assurance level, is valid for the relevant period, and has been issued by an organisation whose competence and impartiality can be established.

9. Where the subservice has been certified under a Certification Scheme recognised for the purposes of this Scheme listed in the NATIONAL SCHEMES COVERED BY THE EUMSS, the

Conformity Assessment Body may simplify the dependency analysis in accordance with CEN/CENELEC TS 18072. Such simplification shall not remove the obligation to determine whether the certified subservice is relevant to the certified Managed Security Service and to the requirements relied upon by the applicant.

10. Where the assurance documentation available for a subservice is incomplete, outdated, insufficient, not relevant to the certified scope, not valid for the relevant period, or does not provide assurance corresponding to the requested assurance level, the Conformity Assessment Body shall request additional information through the applicant or perform additional evaluation activities limited to the controls or assumptions relevant to the subservice.

11. Where sufficient information cannot be obtained to determine whether the assumptions related to a subservice are met, the Conformity Assessment Body shall document the limitation, assess its impact on the evaluation conclusion and take it into account in the certification decision. Where the limitation affects the ability to determine conformity with the requirements of this Scheme, a non-conformity shall be raised.

12. Where assurance documentation related to a subservice identifies non-conformities (e.g. control deficiencies, deviations or exceptions affecting controls relied upon by the applicant), the Conformity Assessment Body shall assess their impact on the conformity of the Managed Security Service with this Scheme, including whether corrective actions or compensating controls are sufficient.

13. The results of the dependency analysis, including the subservices identified, the method applied to each subservice, the assurance documentation used, the assumptions made, any limitations or non-conformities identified, and the conclusions reached, shall be documented in the certification assessment report and considered in the certification decision.

SECTION II: ISSUANCE, RENEWAL AND WITHDRAWAL OF EUMSS CERTIFICATES

2.4 INFORMATION NECESSARY FOR CERTIFICATION

Explanatory note: Section 7.4.4.2.2.3 of TS 18072 requires the Conformity Assessment Body (CAB) to evaluate the "operating effectiveness" of controls over a "specified period," noting that Certification Schemes can specify longer periods for 'high' than for 'substantial'.

1. An applicant for certification under EUMSS shall provide or otherwise make available to the Conformity Assessment Body all information necessary for the certification activities.

2. Applicants for certification may provide to the Conformity Assessment Body existing documentation, audit records, certificates, assessment results or other evidence relevant to the requested EUMSS certification. As specified by ISO/IEC 17065 the Conformity Assessment Body may consider such evidence where it determines that the evidence is relevant, valid, sufficient and appropriate for the specific EUMSS evaluation, taking into account the requested service profile, assurance level and scope of certification.

3. The consideration of existing evidence shall not reduce the responsibility of the Conformity Assessment Body to perform the evaluation activities necessary to support the certification decision in accordance with this Scheme, EN ISO/IEC 17065 and CEN/CENELEC TS 18072. The Conformity Assessment Body shall document in the certification assessment report any existing evidence considered, including its origin, scope, period of validity or period covered, limitations, and the justification for considering it relevant, valid, sufficient and appropriate.

4. In accordance with CEN/CENELEC TS 18072, the evidence required from the applicant shall correspond to the assurance level requested for the certified service profile and shall cover the applicable requirements.

a) For an EUMSS certificate at assurance level ‘basic’, the applicant shall provide sufficient and appropriate evidence demonstrating that the applicable requirements are suitably fulfilled and implemented at the time of the evaluation. The applicant is not required to provide evidence of operating effectiveness over a specified continuous period.
b) For an EUMSS certificate at assurance level ‘substantial’, the applicant shall provide sufficient and appropriate evidence demonstrating that the applicable controls have operated effectively for a minimum period of 6 months immediately preceding the evaluation.
c) For an EUMSS certificate at assurance level ‘high’, the applicant shall provide sufficient and appropriate evidence demonstrating that the applicable controls have operated effectively for a minimum period of 12 months immediately preceding the evaluation.

5. Applicants for certification shall also provide the Conformity Assessment Body with the following information:

a) the link to their website containing the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881 (Cybersecurity Act)
b) a description of the applicant’s vulnerability management and vulnerability disclosure procedures.

6. All relevant documentation referred to in this Chapter shall be retained by the Conformity Assessment Body and the applicant for a period of 5 years after the expiry of the certificate.

7. To enable the Conformity Assessment Body to evaluate the operating effectiveness of the Managed Security Service in accordance with CEN/CENELEC TS 18072, the applicant shall provide access to relevant service records, incident case files, and tamper-evident audit trails covering a minimum operational period of six (6) months for the 'substantial' assurance level, and twelve (12) months for the 'high' assurance level.

2.5 CONDITIONS FOR ISSUANCE OF AN EUMSS CERTIFICATE

Explanatory note: Since the current scope of the EUMSS Scheme is limited to a single service profile, the formal concept of composition is not addressed in this version. The Conformity Assessment Body shall issue an EUMSS certificate only where it has obtained sufficient and appropriate evidence demonstrating conformity with the applicable Horizontal Layer and Vertical Layer requirements for the requested service profile, assurance level and scope of certification.
Where the NCCA applies the "prior approval" (CSA article 56-6(a)) the certificate at Assurance level High shall only be issued after the prior approval from the NCCA involved.

1. The certification bodies shall issue an EUMSS certificate where all of the following conditions are met:

(a) the type of the MSS falls within the scope of the accreditation, and where applicable of the authorisation, of the Conformity Assessment Body issuing the certificate;

(b) the applicant for certification has signed a statement undertaking all commitments listed in paragraph 2;

(c) the Conformity Assessment Body has concluded the review of the evaluation with a positive recommendation in accordance with the evaluation standards, criteria and methods referred to in EVALUATION CRITERIA AND METHODS FOR MSS;

(d) to retain the evidence required for INFORMATION NECESSARY FOR CERTIFICATION 7. for 5 years after the termination or withdrawal of the certificate.

2. The applicant for certification shall undertake the following commitments:

(a) to provide the Conformity Assessment Body with all the necessary complete and correct information, and to provide additional necessary information if requested;

(b) not to promote the MSS as being certified under the EUMSS before the EUMSS certificate has been issued;

(c) to promote the MSS as being certified only with respect to the scope set out in the EUMSS certificate;

(d) to cease immediately the promotion of the MSS as being certified in the event of the suspension, withdrawal or expiry of the EUMSS certificate;

(e) to ensure that the MSS delivered with reference to the EUMSS certificate is strictly identical to the MSS subject to the certification;

(f) to respect the rules of use of the mark and label established for the EUMSS certificate in accordance with section MARK AND LABEL.

(g) inform the Conformity Assessment Body immediately if major/material changes have happened or are imminent to occur, e.g. major changes in the service delivery platform, in the location of the provider or in the ISMS, so that a special evaluation can be scheduled.

2.6 CONTENT AND FORMAT OF A CERTIFICATE

Explanatory note: Any certificate issued under EUMSS needs to be accompanied by a certification report, their respective contents being defined in Annexes, and which be made publicly available. In addition, the Conformity Assessment Body needs to produce a certification assessment report, containing more detailed information, to be shared only with the provider of the MSS and the relevant national cybersecurity certification authority.

1. An EUMSS certificate shall include at least the information set out in ANNEX VI: CONTENT OF A CERTIFICATE

2. The EUMSS certificate shall specify the service profile and the assurance level; the detailed scope and boundaries of the certified MSS shall be unambiguously specified in the EUMSS certificate or the certification report.

3. The Conformity Assessment Body shall provide the applicant with the EUMSS certificate at least in electronic form.

4. The Conformity Assessment Body shall produce a confidential certification assessment report in accordance with ANNEX VIII: CONTENT OF A CERTIFICATION ASSESSMENT REPORT for each EUMSS certificate it issues. The certification assessment report shall contain a detailed description of the evaluation activities performed, the specific criteria and methods used (including those referred to in CEN/CENELEC TS 18072), any dependency analysis of subservices, any consideration of existing evidence, and the detailed technical justification for the assigned assurance level.

5. Due to the highly sensitive nature of the operational and technical data contained within the certification assessment report, it shall be marked as confidential. The Conformity Assessment Body shall provide this report exclusively to the applicant and to the relevant national cybersecurity certification authority. It shall be protected and shall not be made publicly available.

6. The Conformity Assessment Body shall produce a public certification report in accordance with ANNEX VII: CONTENT OF A CERTIFICATION REPORT for each EUMSS certificate it issues. The certification report shall be derived from the certification assessment report but shall be appropriately sanitized to remove any proprietary, sensitive, or confidential operational information regarding the Managed Security Service. It shall provide a clear, high-level summary of the evaluation results suitable for public publication.

7. The Conformity Assessment Body shall provide the national cybersecurity certification authority and ENISA with every EUMSS certificate and every public certification report in electronic form, in order to facilitate ENISA's publication obligations under Article 50 of Regulation (EU) 2019/881 (Cybersecurity Act).

8. To enable ENISA to publish this information effectively in accordance with Article 50 of Regulation (EU) 2019/881 (Cybersecurity Act), the EUMSS certificate and the public certification report shall be provided to ENISA at least in English. Where the original documents are issued by the Conformity Assessment Body in another official language of the Union, an English translation shall also be provided without undue delay.

2.7 MARK AND LABEL

Explanatory note: A mark and label are defined for pointing to the ENISA certification web site. Although it can be used for all certificates issued under EUMSS, the mark and label are intended to be used mostly for providers of MSS, who may need the reference to market their service

1. The holder of a certificate may publish and use a mark and label of the certified Managed Security Service. Mark and label demonstrate that the Managed Security Service has been certified in accordance with this Scheme. Mark and label shall be exposed in accordance with this section and with ANNEX X: MARK AND LABELS.

2. The mark and label shall be issued strictly per service profile and per assurance level. Where a provider holds multiple EUMSS certificates for different service profiles, each profile shall be associated with its own distinct mark and label.

3. The mark and label shall be displayed in a visible, legible and unambiguous manner in connection with the certified Managed Security Service, including, where applicable:

(a) on the official website of the certificate holder describing the certified Managed Security Service;

(b) in service catalogues, datasheets or other service description material, whether in electronic or printed form;

(c) in contractual or pre-contractual documentation relating to the certified Managed Security Service.

4. The mark and label shall be set out as in ANNEX VI: CONTENT OF A CERTIFICATE and contain everything specified in ANNEX X: MARK AND LABELS.

5. The mark and label shall be accompanied by a QR code with a link to ENISA certification website containing at least:

(a) the information on the validity of the certificate;

(b) the necessary certification information as set out in ANNEXES CONTENT OF A CERTIFICATE and CONTENT OF A CERTIFICATION REPORT;

(c) the information to be made publicly available by the holder of the certificate in accordance with Article 55 of Regulation (EU) 2019/881 (Cybersecurity Act); and

(d) where applicable, the historic information related to the specific certification or certifications of the Managed Security Service to enable traceability.

6. The dedicated European cybersecurity certification website maintained by ENISA shall provide an aggregated portfolio view, presenting all active EUMSS certificates held by a given provider to facilitate verification by clients and procurement authorities.

2.8 PERIOD OF VALIDITY OF AN EUMSS CERTIFICATE

Explanatory note: While the European Cybersecurity Certification Framework generally permits certificates to have a validity period of up to 5 years (as seen in product-centric Schemes), the dynamic and operational nature of Managed Security Services necessitates a shorter lifecycle. To align with industry best practices for service management systems (such as ISO/IEC 27001, ISO/IEC 20000-1 and ISO 22301), this Scheme establishes a maximum validity of 3 years, which is strictly conditioned upon the execution of annual surveillance evaluations.

1. The Conformity Assessment Body shall set a period of validity for each EUMSS certificate issued, taking into account the characteristics and the risk profile of the certified Managed Security Service.

2. The period of validity of the EUMSS certificate shall not exceed 3 years.

3. The continued validity of the EUMSS certificate throughout this period shall be strictly subject to the successful completion of annual surveillance evaluations carried out by the Conformity Assessment Body. These evaluations shall be conducted in accordance with the surveillance schedule and procedures laid down in ANNEX IV: ASSURANCE CONTINUITY AND CERTIFICATION LIFECYCLE.

4. By derogation from paragraph 2, the period of validity may be temporarily extended for a strictly limited duration, subject to the prior approval of the national cybersecurity certification authority, solely to accommodate unforeseen delays in the recertification evaluation process. The national cybersecurity certification authority shall notify the European Cybersecurity Certification Group of any granted approval without undue delay.

2.9 REVIEW OF AN EUMSS CERTIFICATE

Explanatory note: In addition to maintenance activities related to changes in the provided EUMSS, regular conformity assessments are required in order to ensure that essential processes used in the provision of the MSS are effectively operated, and to ensure that the evolution of the threat landscape is adequately considered. A maintenance schedule is defined, and each maintenance conformity assessment may lead to the confirmation, withdrawal or update of the certificate.

1. Upon request of the holder of the certificate or for other justified reasons, the Conformity Assessment Body may decide to review the EUMSS certificate. The review shall be carried out in accordance with ANNEX IV: ASSURANCE CONTINUITY AND CERTIFICATION LIFECYCLE. The Conformity Assessment Body shall determine the extent of the review.

2.Following the results of the review, and where applicable of the re-evaluation, the Conformity Assessment Body shall:

(a) confirm the EUMSS certificate;

(b) withdraw the EUMSS certificate in accordance with section WITHDRAWAL OF AN EUMSS CERTIFICATE; or

(c) withdraw the EUMSS certificate in accordance with chapter WITHDRAWAL OF AN EUMSS CERTIFICATE and issue a new EUMSS certificate with a different scope as determined in the re-evaluation augmented in the certification report.

3. The Conformity Assessment Body may decide to suspend, without undue delay, the EUMSS certificate in accordance with section SUSPENSION OF THE EUMSS CERTIFICATE, pending remedial action by the holder of the EUMSS certificate.

2.10 WITHDRAWAL OF AN EUMSS CERTIFICATE

Explanatory note: The withdrawal of EUMSS certificates is a task assigned to the Conformity Assessment Body that issued the certificate, following an issue that cannot be corrected (vulnerability or nonconformity) or non-compliance from the holder of the certificate, or following instructions from the holder of the certificate or from the National Cybersecurity Certification Authority - NCCA

1. Without prejudice to Article 58(8), point (e), of Regulation (EU) 2019/881 (Cybersecurity Act), an EUMSS certificate shall be withdrawn by the Conformity Assessment Body that issued that certificate.

2. The Conformity Assessment Body referred to in requirement 1 shall notify the national cybersecurity certification authority of the withdrawal of the certificate. It shall also notify ENISA of such withdrawal in view of facilitating the performance of its task under Article 50 of Regulation (EU) 2019/881 (Cybersecurity Act). The national cybersecurity certification authority shall notify other relevant market surveillance authorities.

3. The holder of an EUMSS certificate may request the withdrawal of the certificate.

3 CHAPTER III: CONFORMITY ASSESSMENT BODIES

SECTION I: GENERAL REQUIREMENTS FOR CONFORMITY ASSESSMENT BODIES

3.1 ACCREDITATION OF CABS

Explanatory note: Because EUMSS is a service certification, the Conformity Assessment Body (CAB) shall be accredited under ISO/IEC 17065.

1. A CAB performing certification activities under this Scheme shall be accredited by a national accreditation body in accordance with standard EN ISO/IEC 17065 (Conformity assessment — Requirements for bodies certifying products, processes and services) and CEN/CENELEC TS 18072 – Requirements for conformity assessment bodies certifying ICT services.

2. The scope of the accreditation shall explicitly cover the certification of Managed Security Services as defined by the requirements of this Scheme and apply to specific service profiles, including the ability to adequately review evaluation reports, evaluate service processes, and the technical infrastructure used to deliver the service.

3. Where technical testing of IT systems is relevant, the National Accreditation Body shall ensure that the CAB's evaluation teams are complemented by technical experts who possess specific and proven competencies in:

    a) vulnerability assessment and the identification of vulnerabilities within IT service infrastructures;

    b) penetration testing or substitute evaluation activities with equivalent effect to technical penetration testing, such as physical security inspections, social engineering assessments, table-top exercises, and process simulations where the certified Managed Security Service relies heavily on procedural, manual, or physical activities.

    c) the examination of service architecture and secure configurations.

4. In addition to the requirements laid down in EN ISO/IEC 17065, the CAB shall meet the requirements set out in the Article 60 and the Annex of Regulation (EU) 2019/881 (Cybersecurity Act) and REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES.

3.2 ADDITIONAL OR SPECIFIC REQUIREMENTS FOR A CAB

Explanatory note: While the evaluation of a service at the 'high' assurance level legally requires an assessment of its resistance to skilled attackers, the Cybersecurity Act acknowledges this must be done "where relevant." For Managed Security Services that rely heavily on procedural, manual, or physical activities (such as certain Incident Response services) without a dedicated IT delivery platform, mandatory penetration testing may not be appropriate. In such cases, the CAB relies on substitute evaluation activities.

1. A CAB shall be authorised by a national cybersecurity certification authority to issue EUMSS certificates at assurance level 'high' where that body demonstrates that, in addition to meeting the requirements laid down in Article 60(1) of and the Annex to Regulation (EU) 2019/881 (Cybersecurity Act) regarding accreditation of conformity assessment bodies, the following:

(a) it has the expertise and competences required for the certification decision at assurance level 'high', including penetration testing of the IT systems and infrastructure used to provide the service where relevant to the assessment of the service, or substitute evaluation activities with equivalent effect to technical penetration testing, such as physical security inspections, social engineering assessments, table-top exercises, and process simulations where the certified Managed Security Service relies heavily on procedural, manual, or physical activities.

(b) it has the requisite competences and put in place appropriate technical and operational measures to effectively protect confidential and sensitive information for assurance level 'high', in addition to the requirements set out in section PROTECTION OF INFORMATION.

2. The national cybersecurity certification authority shall assess whether a CAB fulfils all the requirements set out in paragraph 1. That assessment shall include at least structured interviews and a review of at least one pilot certification at level high performed by the CAB in accordance with this Scheme if this is the initial authorisation, or at least one ordinary certification at level high performed under the previous authorisation, if this is a reauthorisation.

3. Where the evaluation of a Managed Security Service at the assurance level 'high' requires vulnerability analysis and penetration testing pursuant to Article 52(7) of Regulation (EU) 2019/881 (Cybersecurity Act), such testing shall be understood as the penetration testing of the IT systems and infrastructure used to provide the service, not the full provider IT systems and infrastructure. However, such penetration testing shall only be conducted where relevant to the nature of the service. Where the Managed Security Service relies exclusively on physical, manual, or procedural activities and lacks a dedicated IT delivery platform, substitute evaluation activities with equivalent effect (such as process simulations, table-top exercises, or physical security inspections) shall be undertaken and the Conformity Assessment Bodies shall demonstrate its expertise and competence to do so.

4. In its assessment, the national cybersecurity certification authority may reuse any appropriate evidence from prior authorisation or similar activities granted pursuant to:[6]

(a) this Scheme;

(b) another European Cybersecurity Certification Scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881 (Cybersecurity Act);

[6] In future versions of the scheme reuse of evidence of other Non-Eu Schemes or private schemes may be accepted under strict conditions.

(c) a national Scheme referred to in section NATIONAL SCHEMES COVERED BY THE EUMSSNATIONAL SCHEMES COVERED BY THE EUMSS of this Scheme.

5. The national cybersecurity certification authority shall produce an authorisation report which is subject to peer review in accordance with Article 59(3), point (d), of Regulation (EU) 2019/881 (Cybersecurity Act).

6. The national cybersecurity certification authority shall specify the Managed Security service profiles to which the authorisation extends. The authorisation shall be valid for a period no longer than the validity of the accreditation. It may be renewed upon request provided that the Conformity Assessment Body still meets the requirements set out in this section. For the renewal of the authorisation, no pilot evaluations are required.

7. The national cybersecurity certification authority shall withdraw the authorisation of the Conformity Assessment Bodies where it no longer meets the conditions set out in this section. Upon withdrawal of the authorisation, the Conformity Assessment Bodies shall immediately cease promoting itself as an authorised Conformity Assessment Bodies.

4 CHAPTER IV: MONITORING, NON-CONFORMITY AND NON-COMPLIANCE

SECTION I: COMPLIANCE MONITORING

4.1 MONITORING ACTIVITIES BY THE NATIONAL CYBERSECURITY CERTIFICATION AUTHORITY

Explanatory note: As required in Article 58(7) of (EU) 2019/881, NCCAs have an important role in the compliance monitoring of all certified services and also of certificate holders and certification bodies. Their activities include specific reviews of a sample of certificates, which may here be limited to partial reviews focusing on specific topics, because of the limited number of certificates. The operating rules are expected to be further defined by the dedicated maintenance subgroup of the ECCG . Because Managed Security Services are routinely delivered across borders, this article explicitly defines the proactive oversight jurisdiction to avoid duplication or gaps: the NCCA of the Member State where the issuing Conformity Assessment Bodies is established holds primary responsibility for monitoring that specific certificate. Activities include specific reviews of a sample of certificates, and cooperation with other Member States where an investigation reveals cross-border impacts.

1. Without prejudice to Article 58(7) of Regulation (EU) 2019/881 (Cybersecurity Act), the national cybersecurity certification authority shall monitor the compliance of:

(a) the Conformity Assessment Body with their obligations pursuant to this Scheme and article 60 and the Annex of Regulation (EU) 2019/881 (Cybersecurity Act);

(b) the holders of an EUMSS certificate with their obligations pursuant to this Scheme and Regulation (EU) 2019/881 (Cybersecurity Act);

(c) the certified Managed Security Service with the requirements set out in the EUMSS;

(d) the assurance expressed in the EUMSS certificate addressing the evolving threat landscape.

2. Where a holder of an EUMSS certificate delivers the certified Managed Security Service across multiple Member States, the national cybersecurity certification authority responsible for the monitoring and oversight of that certified service shall be the authority of the Member State in which the Conformity Assessment Body that issued the EUMSS certificate is established.

3. The national cybersecurity certification authority shall perform its monitoring activities in particular on the basis of:

(a) information coming from certification bodies, national accreditation bodies and relevant market surveillance authorities;

(b) information resulting from its own or another authority's assessments and investigations;

(c) sampling, carried out in accordance with paragraph 4;

(d) complaints received.

4. The national cybersecurity certification authority shall, in cooperation with other market surveillance authorities, sample annually a number of EUMSS certificates as determined by a risk assessment. Upon request and acting on behalf of the competent national cybersecurity certification authority, certification bodies shall assist that authority in monitoring compliance.

5. The national cybersecurity certification authority shall select the sample of Managed Security Services to be checked using objective criteria, including:

(a) service profile;

(b) assurance levels of the service;

(c) holder of a certificate;

(d) Conformity Assessment Body;

(e) any other information brought to the authority's attention.

6. The national cybersecurity certification authority shall inform the affected holders of the EUMSS certificate about the selection criteria.

7. The Conformity Assessment Body that certified the sampled Managed Security Service shall, upon request of the national cybersecurity certification authority, conduct additional review in accordance with the procedure laid down in Section ANNUAL SURVEILLANCE EVALUATIONS and inform the national cybersecurity certification authority of the results.

8. Where the national cybersecurity certification authority has sufficient reason to believe that a certified Managed Security Service is no longer in compliance with this Scheme or Regulation (EU) 2019/881 (Cybersecurity Act), it may carry out investigations or make use of any other monitoring powers set out in Article 58(8) of Regulation (EU) 2019/881 (Cybersecurity Act).

9. The national cybersecurity certification authority shall inform the Conformity Assessment Body concerned about ongoing investigations regarding selected Managed Security Services.

10. Where the national cybersecurity certification authority identifies that an ongoing investigation concern Managed Security Services that are certified by certification bodies established in other Member States, it shall inform thereof the national cybersecurity certification authorities of the relevant Member States in order to collaborate in the investigations, where relevant. Such national cybersecurity certification authority shall also notify the European Cybersecurity Certification Group of the cross-border investigations and the subsequent results.

4.2 MONITORING ACTIVITIES BY THE CAB

Explanatory note: The Conformity Assessment Body is also in charge of performing compliance monitoring activities on certified services and certificate holders, as foreseen in standard EN ISO/IEC 17065 and TS 18072

1. The Conformity Assessment Body shall monitor:

(a) the compliance of the holders of a certificate with their obligations under this Scheme and Regulation (EU) 2019/881 (Cybersecurity Act) towards the EUMSS certificate that was issued by the Conformity Assessment Body;

(b) the compliance of the Managed Security Service it has certified with their respective security requirements;

(c) the assurance expressed in the certificate.

2. The Conformity Assessment Body shall undertake its monitoring activities on the basis of:

(a) the information provided on the basis of the commitments of the applicant for certification referred to in section CONDITIONS FOR ISSUANCE OF AN EUMSS CERTIFICATE;

(b) information resulting from activities of other relevant market surveillance authorities;

(c) complaints received;

(d) vulnerability information that could impact the Managed Security Service it has certified.

3. The national cybersecurity certification authority may draw up rules for a periodical physical dialogue between certification bodies and holders of EUMSS certificates to verify and report on compliance with the commitments made pursuant section CONDITIONS FOR ISSUANCE OF AN EUMSS CERTIFICATE, without prejudice to activities related to other relevant market surveillance authorities.

4.3 MONITORING ACTIVITIES BY THE HOLDER OF THE CERTIFICATE

Explanatory note: This section establishes the active monitoring obligations necessary to ensure the continuous conformity of the certified Managed Security Service. Furthermore, to protect the integrity of the certification, the holder is mandated to notify the Conformity Assessment Body without undue delay in the event of any actual breach, compromise, or material change affecting the certified Managed Security Service itself.

1. The holder of an EUMSS certificate shall perform the following tasks to monitor the conformity of the Managed Security Service with its security requirements:

(a) monitor vulnerability information regarding the certified Managed Security Services, including known dependencies and shall include the below:

(1) a publication or a submission regarding vulnerability information by a user or security researcher referred to in Article 55(1), point (c) of Regulation (EU) 2019/881 (Cybersecurity Act);

(2) a submission by any other source;

(b) monitor the assurance expressed in the EUMSS certificate, and in particular the evolution of the status of any certificate, audit report, or assurance information used as objective evidence in the evaluation of the Managed Security Service.

2. The holder of an EUMSS certificate shall work in cooperation with the Conformity Assessment Body and where applicable, the national cybersecurity certification authority to support their monitoring activities.

3. The holder of an EUMSS certificate shall notify the Conformity Assessment Body without undue delay when the following events occur:

(a) any breach or compromise of the Managed Security Service that affects the certification;

(b) any material changes to the Managed Security Service that affect the scope of certification.

SECTION II: CONFORMITY AND COMPLIANCE

4.4 CONSEQUENCES OF NONCONFORMITY OF A CERTIFIED MSS

Explanatory note: The management of nonconformities is centred around the Conformity Assessment Body, which decides on the actions to be performed, starting by a notification of the certificate holder and a request for a remediation plan. Depending on the severity of the nonconformity, the Conformity Assessment Body may also notify the NCCA. The Conformity Assessment Body may also decide to suspend the certificate

1. Where a Managed Security Service does not conform with the requirements laid down in this Scheme and in Regulation (EU) 2019/881 (Cybersecurity Act), the Conformity Assessment Body shall inform the holder of the EUMSS certificate about the identified non-conformity and request remedial actions.

2. Where an instance of non-conformity with the requirements of this Scheme might affect compliance with other relevant Union legislation, which provides for the possibility to demonstrate the presumption of conformity with the requirements of that legal act by using the EUMSS certificate, the Conformity Assessment Body shall inform the national cybersecurity certification authority without delay. The national cybersecurity certification authority shall immediately notify the relevant[7] market surveillance authority responsible for such other relevant Union regulation about the instance of non-conformity identified.

3. Where a Conformity Assessment Body identifies a material non-conformity within the baseline requirements of the Horizontal Layer (ANNEX II) during the evaluation or surveillance of a specific service profile, that Conformity Assessment Body shall, without undue delay, notify the national cybersecurity certification authority with general information about the non-conformity.

To identify whether the provider holds other active EUMSS certificates that may be affected, the national cybersecurity certification authority shall consult the dedicated European cybersecurity certification website maintained by ENISA pursuant to Article 50 of Regulation (EU) 2019/881 (Cybersecurity Act).

Where other affected EUMSS certificates are identified:

a) If the issuing certification bodies are established in the same Member State, the national cybersecurity certification authority shall notify them directly.

b) If the issuing certification bodies are established in other Member States, the national cybersecurity certification authority shall inform the national cybersecurity certification authorities of those relevant Member States without undue delay. Those notified authorities shall subsequently notify the respective certification bodies established in their territory.

The notified certification bodies shall independently contact the responsible CAB (see 3. above) to request the details of the non-conformity and then determine whether the identified horizontal non-conformity materially impacts the certification status of their respective service profiles.

4. Upon receipt of the information referred to in paragraph 1, the holder of the EUMSS certificate shall within the time period set by the Conformity Assessment Body, which shall not exceed 30 calendar

[7] To be determined for MSS

days, propose to the Conformity Assessment Body the remedial action necessary to address the non-conformity. Upon receipt of the action plan, it shall review if the time frame used for remedial is appropriate to the extent of the non-conformity.

5. The Conformity Assessment Body may suspend, without undue delay, the EUMSS certificate in accordance with section SUSPENSION OF THE EUMSS CERTIFICATE if the material non-conformity has significant effect on the service, or where the holder of the EUMSS certificate does not duly cooperate with the Conformity Assessment Body.

6. Upon remedial, the Conformity Assessment Body shall carry out a review in accordance with chapter REVIEW OF AN EUMSS CERTIFICATE assessing whether the remedial action addresses the non-conformity.

7. Where the holder of the EUMSS certificate does not propose appropriate remedial action during the period referred to in paragraph 3, the certificate shall be suspended in accordance with section SUSPENSION OF THE EUMSS CERTIFICATE SUSPENSION OF THE EUMSS CERTIFICATE or withdrawn in accordance with section WITHDRAWAL OF AN EUMSS CERTIFICATE.

8. This Chapter shall not apply to cases of vulnerabilities affecting a certified Managed Security Service, which shall be handled in accordance with CHAPTER V: VULNERABILITY MANAGEMENT AND DISCLOSURE.

4.5 CONSEQUENCES OF NON-COMPLIANCE OF THE HOLDER OF THE CERTIFICATE

Explanatory note: When the holder of a certificate does not comply to its obligations, especially those related to monitoring and maintaining the certified service at the proper assurance level, the consequences may be more significant, with a strict delay to get in compliance, and a possibility of subsequent suspension or withdrawal of the certificate, at the discretion of the Conformity Assessment Body.
Indeed, some of the Scheme's requirements apply to the service provider itself, such as the obligation to provide complete and truthful information or to properly handle vulnerabilities. When a service provider does not comply to these requirements, they expose themselves to direct consequences.
The terms of the Article are stronger than those on the previous Article, because non-compliance (a direct failure to apply well-defined rules) is considered more significant than a nonconformity. Suspensions and withdrawal are more likely to be used, and the various authorities are notified of the issue

1. Where the Conformity Assessment Body finds that:

(a) the holder of the EUMSS certificate or the applicant for certification is not compliant with its commitments and obligations as set out in section CONDITIONS FOR ISSUANCE OF AN EUMSS CERTIFICATE.

or

(b) the holder of the EUMSS certificate does not comply with Article 56(8) of Regulation (EU) 2019/881 (Cybersecurity Act) or Chapter VI of this Scheme;

it shall set a time period of not more than 30 calendar days within which the holder of the EUMSS certificate shall take remedial action.

2. Where the holder of the EUMSS certificate does not propose appropriate remedial action during the time period referred to in paragraph 1, the certificate shall be suspended in accordance with section SUSPENSION OF THE EUMSS CERTIFICATE or withdrawn in accordance with section WITHDRAWAL OF AN EUMSS CERTIFICATE.

3. Continued or recurring infringement by the holder of the EUMSS certificate of the obligations referred to in paragraph 1 shall trigger the withdrawal of the EUMSS certificate in accordance with section WITHDRAWAL OF AN EUMSS CERTIFICATE.

4. The Conformity Assessment Body shall inform the national cybersecurity certification authority of the findings referred to in paragraph 1. This national Conformity Assessment Body shall then initiate the procedure laid out in CONSEQUENCES OF NONCONFORMITY OF A CERTIFIED MSS to inform market authorities and possibly further affected CABs.

4.6 SUSPENSION OF THE EUMSS CERTIFICATE

Explanatory note: A certificate may be suspended because of a nonconformity or vulnerability in the certified service, or because of non-compliance from the certificate holder, when the Conformity Assessment Body believes that the issue can be addressed by the certificate holder in a timely manner. A suspended certificate remains valid, but it is an indication to users to be careful with this service, and the suspension is always accompanied by guidance for the users of the service whose certificate is suspended.
The suspension of a certificate is an intermediary step before the more radical withdrawal of a certificate. It is particularly useful in the context of a Regulation that makes certification a legal requirement.
However, suspension is often misunderstood. A suspended certificate remains valid, but it becomes publicly known that it is facing some issues, which may lead to trust issues. For this reason, this Article requires specific information of users, containing at least some recommendations for the continued use of the service in acceptable security conditions.

1. Where this Scheme refers to suspension of an EUMSS certificate, the Conformity Assessment Body shall suspend an EUMSS certificate concerned for a period appropriate to the circumstances triggering suspension. The suspension period shall begin on the day following the day of the decision of the Conformity Assessment Body. The suspension shall not affect the validity of the certificate.

2. The Conformity Assessment Body shall notify the holder of the certificate and the national cybersecurity certification authority of the suspension without undue delay and shall provide the reasons for the suspension, the requested actions to be taken and the suspension period.

3. Certification holders shall notify the clients of the Managed Security Service concerned about the suspension and the reasons provided by the Conformity Assessment Body for the suspension, except those parts of the reasons the sharing of which would constitute a security risk or which contain sensitive information. This information shall also be made publicly available by the holder of the certificate.

4. Where other relevant Union legislation provides for a presumption of conformity based on certificates issued under the requirements of this Scheme, the national cybersecurity certification authority shall inform the market surveillance authority responsible for such other relevant Union legislation about the suspension.

5. The suspension of a certificate shall be notified to ENISA in accordance with INFORMATION MADE AVAILABLE BY ENISA.

6. In duly justified cases, the national cybersecurity certification authority may authorise an extension of the period of suspension of an EUMSS certificate. The total period of suspension may not exceed 1 year.

7. After established time limit for suspension of the certificate is expired, if the MSSP has not yet solved the nonconformities identified by the CAB, the EUMSS certificate will be Withdraw in accordance with WITHDRAWAL OF AN EUMSS CERTIFICATE.

4.7 CONSEQUENCES OF NON-COMPLIANCE BY THE CAB

Explanatory note: Non-compliance by the Conformity Assessment Body of course may impact its accreditation, authorisation and notification, and it may as well impact certificates issued by that Conformity Assessment Body, if it is found that the operation of the Conformity Assessment Body when issuing a certificate was inadequate and casts doubts on the validity of the certificate. The NCCA may organise a review of impacted certificates by another Conformity Assessment Body, and if issues are identified, require some conformity assessment activities to be performed again.

1. In case of non-compliance by a Conformity Assessment Body with its obligations, the national cybersecurity certification authority shall, without undue delay:

(a) identify, the potentially affected EUMSS certificates;

(b) where necessary, request evaluation activities to be performed on one or more Managed Security Services by any other accredited and where applicable authorised Conformity Assessment Bodies that may be in a better technical position to support that identification;

(c) analyse the impacts of non-compliance;

(d) notify the holder of the EUMSS certificate affected by non-compliance.

2. On the basis of the measures referred to in paragraph 1, the Conformity Assessment Body shall adopt either of the following decisions with respect to each affected EUMSS certificate:

(a) maintain the EUMSS certificate unaltered;

(b) withdraw the EUMSS certificate in accordance with section WITHDRAWAL OF AN EUMSS CERTIFICATE and, where appropriate, issue a new EUMSS certificate.

3. On the basis of the measures referred to in paragraph 1, the national cybersecurity certification authority shall:

(a) report the non-compliance of the Conformity Assessment Body to the national accreditation body;

(b) where applicable, assess the potential impact on the authorisation.

5 CHAPTER V: VULNERABILITY MANAGEMENT AND DISCLOSURE

SECTION I: VULNERABILITY MANAGEMENT

5.1 VULNERABILITY MANAGEMENT PROCEDURES

Explanatory note: Since Managed Security Services operate in highly dynamic environments that may rely on IT platforms, human expertise, physical facilities, or purely procedural workflows, the concept of a "vulnerability" is broadened. The provider is required to manage vulnerabilities across all domains—including using process simulations and physical inspections as the equivalent of "penetration testing" for non-IT assets. Rules are established for managing these vulnerabilities, including conditional technical requirements like Software Bill of Materials (SBOMs) for IT components, and disclosing them safely.

1. The holder of an EUMSS certificate shall establish, maintain, and operate vulnerability management procedures in accordance with the rules laid down in this chapter and, where necessary, supplemented by the procedures set out in EN ISO/IEC 30111.

2. Where the delivery of the certified Managed Security Service relies on specific ICT systems, service platforms, sensors, or software tools, the vulnerability management procedures for those relevant components shall additionally include:

(a) the maintenance of an SBOM in a commonly used machine-readable format for components over which the certificate holder has sufficient visibility;

(b) for commercial off-the-shelf products, proprietary appliances, or externally managed services for which the certificate holder cannot produce or obtain an SBOM, documented procedures to request, obtain, or otherwise track equivalent vulnerability information from the manufacturer, vendor, or service provider, including security advisories, patch notifications, and end-of-support information;

(c) procedures for timely remediation of vulnerabilities, whether by the certificate holder or by documented monitoring and verification of third-party remediation;

(d) a documented risk-based treatment process for cases where an SBOM or timely remediation is not available.

3. To proactively identify vulnerabilities, the certificate holder shall continuously monitor its service delivery model. The extent and frequency of monitoring and testing activities shall be commensurate with the assurance level and the nature of the service. This monitoring shall include a range of security tests appropriate to the nature of the service, such as technical vulnerability assessments, cyber-attack simulations, red teaming, and cyber response exercises, validation of digital evidence preservation during incident scenarios, included Chain of Custody.

4. Where the certified Managed Security Service relies heavily on procedural, manual, or physical activities rather than solely on an IT delivery platform, the identification of vulnerabilities shall

encompass the regular testing of these non-technical elements. For assurance levels basic and substantial, such testing may include activities such as table-top exercises, process walkthroughs, and selected physical or procedural checks performed on a risk-based basis.

To evaluate the resistance of these elements to skilled attackers at assurance level high, the certificate holder shall conduct substitute evaluation activities with equivalent effect to technical penetration testing, such as physical security inspections, social engineering assessments, table-top exercises, and process simulations.

5. The holder of an EUMSS certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their Managed Security Services from external sources, including users, certification bodies, security researchers and relevant databases such as EU Vulnerability Database[8]

6. Where a holder of an EUMSS certificate detects or receives information about a potential vulnerability—whether a software flaw in its IT infrastructure, a weakness in its physical security perimeters, or a critical gap in its operational processes and playbooks —affecting the certified Managed Security Service, it shall record it and carry out a vulnerability impact analysis without undue delay.

7. In response to a reasonable request by the Conformity Assessment Body that issued the certificate, the holder of an EUMSS certificate shall transmit all relevant information about potential vulnerabilities to that Conformity Assessment Body.

[8] Home | EUVD

5.2 VULNERABILITY IMPACT ANALYSIS AND REPORTING

Explanatory note: Because Managed Security Services (MSS) can be purely procedural, physical, or highly technical, a "vulnerability" is broadly defined to include software flaws, physical weaknesses, or critical gaps in operational playbooks. Crucially, this section introduces a reporting guidelines: routine vulnerabilities are handled internally by the provider and audited annually, whereas vulnerabilities that have a "likely impact on conformity" must be immediately reported to the Conformity Assessment Body.

1. The vulnerability impact analysis shall determine the exploitability and criticality of the identified vulnerability. This analysis shall take into account:

    (a) known threat information and the relevant threat environment;

    (b) the potential impact on the confidentiality, integrity, and availability of the certified service;

    (c) the potential impact on the clients utilising the certified service.

    d) Potential impact on evidentiary integrity (e.g. corruption or loss of digital evidence)

2. To ensure agile service delivery without overwhelming the Conformity Assessment Body with routine operational data, the certificate holder shall produce and transmit a vulnerability impact analysis report to the Conformity Assessment Body without undue delay only where the impact analysis determines that the vulnerability has a likely impact on the conformity of the service with the assurance expressed in the EUMSS certificate.

3. For vulnerabilities (whether technical, physical, or procedural) that the initial impact analysis determines do not have a likely impact on the conformity of the certified service, the certificate holder shall manage them internally in accordance with its standard vulnerability management procedures. The effectiveness of these internal procedures, and the justification for classifying such vulnerabilities as not impacting conformity, shall be evaluated by the Conformity Assessment Body during the annual surveillance evaluations.

5.3 VULNERABILITY IMPACT ANALYSIS REPORT

Explanatory note: This section specifies the mandatory content and handling procedures for the vulnerability impact analysis report. Crucially for Managed Security Services, it requires the provider to document not only software flaws, but also physical or procedural vulnerabilities. Because this report may contain sensitive details about how a service could be exploited, it imposes strict confidentiality requirements on its distribution.

1. The holder of an EUMSS certificate shall produce a vulnerability impact analysis report where the impact analysis shows that the vulnerability has a likely impact on the conformity of the Managed Security Service with the assurance expressed in the EUMSS certificate.

2. The vulnerability impact analysis report shall contain an assessment of the following elements:

a) a description of the vulnerability and its origin, specifying whether it affects the IT infrastructure, physical security perimeters, or operational processes;

b) the affected components, tools, physical sites, third-party dependencies, or procedural workflows of the certified Managed Security Service;

c) an assessment of the potential impact on the confidentiality, integrity, and availability of the Managed Security Service and the potential impact on its clients;

d) an assessment of the likelihood of exploitation, taking into account the relevant threat environment, the skills and resources required by an attacker, and the operational context;

e) the proposed remediation or mitigation measures, where applicable.

3. The vulnerability impact analysis report shall, where applicable, contain details about the possible means of exploitation of the vulnerability. Information pertaining to the possible means of exploitation shall be handled in accordance with appropriate security measures to protect its confidentiality and ensure, where necessary, it's strictly limited distribution.

4. The holder of an EUMSS certificate shall transmit the vulnerability impact analysis report to the Conformity Assessment Body without undue delay.

5. In cases where the vulnerability is assessed as not having a likely impact on the conformity of the certified Managed Security Service, the vulnerability impact analysis report shall explicitly justify the reasoning supporting the conclusion that the vulnerability remains within the accepted risk level and that no special evaluation, suspension, or withdrawal of the EUMSS certificate is required.

6. Where the vulnerability impact analysis report determines that the vulnerability has a likely impact on the conformity of the certified Managed Security Service and that it can be remedied, the requirements regarding VULNERABILITY REMEDIATION shall apply.

7. Where the vulnerability impact analysis report determines that the vulnerability has a likely impact on the conformity of the certified Managed Security Service and that it cannot be remedied, the EUMSS certificate shall be withdrawn.

8. The holder of the EUMSS certificate shall document and monitor any residual vulnerabilities to ensure that they cannot be exploited in case of changes in the operational environment. These

residual vulnerabilities shall be reviewed by the Conformity Assessment Body during the annual surveillance evaluations.

5.4 VULNERABILITY REMEDIATION

Explanatory note: Recognizing the dynamic nature of Managed Security Services, immediate action is required in case of a vulnerability with likely service impact. In such cases, the provider must implement immediate mitigation or full remediation measures—whether that involves deploying an IT patch, updating a procedural playbook, or reinforcing physical access controls. The Conformity Assessment Body's role is to subsequently validate the effectiveness of the actions taken, ensuring the service returns to full conformity.

1. Where the vulnerability impact analysis report determines that a vulnerability has a likely impact on the conformity of the certified Managed Security Service, the holder of the EUMSS certificate shall design and implement mitigation measures, compensating controls or full remediation measures without undue delay to ensure the security of the service and its clients. These measures shall address the specific nature of the vulnerability, whether it resides within the IT infrastructure, physical security perimeters, or operational processes and workflows.

2. The holder of the EUMSS certificate shall submit a comprehensive remediation report to the Conformity Assessment Body. This report shall detail the exact remedial actions already taken which may include, but are not limited to, applying security updates, modifying procedural playbooks, implementing new administrative controls, conducting staff retraining, upgrading physical security safeguards or applying compensating controls. In cases where full remediation requires a longer timeframe, the report shall detail the immediate compensatory mitigations applied alongside a defined timeline for the complete resolution of the vulnerability.

3. The Conformity Assessment Body shall carry out an assessment to validate whether the implemented remediation effectively addresses the vulnerability and restores the service's conformity. Depending on the severity and the nature of the vulnerability (technical, physical, or procedural), the Conformity Assessment Body may conduct a special evaluation. To verify the operating effectiveness of the remedial action, this special evaluation may include targeted technical penetration testing, or, where the service relies on non-technical elements, substitute evaluation activities with equivalent effect such as process simulations, table-top exercises, or physical infrastructure inspections.

4. Where the vulnerability cannot be remedied, or where the certificate holder fails to implement effective remediation measures within the appropriate timeframe, the Conformity Assessment Body shall withdraw the EUMSS certificate.

SECTION II: VULNERABILITY DISCLOSURE AND NOTIFICATION

5.5 COORDINATED VULNERABILITY DISCLOSURE

Explanatory note: As the present Scheme requires notification of some stakeholders very early after the discovery of a vulnerability, possibly before its remediating, Scheme users, including clients of the certified service, may have to participate in the remediation. This mandates clearly defined and coordinated policy for vulnerability disclosure of the MSS.

1. The holder of an EUMSS certificate shall establish, maintain, and operate a coordinated vulnerability disclosure policy and related procedures, supplemented by the procedures set out in EN ISO/IEC 29147 where necessary, and shall make this policy publicly available.

2. The coordinated vulnerability disclosure policy shall ensure that the client of the certified service is informed of a potentially impactful vulnerability before it is made public, allowing them to apply the recommended measures before the vulnerability becomes known to the general public, notwithstanding any national legal provisions regarding coordinated vulnerability disclosure.

5.6 INFORMATION SHARED WITH THE NATIONAL CYBERSECURITY CERTIFICATION AUTHORITY

Explanatory note: The coordinated vulnerability disclosure policy needs to mention the NCCA, who may then decide to further share the information with other NCCAs

1. The information provided by the Conformity Assessment Body to the national cybersecurity certification authority regarding material vulnerabilities or incidents shall include all elements necessary to understand the impact on the Managed Security Service.

2. The information provided shall not contain details of the exact means of exploitation of the vulnerability, in order to protect the integrity and security of the service provider's operational infrastructure.

3. The national cybersecurity certification authority shall share the relevant information received with other national cybersecurity certification authorities and ENISA.

5.7 PUBLICATION OF THE VULNERABILITY

Explanatory note: While standard software or hardware flaws must be registered in the European Vulnerability Database, Managed Security Services can also suffer from procedural, manual, or physical vulnerabilities. Because these do not fit standard CVE tracking, this section gives providers the flexibility to publish such service-specific vulnerabilities in other public repositories or through their own security advisories.

1. Upon withdrawal of a certificate, or where appropriate upon remediation of a material vulnerability, the holder of the EUMSS certificate shall disclose and register any publicly known and remediated vulnerability affecting the certified Managed Security Service.

2. Where the vulnerability relates to technical ICT products, software, or IT delivery components, and where it is technically feasible, such vulnerabilities shall be registered in the European Vulnerability Database[9] established pursuant to Article 12 of Directive (EU) 2022/2555.

3. Where registration in the European vulnerability database is not appropriate due to the procedural, physical, or bespoke operational nature of the vulnerability, the vulnerability shall be disclosed through other publicly accessible vulnerability repositories, or the provider's own public security advisories, as referred to in Article 55(1), point (d), of Regulation (EU) 2019/881 (Cybersecurity Act).

[9] Home | EUVD

6 CHAPTER VI: RETENTION, DISCLOSURE AND PROTECTION OF INFORMATION

6.1 RETENTION OF RECORDS BY CERTIFICATION BODIES

Explanatory note: Certification bodies keep the information about certificates for five years after their withdrawal, and if applicable, after the withdrawal of certificates that extend this certificate.

1. The certification bodies shall maintain a record system, which shall contain all documents produced in connection with each evaluation and certification they perform.

2. Certification bodies shall store the records in a secure manner and shall keep those records for the period necessary for the purposes of this Scheme and for at least 5 years after the expiry or the withdrawal of the relevant EUMSS certificate. When the Conformity Assessment Body has issued a new EUMSS certificate in accordance with the section REVIEW OF AN EUMSS CERTIFICATE, it shall retain the documentation of the withdrawn EUMSS certificate together with and as long as for the new EUMSS certificate.

6.2 INFORMATION MADE AVAILABLE BY THE HOLDER OF THE CERTIFICATE

Explanatory note: In addition to maintaining publicly available information, the certificate holder needs to keep all the information provided to the Conformity Assessment Body in the context of the evaluation for at least 5 years after the withdrawal of the certificate.
If applicable, after the withdrawal of the certificates that extend this certificate.

1. The information referred to in Article 55 of Regulation (EU) 2019/881 (Cybersecurity Act) shall be available in a language that can be easily accessible to users.

2. The holder of an EUMSS certificate shall store the information provided to the Conformity Assessment Body during the certification process securely for the period necessary for the purposes of this Scheme and for at least 5 years after the expiry or withdrawal of the relevant EUMSS certificate.

3. When the Conformity Assessment Body has issued a new EUMSS certificate in accordance with the section REVIEW OF AN EUMSS CERTIFICATE the holder shall retain the documentation of the withdrawn EUMSS certificate together with and as long as for the new EUMSS certificate.

4. Upon request by the Conformity Assessment Body or the national cybersecurity certification authority, the holder of an EUMSS certificate shall make available the records and copies referred to in paragraph 2.

6.3 INFORMATION MADE AVAILABLE BY ENISA

Explanatory note: According to Article 50(1) of Regulation (EU) 2019/881 (Cybersecurity Act), ENISA maintains a certification web site that lists all relevant and publicly available information about the EUMSS Scheme, which needs to be available at least in English. In support of this activity, all stakeholders need to inform ENISA without delay of all decisions that affect the content and status of EUMSS certificates

1. ENISA shall publish the following information on the website referred to in Article 50(1) of Regulation (EU) 2019/881 (Cybersecurity Act)[10]:

(a) all EUMSS certificates;

(b) the information on the status of an EUMSS certificate, notably whether it is in force, suspended, withdrawn, or expired;

(c) certification reports corresponding to each EUMSS certificate;

(d) a list of accredited conformity assessment bodies;

(e) a list of authorised conformity assessment bodies;

(f) the opinions of the European Cybersecurity Certification Group referred to in Article 62(4), point (c), of Regulation (EU) 2019/881 (Cybersecurity Act);

(g) peer assessment reports issued in accordance with ANNEX VII: CONTENT OF A CERTIFICATION REPORT.

2. The information referred to in paragraph 1 shall be made available at least in English.

3. Certification bodies and, where applicable, national cybersecurity certification authorities shall inform ENISA without delay about their decisions which affect the content or the status of an EUMSS certificate referred to in paragraph 1, point (b).

4. ENISA shall ensure that the information is published in accordance with paragraph 1 points (a), (b) and (c), clearly identifies Service profile of the EUMSS certificate.

[10] Homepage - European Union Cybersecurity Certification - European Union

6.4 PROTECTION OF INFORMATION

Explanatory note: This section establishes the rules for protecting sensitive information gathered during the certification process. Unlike standard ICT product evaluations, Managed Security Service (MSS) evaluations require the conformity assessment body to review highly sensitive operational artifacts to prove "operating effectiveness", such as historical incident case files, live service logs, client Service Agreement, and proprietary response playbooks. To protect the MSS provider's trade secrets and their clients' confidentiality, this chapter introduces specific safeguards beyond the standard baseline. Strict purpose limitation, requires the anonymisation or pseudonymisation of client-identifying data before evidence is shared, and enforces a restricted, need-to-know handling procedure for any discovered actionable vulnerabilities.

1. Conformity assessment bodies, national cybersecurity certification authorities, ECCG, ENISA, the Commission, and all other parties shall ensure the security and protection of business secrets and other confidential information, including trade secrets, as well as preserving intellectual property rights, and take the necessary and appropriate technical and organisational measures.

2. Information, records, and evidence received or generated by conformity assessment bodies and national cybersecurity certification authorities pursuant to this Scheme shall be used exclusively for the purpose of conducting conformity assessments, issuing certificates, and performing compliance monitoring and supervision.

3. Due to the operational nature of Managed Security Services, evaluation activities may require the review of historical incident case files, service logs, or operational playbooks depending on contractual limitations the MSSP has in place and ensuring the correct anonymization of the data. To protect the confidentiality of the certificate holder’s clients, the certificate holder shall, to the greatest extent possible, strictly anonymise or pseudonymise client-identifying data before sharing evidence with the conformity assessment body. Conformity assessment bodies may not extract, store, or retain unredacted sensitive client data in their record systems.

4. Any documentation containing detailed, actionable information on unpatched vulnerabilities, exploit mechanisms, or critical operational weaknesses of the Managed Security Service—including the confidential certification assessment report and vulnerability impact analysis reports—shall be classified appropriately. It shall be distributed in a restricted manner on a strict need-to-know basis exclusively to the relevant national cybersecurity certification authority and the conformity assessment body, and shall be exempt from public disclosure.

7 CHAPTER VII: RECOGNITION AGREEMENTS WITH THIRD COUNTRIES

7.1 CONDITIONS FOR A RECOGNITION AGREEMENT

Explanatory note: TBD

8 CHAPTER VIII: PEER ASSESSMENT OF CABs

8.1 PEER ASSESSMENT PROCEDURE

Explanatory note: Because EUMSS certificates may be issued at assurance level 'high', a peer assessment procedure needs to be established between the certification bodies that issue EUMSS certificates at that level high.

1. A Conformity Assessment Body issuing EUMSS certificates at assurance level 'high' shall undergo a peer assessment on a regular basis and at least every 5 years. The different types of peer assessment are listed in Annex VI. Additional types of peer assessment may be introduced through the update process UPDATE OF THE SCHEME.

2. The European Cybersecurity Certification Group shall draw up and maintain a schedule of peer assessments ensuring that such periodicity is respected. Except in duly justified cases, peer assessments shall be performed on-site.

3. The peer assessment may rely on evidence gathered in the course of previous peer assessments or equivalent procedures of the peer-assessed Conformity Assessment Body or national cybersecurity certification authority, provided that:

(a) the results are not older than 5 years;

(b) the results are accompanied by a description of the peer assessment procedures established for that Scheme where they relate to a peer assessment conducted under a different Certification Scheme;

(c) the peer assessment report referred to in ANNEX VIII: CONTENT OF A CERTIFICATION ASSESSMENT REPORT specifies which results were reused with or without further assessment.

4. The peer-assessed Conformity Assessment Body and, where necessary, the national cybersecurity certification authority shall ensure that all relevant information is made available to the peer assessment team.

5. The peer assessment shall be carried out by a peer assessment team set up in accordance with ANNEX IX: SCOPE AND TEAM COMPOSITION FOR PEER ASSESSMENTS.

8.2 PEER ASSESSMENT PHASES

Explanatory note: The peer assessment needs to follow a well-established process, with several phases, from preparation to reporting, which should be harmonised with other peer assessment processes in other relevant Schemes, such as EUCC.

1. During the preparatory phase, the members of the peer assessment team shall review the Conformity Assessment Body's documentation, covering its policies and procedures, including the use of state-of-the-art documents.

2. During site visit phase, the peer assessment team assesses the body's technical competence.

3. The duration of the site visit phase may be extended or reduced depending on such factors as the possibility of reusing existing peer assessment evidence and results or the service profile(s) for which the Conformity Assessment Body issues certificates.

4. In the reporting phase, the assessment team shall document their findings in a peer assessment report including a verdict and, where applicable, a list of observed non-conformities, each graded by a criticality level.

5. The peer assessment report must be first discussed with the peer-assessed Conformity Assessment Body. Following those discussions, the peer-assessed Conformity Assessment Body establishes a schedule of the measures to be taken to address the findings.

8.3 PEER ASSESSMENT REPORT

Explanatory note: The peer assessment procedure results in a report, and the peer assessed Conformity Assessment Body is given the opportunity to address the identified nonconformities, if any, within an appropriate time limit set by the ECCG. The peer assessment report, after removing sensitive information from it, is published by ENISA, possibly with a negative opinion of the ECCG if the Conformity Assessment Body has not addressed the nonconformities in the allotted time.

1. The peer assessment team shall provide the peer-assessed Conformity Assessment Body with a draft of the peer assessment report.

2. The peer-assessed Conformity Assessment Body shall submit to the peer assessment team comments regarding the findings and a list of commitments to address the shortcomings identified in the draft peer assessment report.

3. The peer assessment team shall submit to the European Cybersecurity Certification Group a final peer assessment report, which shall also include the comments and the commitments made by the peer-assessed Conformity Assessment Body. The peer assessment team shall also include their position on the comments and on whether those commitments are sufficient to address the shortcomings identified.

4. Where non-conformities are identified in the peer-assessment report, the European Cybersecurity Certification Group may set an appropriate time limit for the peer-assessed Conformity Assessment Body to address the non-conformities.

5. The European Cybersecurity Certification Group shall adopt an opinion on the peer assessment report:

(a) where the peer-assessment report does not identify non-conformities or where non-conformities have been appropriately addressed by the peer-assessed Conformity Assessment Body, the European Cybersecurity Certification Group may issue a positive opinion and all relevant documents shall be published on ENISA's certification website;

(b) where the peer-assessed Conformity Assessment Body does not address the non-conformities appropriately within the set time limit, the European Cybersecurity Certification Group may issue a negative opinion that shall be published on ENISA's certification website, including the peer assessment report and all relevant documents.

6. Prior to the publication of the opinion, all sensitive, personal or proprietary information shall be removed from the published documents.

9 CHAPTER IX: UPDATE OF THE SCHEME

9.1 UPDATE OF THE SCHEME

Explanatory note: Due to the dynamic operational nature of Managed Security Services and the rapidly evolving cyber threat landscape, continuous update of the EUMSS is essential to ensure its ongoing relevance and effectiveness. Because the EUMSS employs a modular architecture, update activities may concern the Horizontal Layer, existing Vertical Layers and service profiles, the preparation and integration of new service profiles and new Vertical Layers, and the updating of supporting documents, state-of-the-art documents and guidance to facilitate the consistent application, evaluation and update of the Scheme. ENISA shall carry out updates in cooperation with the Commission and with the support of the European Cybersecurity Certification Group (ECCG) and relevant stakeholders. This chapter complements the activities described in Regulation (EU) 2019/881 (Cybersecurity Act) article 49.

1. The Commission may request the European Cybersecurity Certification Group to adopt an opinion in view of maintaining the EUMSS and to undertake the necessary preparatory works in accordance with Regulation (EU) 2019/881 (Cybersecurity Act) article 62(e); this may comprise the endorsement of state-of-the-art documents, supporting guidance and other documents referred to in paragraph 2.

2. To ensure that the Scheme remains aligned with technological developments, emerging threats, and Union legislative priorities, the update activities of the EUMSS shall include, inter alia:

    (a) the continuous review and update of the baseline security, reliability and operational resilience requirements in the Horizontal Layer set out in Annex II;

    (b) the continuous review and update of the requirements applicable to existing Vertical Layers and service profiles set out in Annex III;

    (c) the preparation and integration of additional service profiles and additional Vertical Layers falling within the MSS scope and mandate of this Scheme;

    (d) the preparation, update and endorsement of supporting documents, including state-of-the-art documents and guidance to facilitate the consistent application, evaluation and update of the Scheme.

3. The addition of a new service profile or Vertical Layer through update shall define at least:

    (a) the scope and boundaries of the new service profile or Vertical Layer;

    (b) any service-profile-specific or Vertical Layer-specific requirements;

    (c) the applicable assurance-level approach, including any requirements or reinforcements applicable to ‘basic’, ‘substantial’ or ‘high’;

(d) the evaluation approach, including any applicable state-of-the-art documents or guidance;

(e) the applicable certificate content, reporting requirements and transition arrangements;

(f) the date from which certification against the new service profile or Vertical Layer may be performed.

4. Supporting documents which have been endorsed by the European Cybersecurity Certification Group shall be published by ENISA on the dedicated European cybersecurity certification website.

In support of the update of the EUMSS, ENISA may organise the involvement of the private sector, conformity assessment bodies, and standardisation organisations in the form of ad hoc working groups to gather technical contributions and expert advice regarding the evolution of the Scheme.

10 CHAPTER X: FINAL REQUIREMENTS

10.1 NATIONAL SCHEMES COVERED BY THE EUMSS

Explanatory note: Because Managed Security Services are dynamic and rely on annual surveillance audits, this section requires providers holding valid national certificates to transition to an EUMSS certificate during their next scheduled annual review.

1. In accordance with Article 57(1) of Regulation (EU) 2019/881 (Cybersecurity Act) and without prejudice to Article 57(3) of that Regulation, all national cybersecurity Certification Schemes and the related procedures for Managed Security Services that are covered by the EUMSS shall cease to produce effects from 12/24[11] months after the entry into force of this Scheme.

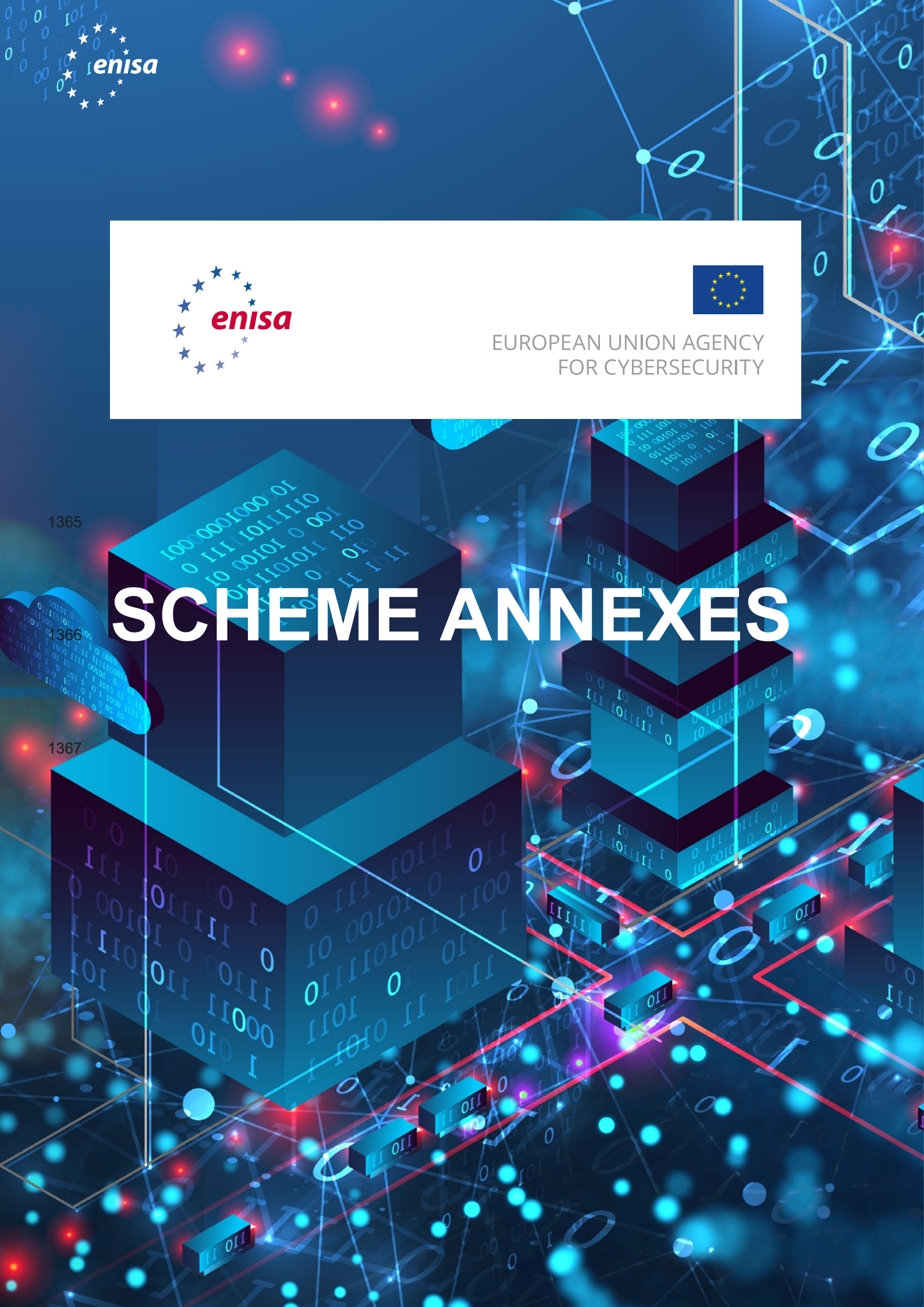
2. On the entry into Force, a certification process may be initiated under a national cybersecurity Certification Scheme within 12 months from the entry into force of this Scheme provided that the certification process is finalised not later than 24 months after the entry into force of this Scheme.

3. Existing certificates for Managed Security Services issued under national cybersecurity Certification Schemes that are covered by the EUMSS shall remain valid until their next scheduled annual surveillance or reassessment evaluation. At the time of this required yearly evaluation, the provider must transition to the EUMSS Scheme.

4. To facilitate the transition referred to in paragraph 3, the Conformity Assessment Body shall carry out a targeted evaluation and conduct a documented gap analysis to identify the deltas between the requirements of the relevant national Scheme and the applicable EUMSS requirements.

5. Where the provider successfully demonstrates that the necessary measures to bridge the identified deltas have been implemented, the Conformity Assessment Body shall issue a new EUMSS certificate replacing the reviewed national certificate, with same validity of the original certificate.

[11] Exceptions CSA Article 1-paragraph 2 ; CSA Article 57-paragraph 3.


enisa
enisa
EUROPEAN UNION AGENCY
FOR CYBERSECURITY
1365
1366
1367
SCHEME ANNEXES

11 ANNEX I: STATE-OF-THE-ART DOCUMENTS

11.1 CATEGORIES OF STATE-OF-THE-ART DOCUMENTS

Explanatory note: At the time of the initial review for opinion of the candidate EUMSS Scheme by the ECCG and its adoption, specific supporting documents that complement the Scheme may not be yet available. This Annex therefore establishes the structural categories for these documents.

1. State-of-the-Art documents are mandated to be used as explanation of the EUMSS.
2. Guidance may support the consistent application, evaluation and update of the EUMSS Scheme.
3. State-of-the-art documents and guidance shall not, by themselves, modify the scope of this Scheme or make a new service profile or Vertical Layer available for certification. A new service profile or Vertical Layer shall become available for certification only once introduced through the update process set out in CHAPTER IX: UPDATE OF THE SCHEME, including the definition of the applicable requirements and evaluation approach.
4. The guidance documents may cover:
    (a) the application of CEN/CENELEC TS 18072 and other relevant standards in the context of Managed Security Services;
    (b) acceptable evidence, sampling, on-site activities, operating-effectiveness assessment and assessment of subservices and dependency analysis;
    (c) certification assessment bodies in determining whether existing documentation, audit records, certificates, assessment results or other evidence may be considered relevant, valid, sufficient and appropriate for EUMSS evaluation activities;
    (d) accreditation, authorisation and notification of certification bodies;
    (e) the review, update or introduction of Horizontal Layer requirements, Vertical Layer requirements, service profiles, evaluation approaches or transition arrangements under Chapter IX.
    (f) MSSPs in the certification process.
    (g) applicants in conducting internal audits and self-assessments for the ‘basic’ assurance level, including templates, methodologies and examples of acceptable evidence.
    (h) List of accepted ISMS standards.

11.2 TRANSITION AND UNAVAILABILITY OF DOCUMENTS

Explanatory note: State-of-the-art documents and guidance may be developed, published or updated in accordance with the update process set out in CHAPTER IX: UPDATE OF THE SCHEME*of this Scheme.*

1. State-of-the-art documents and guidance may be developed, published or updated in accordance with the update process set out inCHAPTER IX: UPDATE OF THE SCHEME.
2. Where state-of-the-art documents are identified as applicable to a requirement, evaluation activity, service profile, Vertical Layer or assurance level, the Conformity Assessment Body shall take them into account as part of the evaluation.
3. Where no applicable state-of-the-art document is available for a particular evaluation activity or interpretation matter, the Conformity Assessment Body shall directly apply the requirements set out in Annex II and Annex III, together with the evaluation criteria, methods and standards referred to in Chapter II.
4. In such cases, the Conformity Assessment Body shall document the evaluation approach used and, where necessary, coordinate with the national cybersecurity certification authority to support consistent application of the Scheme.
5. The absence of state-of-the-art documents shall not prevent certification where the applicable requirements, evaluation criteria and methods are sufficiently defined in this Scheme.
6. State-of-the-art documents and guidance shall be published by ENISA on the dedicated European cybersecurity certification website, indicating their title, version, date of applicability and scope of application.

12 ANNEX II: HORIZONTAL LAYER

12.1 SCOPE AND OBJECTIVE OF THE HORIZONTAL LAYER

1. The Horizontal Layer provides one common set of baseline cybersecurity, reliability and operational resilience requirements applicable to all Managed Security Services certified under this Scheme. It shall be applied as a mandatory prerequisite for each certified service profile.
2. The Horizontal Layer does not constitute a stand-alone object of certification. An EUMSS certificate shall not be issued solely against the requirements of the Horizontal Layer. Compliance with this Annex shall be evaluated only in conjunction with the specific technical, operational and competence requirements of the requested service profile set out in Annex III: VERTICAL LAYER.
3. No EUMSS certificate or separate assurance level shall be issued for the Horizontal Layer alone. Assurance levels (‘basic’, ‘substantial’ or ‘high’) shall be granted at the level of the certified service profile within Annex III.
4. Requirements in this Annex are addressed to the Managed Security Service (MSS). Where a requirement is expressed as an obligation of the MSSP, it shall be read as applying to the MSSP solely in its capacity as provider of the certified MSS and limited to the assets, people and processes within the scope of the service (cf. OIS-01.1)." This avoids re-drafting each control and is consistent with Annex VIII (L2554), which already states that the Scheme "certifies the Managed Security Service and not the provider as an organisation".

5. The Horizontal Layer requirements set out in this Annex apply to all assurance levels. However, where those requirements are evaluated as part of a service-profile certification, the depth and rigour of their assessment shall correspond to the assurance level requested for that service profile, in accordance with Chapter I, Chapter II and the applicable evaluation methodology.

6. For the ‘basic’ assurance level, the evaluation of the Horizontal Layer shall verify the suitability of the design and implementation of the applicable requirements at the time of the evaluation. For the ‘substantial’ and ‘high’ assurance levels, the evaluation shall also verify, where applicable, the operating effectiveness of the relevant Horizontal Layer controls over the period defined by this Scheme.

12.2 BASELINE SECURITY DOMAINS

1. The baseline security controls of the Horizontal Layer are organised to secure the assets, personnel, facilities, and technologies used by the Managed Security Service Provider (MSSP) to deliver the service.
2. The requirements defined in this Annex cover the following cross-cutting operational domains:

a) Secure service and platform design: ensuring that Managed Security Services embed security-by-design and security-by-default principles;

b) Deployment and transition management: ensuring that services are securely integrated into client environments and that transitions are managed in a controlled and secure manner;

c) Availability and continuity management: ensuring resilience against disruptions and the continuity of service delivery;

d) Operational service management: ensuring that services are effectively operated, monitored, and managed on an ongoing basis;

e) Continuous improvement and technology update: ensuring that technologies supporting Managed Security Services remain secure, up to date, and fit for purpose over time.

12.3 HORIZONTAL LAYER SECURITY REQUIREMENTS

Explanatory note: The Horizontal Layer security controls have been split in technical security requirements and service delivery process requirements.
For the purposes of this review cycle, the detailed technical security requirements and operational controls for this Layer have been structured as distinct, self-contained chapters. This structural separation is intended to clearly distinguish the highly prescriptive technical and methodological evaluation criteria from the core legal, administrative, and procedural framework of the Scheme. This format facilitates a focused technical review by the experts and ensures the technical controls can be evaluated as a cohesive, modular framework.

12.3.1 Technical Security Requirements

This section establishes the security requirements for the Horizontal Layer of the EUMSS Certification Scheme, focusing on the baseline security requirements that need to be in place ahead of delivering any type of managed security services.

In reference to Article 51a of the Regulation (EU) 2019/881 (Cybersecurity Act)" of 25/04/2025, the requirements are designed to be able to evaluate that:

(a) *the managed security services are provided with the requisite competence, expertise and experience, including that the staff tasked with providing those services have a sufficient and appropriate level of technical knowledge and competence in the specific field, sufficient and appropriate experience, and the highest degree of professional integrity;*

(b) *the provider has appropriate internal procedures in place to ensure that the managed security services are provided at a sufficient and appropriate level of quality at all times;*

(c) *data accessed, stored, transmitted or otherwise processed in relation to the provision of managed security services are protected against accidental or unauthorised access, storage, disclosure, destruction, other processing, or loss or alteration or lack of availability;*

(d) *the availability of, and access to, data, services and functions is restored in a timely manner in the event of a physical or technical incident;*

(e) *authorised persons, programs or machines are able to access only the data, services or functions to which their access rights refer;*

(f) *a record is kept and is available for assessment, of the data, services or functions that have been accessed, used or otherwise processed, at what times and by whom;*

(g) *the ICT products, ICT services and ICT processes deployed in the provision of the managed security services are secure by design and by default and, where applicable, include the latest security updates and do not contain publicly known vulnerabilities.*

The requirements listed below are inspired from existing national Schemes.

12.3.2 MSS Service Delivery Process Requirements

This section establishes the security requirements for the Horizontal Layer of the EUMSS Certification Scheme, focusing on the process in place to deliver the service.

In reference to Article 51a of the Regulation (EU) 2019/881 (Cybersecurity Act)" of 25/04/2025, the following requirements are designed to be able to evaluate that:

"(b) that the provider has appropriate internal procedures in place to ensure that the managed security services are provided at a sufficient and appropriate level of quality at all times;

(c) that data accessed, stored, transmitted or otherwise processed in relation to the provision of managed security services are protected against accidental or unauthorised access, storage, disclosure, destruction, other processing, or loss or alteration or lack of availability;"

13 HoLa -Technical Security Requirements

The Technical Security Requirements listed below, apply uniformly across all MSSP service offerings and client engagements, providing a common foundation for security, resilience, and risk management.

The requirements listed below cover fifteen (15) categories, and each category is divided into themes. Each theme is structured as follows:

- A cybersecurity objective that the requirements aim to achieve.
- The conditions that must be satisfied to achieve the cybersecurity objective associated with each requirement.

There are many cross-references between requirements and themes. For instance, the ISP-02 theme, which defines how policies and procedures are to be defined, is referenced many times.

The categories, and their intended purposes, are:

1. Organisation of Information Security

Plan, implement, maintain and continuously improve the information security framework applicable to the MSS service.

2. Information Security Policies

Provide an information security policy, decomposed into topic-specific policies and procedures regarding security of the service, with the goal to address cyber risks and mitigate impact of incidents on persons, organisations and society.

3. Risk Management

Provide a risk management framework, to manage the risks associated to the service, from identification to treatment.

4. Human Resources

Ensure that personnel understand their responsibilities based on job role descriptions, are aware of their responsibilities regarding information security, and that the assets that are used to provide the service are protected in the event of changes in responsibilities or termination.

5. Asset Management

Identify the assets that are used to provide the service and ensure an appropriate level of protection throughout their lifecycle.

6. Physical Security

Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.

7. Operational Security

Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.

8. Identity, Authentication and Access Control Management

Limit access to information and information processing facilities.

9. Cryptography and Key Management

Document, communicate and implement policies and procedures for cryptography and key management related to the managed security service, including technical and organisational safeguards, in order to ensure the confidentiality, authenticity and integrity of the information.

10. Communication Security

Ensure the protection of information in networks and the corresponding information processing systems.

11. Change and Configuration Management

Ensure that changes and configuration actions to information systems guarantee the security of the delivered service.

12. Procurement Management

Ensure the protection of information that suppliers related to the managed security service can access and monitor the agreed services and security requirements.

13. Incident Management

Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of information security incidents related to the service.

14. Service Continuity

Plan, implement, maintain and test procedures and measures for business continuity and emergency management for the service.

15. Compliance and Continuous Improvement

Identify and audit the legal, regulatory and contractual requirements applicable to the information security and quality of the managed security service. Appy measures to improve information security, and quality of the MSS.

Controls shall be interpreted technology-neutrally, with compliance assessed against security outcomes achieved rather than the specific architectural pattern used.

13.1 Organisation of Information Security

13.1.1 OIS -01 Information Security Management System

13.1.1.1 Objective

The MSSP shall operate an Information Security Management System (ISMS). that covers the necessary organisational units, locations and processes for providing the service.

13.1.1.2 Requirements

The MSSP shall conform to EN ISO/IEC 27001:2022 and 27001:2024. Alternatively it shall conform to other equivalent ISMS specifications included in a list maintained by ENISA ANNEX XI: ACCEPTABLE ISMS STANDARDS FOR HOLA.	OIS-01.1
The MSSP shall document the scope of the managed security service that is under the MSSP's control.	OIS-01.2
The MSSP shall have an information security management system (ISMS), covering at least the operational units, locations, people and processes involved in providing the service.	OIS-01.3
The MSSP shall maintain documented information about the ISMS as applied to the managed security service, covering what is applicable to the service regarding: • Scope and boundaries of the ISMS; • The context of the MSSP; • Description of how the MSS is covered by activities in the ISMS; and • How the security of the service is maintained and improved.	OIS-01.4

13.1.2 OIS-02 Contact with Authorities and Interest Groups

13.1.2.1 Objective

The MSSP stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks (cf. RM-01) and vulnerabilities (cf. OPS-05). This requirement is not intended to cover the communication to authorities in relation to client incidents under report obligations. Such incident reporting obligations remain with the client. MSSP can only support the Customers in their communication with authorities.

13.1.2.2 Requirements

The MSSP shall maintain contact with relevant information security related authorities and appropriate technical groups to stay informed about current threats and vulnerabilities related to the managed security service.	OIS-02.1

13.1.3 OIS-03 Information Security in Project Management

13.1.3.1 Objective

Information security is considered in project management, regardless of the nature of the project.

13.1.3.2 Requirements

The MSSP shall perform a risk assessment according to RM-01 and assess and treat the risks on all projects that may affect the provision of the managed security service, regardless of the nature of the project.	OIS-03.1

13.2 Information security policies

13.2.1 ISP-01 Information Security Policy

13.2.1.1 Objective

Have an Information Security Policy adopted by the top management of the MSSP, communicated and made available to personnel of the MSSP and a statement on the MSSP commitment to information security to the relevant clients.

13.2.1.2 Requirements

The MSSP shall document an information security policy, covering the service, including at least the following aspects: • The importance of information security, based on the requirements of the clients in relation to information security, as well as on the need to ensure the security of the information processed and stored by the MSSP and the assets that support the service provided • The information security objectives, based on the business objectives and tasks of the MSSP; • The commitment of the MSSP to implement the security measures required to achieve the established security objectives • The most important aspects of the security strategy to achieve the established security objectives; and • The organisational structure for information security in the scope of the service. • A cybersecurity policy steering structure, being in charge of directing, monitoring the implementation of cybersecurity policy as well as reporting cybersecurity issues to top management.	ISP-01.1
The cybersecurity policy steering structure shall be responsible for the establishment, evolution, monitoring and control of the Information Security Policy. It shall report to top management on cyber issues.	ISP-01.2
The MSSP's top management shall approve and endorse the information security policy.	ISP-01.3
The MSSP shall communicate and make available the information security policy to personnel and a statement on the MSSP commitment to information security to the relevant clients.	ISP-01.4
The MSSP shall review the information security policy on a regular basis and at least following significant changes that are likely to affect the principles defined in the policy, including the approval and endorsement by top management.	ISP-01.5

13.2.2 ISP-02 **Topic**-specific policies and procedures

13.2.2.1 Objective

Topic-specific policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all relevant personnel of the MSSP and the personnel of the client involved in the service in an appropriate manner.

13.2.2.2 Requirements

The MSSP shall derive topic-specific policies and procedures from the information security policy for all relevant subject matters applicable to the managed security service, documented according to a uniform structure, including at least the following aspects: • Objectives; • Scope; • Roles and responsibilities within the organisation, including personnel competence requirements and the establishment of substitution rules; • Roles and dependencies on other organisations (especially managed security service clients and subservice providers); • Steps for the execution of the security strategy; and • Applicable legal and regulatory requirements	ISP-02.1
The MSSP shall communicate and make available the topic-specific policies and procedures to all personnel involved in the service.	ISP-02.2
The topic-specific policies and procedures shall be approved by the appropriate level of management.	ISP-02.3
The MSSP shall review the information security policy on a regular basis and at least following significant changes that are likely to affect the principles defined in the policy, including the approval and endorsement by top management. The appropriate level of management shall report at least annually to the top management on the topic-specific policies and procedures and their implementation. This reporting should include at least: • Implemented changes to address cyber risks for the topic; • Information security incidents for the topic and the follow-up; • Performance of the internal controls regarding information security for the topic (Cf. CCI-04) and • Planned changes for the topic to address cyber risks and information security and cybersecurity.	ISP-02.4
The MSSP's subject matter experts shall review the topic-specific policies and procedures for adequacy at least annually, and when major changes may affect the security of the service.	ISP-02.5
After a modification of topic-specific policies and procedures, they shall be approved by the appropriate level of management before they become effective, then communicated and made available to personnel.	ISP-02.6

13.2.3 ISP-03 Exceptions

13.2.3.1 Objective

Exceptions to the policies and procedures for information security are documented.

13.2.3.2 Requirements

The MSSP shall maintain a list of exceptions to the information security policies and procedures, including associated controls.	ISP-03.1
The exceptions shall be limited in time where applicable.	ISP-03.2
The exceptions shall be documented.	ISP-03.3
Exceptions leading to a nonconformity to any of the certification requirements of a certified managed security service shall not be allowed.	ISP-03.4
The exceptions shall be subjected to the RM-01 risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners.	ISP-03.5
The list of exceptions shall be reviewed at least annually.	ISP-03.6
The approval of the exceptions by risk owners shall be reviewed at least annually, even if the list has not been modified.	ISP-03.7

13.3 Risk Management

13.3.1 RM-01 Risk Management Policy

13.3.1.1 Objective

Have defined and documented risk management policies and procedures.

13.3.1.2 Requirements

The MSSP shall define risk management policies and procedures for the managed security service in accordance with ISP-02 and using a documented risk assessment methodology that enables reproducibility and comparability, for the following aspects: • Identification of the risks associated with the loss of confidentiality, integrity and availability of information within the scope of the service (cf. OIS-01.1) and assigning risk owners within the MSSP; • Analysis and determination of the likelihood, level and consequence of the identified risks on people, society, organisations and nations; • Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of risk treatment; • Treatment of the identified risks, including approval of authorisation and acceptance of residual risk by risk owners; • Ensuring that the risk assessment activities provide consistent, valid and comparable results, where possible; and • Retaining documented information of the risk assessment activities; • Conducting a review of the risk assessment and status of risk treatment plans by the management responsible for the security of the managed security service.	RM-01.1
The risk assessment shall include information security and cybersecurity risks, risks having to do with the competence, technical knowledge and experience of the staff tasked with providing the MSS and risks related to the quality of the service.	RM-01.2

13.3.2 RM-02 Risk Assessment Implementation

13.3.2.1 Objective

Risk assessment-related policies and procedures are implemented and have the entire managed security service in scope, and the results of the risk assessments made available to relevant parties.

13.3.2.2 Requirements

The MSSP shall implement the policies and procedures covering risk assessments on the entire MSS.	RM-02.1
The MSSP shall make the results of the risk assessments available to relevant internal parties	RM-02.2
Information, specific for their purposes, shall be made available to relevant external parties.	RM-02.3
The MSSP shall review the risk assessments at least annually, and after each major change that may affect the security of the managed security service.	RM-02.4
The MSSP shall monitor the evolution of the risk and review the risk assessments accordingly.	RM-02.5

13.3.3 RM-03 Risk Treatment Implementation

13.3.3.1 Objective

Cyber risks related to the managed security service are treated through a prioritised and documented risk treatment plan, reviewed after changes, communicated to relevant parties as appropriate, and formally accepted by risk owners based on acceptable residual risk.

13.3.3.2 Requirements

The MSSP shall prioritize the risk treatment according to the level of cyber risks related to the service.	RM-03.1
The MSSP shall document and implement a risk treatment plan based on the risk assessment (RM-01.1).	RM-03.2
The risk treatment plan shall reduce the risk level to a residual risk acceptable to the risk owners.	RM-03.3
The risk owners shall formally accept the risk treatment plan.	RM-03.4
The MSSP shall make the risk treatment plan available to relevant internal parties, including appropriately summarised and abstracted versions.	RM-03.5
The MSSP shall determine if relevant external parties shall receive information, specific for their purposes, about the risk treatment plan and to what extent.	RM-03.6
The MSSP shall review the risk treatment plan on an annual basis or every time the risk assessment is modified.	RM-03.7
The risk owners shall review for adequacy the analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, after each modification of the risk assessment and treatment plans.	RM-03.8

13.4 Human Resources

13.4.1 HR-01 Human Resources Policies

13.4.1.1 Objective

The policies applicable to the management of personnel involved in the delivery of the service include provisions that cover the legal, regulatory and contractual requirements. Furthermore, these policies include: a risk classification of all information security sensitive positions, a code of conduct and a disciplinary procedure that applies to all the personnel involved in supplying the managed security service who have breached the security policy.

13.4.1.2 Requirements

The MSSP shall classify information security-sensitive positions according to their level of risk, including positions related to IT administration and to the provisioning of the service in the production environment, and all positions with access to client data or system components.	HR-01.1
The MSSP shall include in its employment contracts, or in a dedicated code of conduct, an overarching agreement by personnel involved in the delivery of the MSS to act ethically in their professional duties.	HR-01.2
The MSSP shall define, document and implement a policy that describes actions to take in the event of violations of policies and procedures or applicable legal and regulatory requirements, including at least the following aspects: • Verifying whether a violation has occurred; and • Consideration of the nature and severity of the violation and its impact.	HR-01.3
If disciplinary measures are defined in this policy, then the personnel of the MSSP shall be informed about possible disciplinary measures.	HR-01.4
The policy shall state that use of these disciplinary measures shall be appropriately documented.	HR-01.5

13.4.2 HR-02 Verification of Competence and Trustworthiness

13.4.2.1 Objective

The competence and integrity of all personnel involved in the provision of the MSS, including the positions classified in objective HR-01 are verified by the MSSP prior to commencement of employment, follow-up changes in work-related personal situations and related risks identified and mitigated, in accordance with local legislation and regulation.

13.4.2.2 Requirements

The MSSP shall define and document the minimum staffing and skill levels for the service teams for each Service Profile and each assurance level it intends to pursue certification for.	HR-02.1
The qualification of the personnel shall be based on the European Cybersecurity Skills Framework (ECSF) or an equivalent framework or standard, or a documented internal competency framework demonstrating equivalent coverage of roles, responsibilities,	HR-02.2

knowledge, skills, competences, and proficiency levels relevant to the managed security service.. For all personnel with access to service data, including client personal data or system components under its responsibility, or personnel who are responsible to provide the service in the production environment, the MSSP shall: • Assess the competence and integrity before commencement of employment in a position classified in HR-01; and • Ensure personnel possess appropriate competence regarding personal data breach assessment, privacy requirements	HR-02.3
• Identify and mitigate of risks associated with personnel.	HR-02.4
The MSSP shall assess the competence and integrity of its personnel before commencement of employment in a position with a higher risk classification than their current position within the company.	HR-02.5
The extent of the assessment defined in HR-02.1 and HR-02.3, shall be proportional to the business context, the sensitivity of the information that will be accessed by the personnel, and the associated risks.	HR-02.6

13.4.3 HR-03 Personnel terms and **conditions**

13.4.3.1 Objective

The MSSP's personnel are required by the terms and conditions to comply with applicable policies and procedures relating to information security, and to the client's code of conduct, before being granted access to any client data or system components under the responsibility of the MSSP used to provide the service in the production environment.

13.4.3.2 Requirements

The MSSP shall ensure that all personnel are required by their terms and conditions to comply with all applicable information security policies and procedures.	HR-03.1
The non-disclosure provision shall cover any information that has been obtained or generated as part of the managed security service, even if anonymised and decontextualized.	HR-03.2 HR-03.3
The MSSP shall give a presentation of all applicable information security policies and procedures to personnel before granting them any access to client data, the production environment, or any functional component thereof related to the managed security service.	HR-03.4
Personnel shall acknowledge in a documented form the information security policies and procedures applicable to them before they are granted any access to client data, the production environment, or any functional component thereof.	HR-03.5

13.4.4 HR-04 Security Awareness and Training

13.4.4.1 Objective

The MSSP operates a target group-oriented training program and security awareness activities, which is completed by all personnel of the MSSP related to the service on a regular basis.

13.4.4.2 Requirements

The MSSP shall define a security training program, taking into account at least the position's risk classification and technical duties and, as applicable to specific target groups relevant for the service. Training shall ensure personnel possess sufficient competence to securely operate and manage all components relevant to the managed security service they deliver.	HR-04.1
The MSSP shall define a training program, taking into account the position's technical or managerial duties and, as applicable to specific target groups relevant for the service. The program shall cover at least the following aspects: • technical skills • editorial skills •	HR-04.2
The MSSP shall organise awareness activities tailored to the personnel of the MSSP related to the service. The activities may include emails, notices, meetings, a dedicated intranet section, etc. The activities shall cover at least the following topics: • The organisation's objectives and challenges regarding information system security; • Information considered sensitive; • Regulations and legal obligations; • The security rules and guidelines governing day-to-day activities: compliance with the security policy, not connecting personal devices to the organisation's network, not disclosing passwords to third parties, not reusing work passwords in private life and vice versa, reporting suspicious incidents, etc.; • The measures available and contributing to system security: systematic session lockout when the user leaves their workstation, password protection tools, etc. • Risks associated with the use of communication channels and methods, including verifying the authenticity and relevance of messages and using alternative channels where necessary	HR-04.3 HR-04.4
The MSSP shall review their security training programs and their awareness activities and based on changes to policies and procedures and the current threat situation.	HR-04.5
The MSSP shall ensure that all personnel complete the training and awareness activities defined for them.	HR-04.6
The MSSP shall measure and evaluate the learning outcomes achieved through the awareness and training activities.	HR-04.7
The results shall be used to improve the awareness and training program.	HR-04.8

13.4.5 HR-05 Roles, **Responsibilities** and Authorities

13.4.5.1 Objective

The MSSP has clear roles and responsibilities documented in relation to the provision of the MSS.

13.4.5.2 Requirements

The MSSP shall specify the roles that are related to the service.	HR-05.1
The first point of contact shall be published and easy to find by clients.	HR-05.2

The MSSP shall appoint a coordinator or engagement manager, responsible to oversee the activities throughout the managed security service, until the engagement is closed.	HR-05.3
The engagement manager shall establish a service team composed of appropriately skilled and trusted experts required for the service to be provided.	HR-05.4

13.4.6 HR-06 Segregation of Duties

13.4.6.1 Objective

Conflicting tasks and responsibilities are separated based on an RM-01 risk assessment to reduce the risk of unauthorised or unintended changes or misuse of client data in use, in motion or at rest in the managed security service.

13.4.6.2 Requirements

The MSSP shall perform a risk assessment as defined in RM-01 about the accumulation of responsibilities or tasks on roles or individuals, regarding the provision of the service, covering at least the following areas, insofar as these are applicable to the provision of the service and are in responsibility of the service: • Administration of rights profiles, approval and assignment of access and access authorisations (cf. IAM-01); • Development, testing and release of changes (cf. CCM-01); • Operation of the system components.	HR-06.1
The MSSP shall implement the mitigating measures defined in the risk treatment plan, prioritising, when possible, separation of duties.	HR-06.2
If implementation is impossible for organisational or technical reasons, the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions.	HR-06.3
The MSSP shall: • Introduce and maintain an inventory of conflicting roles including resolving measures;	HR-06.4
• Enforce the segregation of duties during the assignment or modification of roles as part of the role management process.	HR-06.5
The MSSP shall monitor and enforce measures related to segregation of duties to resolve conflicting roles.	HR-06.6

13.5 Asset Management

13.5.1 AM-01 Asset Inventory

13.5.1.1 Objective

The MSSP has established procedures for inventorying assets that are used to provide the managed security service, including applicable IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.

13.5.1.2 Requirements

The MSSP shall define, document and implement policies and procedures for maintaining a complete, accurate and consistent inventory of assets that are used to provide the service.	AM-01.1
The MSSP shall establish and maintain an inventory of assets relevant to the provision of the service (e.g. servers, workstations, network devices, applications and operating systems, monitoring tools, and supporting infrastructure), ensuring that tools and devices are authorised, centrally managed, and configured according to approved security baselines, protecting the integrity and availability of inventory data. The level of detail and completeness of the inventory shall be commensurate with the nature, scale and complexity of the service, and sufficient to support risk management, monitoring, vulnerability management and incident response .	AM-01.2
Asset information shall be sufficient to support risk management and operational security processes. Relevant attributes may include ownership, purpose, location, criticality and configuration state, version information and other relevant data, as appropriate. Asset information shall also support the application of the risk management procedure defined in RM-01, including the measures taken to manage the risks associated to the asset through its life cycle.	AM-01.3
The MSSP shall define roles and responsibilities for maintaining the inventory.	AM-01.4
Any change affecting the environment such as onboarding or decommissioning systems, modifying configurations, or adjusting cloud resources shall be reflected promptly in the inventory to ensure accuracy, traceability and alignment with the services operational reality.	AM-01.5
The MSSP shall implement processes and periodic verification mechanisms, preferably supported by automated discovery tools, to ensure that the inventory remains complete, reliable and consistent with the actual infrastructure.	AM-01.6
The MSSP shall provide relevant information on assets used for the service to the client upon request, taking into account security and confidentiality considerations.	AM-01.7
Where the Managed Security Service relies on specific ICT systems, service platforms, or software tools, the asset inventory shall include, or securely link to, a Software Bill of Materials (SBOM) in a commonly used machine-readable format. This SBOM information shall be maintained to directly support the vulnerability management procedures, monitoring, and impact analysis required under Chapter V CHAPTER V: VULNERABILITY MANAGEMENT AND DISCLOSURE.	AM-01.8

13.5.2 AM-02 Acceptable Use and Safe Handling of Assets Policy

13.5.2.1 Objective

Policies and procedures for acceptable use and safe handling of assets that are used to provide the managed security service, are documented, communicated and implemented in accordance with ISP-01, including removable media.

13.5.2.2 Requirements

The MSSP shall define, document, according to ISP-02, and implement policies and procedures for acceptable use and safe handling of assets that are used to provide the service.	AM-02.1
Only equipment provisioned and maintained by the MSSP shall be connected to networks of the MSSP or the client (if applicable for the service).	AM-02.2
The use of unmanaged or personal devices for delivering the service shall be forbidden	AM-02.3
The use of removable media shall be restricted and permitted only for unavoidable essential system administration actions, and only where no alternative mechanism is available. Where removable media is used, the MSSP shall ensure that its use is authorised and limited to a single specific purpose. The decision to use removable media shall be documented.	AM-02.4
All devices and media used for the service shall be suitably encrypted and further anti-theft measures shall be employed to ensure availability. If, for technical reasons, suitable encryption is not possible, anti-theft measures shall be strictly required.	AM-02.5
MSSP employees shall be instructed to store sensitive assets securely and encrypt sensitive data when applicable.	AM-02.6
Printers and multifunction devices shall be managed as full IT assets, hardened according to security best practices, and prevented from communicating with external networks.	AM-02.7
Any loss or theft of organisational equipment or media shall be reported immediately through an established incident-reporting process.	AM-02.8

13.5.3 AM-03 Commissioning and Decommissioning

13.5.3.1 Objective

Procedures for the commissioning and decommissioning of hardware assets used in the provision of the managed security service are documented, communicated and implemented, ensuring the proper configuration before commissioning and the proper deletion of data during decommissioning.

13.5.3.2 Requirements

The MSSP shall define, document and implement procedures for the commissioning of applicable hardware that is used to provide the service in the production environment, based on applicable policies and procedures, including those defined in RM-01, to ensure that the risks arising from the commissioning are identified, analysed and mitigated.	AM-03.1
The commissioning procedure shall include verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication and approval according to the intended use and based on the applicable policies, before authorisation to commission the asset can be granted.	AM-03.2
The MSSP shall define, document and implement procedures for the decommissioning of applicable hardware that is used to provide the service in the production environment, including the complete and permanent deletion of the data or the proper destruction of the media and requiring approval based on applicable policies.	AM-03.3

13.5.4 AM-04 Asset Classification and Labelling

13.5.4.1 Objective

Assets under the MSSP's control that are directly used to provide the managed security service, or that process, store or transmit service-related information, are classified and, where applicable, labelled according to the protection needs of that information.

13.5.4.2 Requirements

The MSSP shall document an asset classification schema that reflects for each asset that is used to provide the managed security service, the protection needs of the categories of information it embodies or may process, store, or transmit, and provide levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives.	AM-04.1
Where applicable, the MSSP shall label all assets according to their classification in the asset classification schema.	AM-04.2
The need for protection shall be determined by the individuals or groups responsible for the assets.	AM-04.3

13.6 Physical security

13.6.1 PS-01 Physical site access control

13.6.1.1 Objective

Physical access is subject to access control measures that match the area's security requirement and that are supported by an access control system.

13.6.1.2 Requirements

The MSSP shall define and document security perimeters in the buildings and premises used for providing the MSS.	PS-01.1
The MSSP shall define and document at least two security areas, with at least one sensitive area covering sensitive activities such as the buildings and premises hosting the information system for the provision of the MSS, and at least one public area covering all remaining buildings and premises, not covered by other security areas.	PS-01.2
The MSSP shall define, document and implement policies and procedures according to ISP-02 related to the physical access control to the security areas and based on the principles defined in IAM-01, including requirements on the physical access control measures to be implemented.	PS-01.3
The topic-specific policy for the physical access control shall include requirements concerning preventive and detective physical access control.	PS-01.4
The topic-specific policy for the physical access control shall include measures to identify individuals who are not part of the personnel, incorporating them into the access policy system, and define the conditions under which they may be granted access, if any, to the premises.	PS-01.5
Access to server rooms and technical areas shall be controlled using appropriate access control systems.	PS-01.6
Unaccompanied access by external contractors to server rooms and technical areas shall be prohibited, unless it is possible to strictly track access and restrict it to specific time slots.	PS-01.7
Access rights must be reviewed regularly to identify unauthorized access.	PS-01.8
Network sockets located in areas open to the public (meeting rooms, reception areas, corridors, cupboards, etc.) must be restricted or deactivated to prevent an attacker from easily gaining access to the company network.	PS-01.9
When the MSSP relies on third parties to host assets used for providing the MSS they shall apply the requirements defined in 13.12 Procurement Management.	PS-01.10

13.6.2 PS-02 Equipment protection

13.6.2.1 Objective

The equipment used in the client's premises and buildings to provide the managed security service is protected physically against damage and unauthorised access by specific measures.

13.6.2.2 Requirements

The MSSP shall define, document and implement policies and procedures according to ISP-02 concerning the protection of equipment that is used to provide the managed security service, and including at least the following aspects: PS-02.1

- Protecting power and communications cabling from physical interception, or damage;
- Protecting equipment during maintenance operations; and
- Protecting equipment holding client data.

These procedures shall include at least: PS-02.2

- A procedure to check the protection of power and communications cabling, to be performed regularly by qualified personnel, at least every two years, as well as in case of suspected manipulation; (a)
- A procedure for transferring any equipment containing client data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site, including approval by top management of the client, or by the appropriate level of management of the client that is responsible for this procedure; (b)
- A procedure to maintain and keep up to date a wiring Scheme; and (c)
- Measures to ensure that the conditions for installation, maintenance and servicing of the related technical equipment (e.g., electrical power, air conditioning, fire protection) are compatible with the managed security service's availability and security requirements. (d)

Where equipment containing media that stores client data or managed security service derived data is transferred to a third party and is no longer within the operational scope of the managed security service, the MSSP shall ensure that the third party is not granted access to such data. Before the transfer, the MSSP shall ensure that the data is either encrypted in accordance with CKM-03 or securely deleted using an appropriate secure deletion mechanism. PS-02.3

13.7 Operational security

13.7.1 OPS-01 Protection against malware

13.7.1.1 Objective

Policies are defined about the protection against malware of IT equipment related to the managed security service. Malware protection is deployed and maintained on systems that provide the service.

13.7.1.2 Requirements

Where applicable, the MSSP shall define, document and implement policies and procedures according to ISP-02 to protect its systems and clients' systems from malware, covering at least the following aspects: OPS-01.1

- Use of system-specific protection mechanisms;
- Operating protection programs on system components under the responsibility of the MSSP that are used to provide the managed security service in the production environment;
- Operation of protection programs for equipment assigned to personnel; and
- Operation of protection programs on all the incoming flows, including those over MSSP end-devices.

The MSSP shall deploy malware protection on all systems that support delivery of the MSS in the production environment, according to policies and procedures.	OPS-01.2
Signature-based and behaviour-based malware protection tools shall have regular automatic updates of malware definitions when such updates are available.	OPS-01.3
The MSSP shall update the anti-malware products according to established policies and procedures ensuring a timely update at the highest appropriate frequency consistent with the risk assessment.	OPS-01.4

13.7.2 OPS-02 Data Backup and Recovery

13.7.2.1 Objective

Policies define measures for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity. The proper execution of data backups is monitored and the proper restoration of data backups is regularly tested.

13.7.2.2 Requirements

The MSSP shall define, document and implement policies and procedures according to ISP-02 for, for data backup and recovery according to the sensitivity of the data, , covering at least the following aspects: • Data shall include client and MSS -derived data • The extent and frequency of data backups of the systems that are used by the MSSP to provide the service and the duration of data retention are consistent with the contractual agreements with the clients and the MSSP's; • Operational continuity requirements for recovery time objective (RTO) and recovery point objective (RPO); • Backup methods and data formats, including encryption, if relevant; • How backup data is stored, moved, managed, and disposed of; • Procedures for verifying integrity of backup data; • Procedures and timescales involved in restoring data from backup; • How a client-initiated recovery or recovery test is performed; • Restricted access to the backed-up data and the execution of restores only by authorised persons; and • Tests of recovery procedures	OPS-02.1
The MSSP shall document and implement technical and organisational measures to monitor the execution of data backups in accordance to the policies and procedures defined in OPS-02.	OPS-02.2
The MSSP shall test the restore procedures at least annually, including tests assessing if the specifications for the RTO and RPO agreed with the clients are met. The MSSP shall use only data in test accounts controlled by MSSP staff for testing purposes.	OPS-02.3
Any deviation from the specification during the restore test shall be reported to the MSSP's responsible person for assessment and remediation.	OPS-02.4
The MSSP shall transfer backup data to a remote location or transport them on backup media to a remote location, selected upon criteria of distance, recovery times and impact of disasters on backup and main sites.	OPS-02.5

The data classification of the original data shall be applied to backups.	OPS-02.6
The security measures at the remote site shall have at least the same level as at the main site.	OPS-02.7
When the backup data is transmitted to a remote location via a network, the transmission of the data shall take place in an encrypted form that corresponds to the state-of-the-art (cf. CKM-02).	OPS-02.8

13.7.3 OPS-03 Service IT hardening

13.7.3.1 Objective

Secure the service IT infrastructure.

13.7.3.2 Requirements

The MSSP must establish a minimum level of security across the service IT infrastructure (user workstations, servers, printers, telephones, USB devices, etc.) by implementing the following measures: • Limit installed applications and optional web browser modules to those that are strictly necessary; • Equip user workstations with a local firewall and antivirus software (these are sometimes included in the operating system); • Encrypt the partitions where user data is stored; • Disable autorun;	OPS-03.1
Where an exception to the general security rules applicable to workstations is necessary, these workstations must be isolated from the system (for example, if it is impossible to update certain applications for compatibility reasons)	OPS-03.2

13.7.4 OPS-04 Logging and Monitoring

13.7.4.1 Objective

Policies are defined to govern logging and monitoring events on system components under the MSSP's responsibility. Logs are monitored to identify information security events that may lead to information security incidents related to the managed service.

13.7.4.2 Requirements

The MSSP shall define, document and implement policies and procedures according to ISP-02 that govern the logging and monitoring of events on system components under its responsibility, covering at least the following aspects: • Definition of events that could lead to a violation of the protection goals; • Specifications for activating, stopping and pausing the various logs; • Information regarding the purpose and retention period of the logs; • Definition of roles, responsibilities and authorities for setting up and monitoring logging; • Definition of log data that may be transferred to the clients and technical requirements of such log forwarding; • Information about timestamps in event creation; and • Compliance with legal and regulatory frameworks	OPS-04.1

The MSSP shall maintain activity logs on the systems. The activity records shall include, at minimum, the identity of the operator, the date and time of the action, the systems affected, and the type of operations performed. The records shall include: • Outbound and inbound network traffic; • activities regarding user administration and permission management, access (including privileged access) to systems and applications • Activities performed with administrator accounts; • Assess or changes to logs, critical configuration files and backups; • Security relevant logs • Use and performance of system resources; • Physical access to facilities, where appropriate; • Environmental events, where appropriate; • Access and use of network equipment and devices; • Program installation and removal • Changes in scheduled tasks or automatic services.	OPS-04.2
These logs shall be maintained in a dedicated and tamper-resistant log, in a secure and controlled environment, and their availability, integrity and confidentiality shall be ensured.	OPS-04.3
The communication between the assets to be logged and the logging servers shall be authenticated, encrypted using state-of-the-art encryption.	OPS-04.4
When encryption is not feasible, the communication shall be accessible only by authorised personnel.	OPS-04.5
The logs shall be retained for at least a year. In case of an ongoing investigation the records shall not be deleted even if the one-year period has expired.	OPS-04.6
The MSSP shall provide clients, upon request, access to client-specific logging through secure and controlled mechanisms (e.g., APIs), ensuring appropriate authentication, authorization, and segregation of customer data.	OPS-04.7
The logging shall comply with the MSSP's protection requirements, including logical or physical separation of log and client data.	OPS-04.8
The MSSP shall monitor with automation log data in order to identify information security events that might lead to information security incidents related to the managed security service, in accordance with the logging and monitoring requirements.	OPS-04.9
The identified events shall be reported to the appropriate departments for timely assessment and remediation.	OPS-04.10

13.7.5 OPS-05 Managing Vulnerabilities, Malfunctions and Errors[12]

13.7.5.1 Objective

Vulnerabilities in the system components used to provide the managed security service are identified and addressed in a timely manner.

[12] The policies and procedures for identification and addressing of vulnerabilities in the system components used to provide the managed security service are aligned with Chapter V.

13.7.5.2 Requirements

The MSSP shall define and implement, in accordance with ISP-02, policies and procedures, including technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the managed security service, covering at least the following aspects: • Regular identification of vulnerabilities; • Assessment of the severity of identified vulnerabilities; • Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined case specific timelines; and • Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.	OPS-05.1

13.7.6 OPS-06 Clock synchronization

13.7.6.1 Objective

Provide a reliable clock synchronization service for time-based security controls (log management, tokens authentications).

13.7.6.2 Requirements

The MSSP shall define and implement, in accordance with ISP-02, policies and procedures, including technical and organisational measures to ensure synchronization of the clocks of all equipment on one or more internal time sources that are consistent with each other. These sources can themselves be synchronized to several external reliable sources, except for isolated networks.	OPS-06.1

13.7.7 OPS-07 Remote working

13.7.7.1 Objective

Implement measures to secure remote working.

13.7.7.2 Requirements

The MSSP shall define and implement, in accordance with ISP-02, policies and procedures, including technical and organisational measures to ensure that remote working is secured	OPS-07.1
The MSSP shall encrypt all the service's mobile devices (laptops, smartphones, USB sticks, external hard drives, etc.) in accordance with CKM-01, in order to preserve their confidentiality.	OPS-07.2
The MSSP shall implement safeguards (such as use of password, smart card, PIN code, etc.) for accessing data in the mobile devices.	OPS-07.3
The MSSP shall set up a network traffic control mechanism, such as a VPN connection or a Security Service Edge (SSE) solution, between the mobile device and the department's information system that cannot be disabled by the user. The choice of protocol used must be justified by the MSSP.	OPS-07.4

13.7.8 OPS-08 AI/ML Governance

13.7.8.1 Objective

Implement measures to secure the use of AI, ML and LLMs.

13.7.8.2 Requirements

OPS -08.1

Where artificial intelligence (AI), machine learning (ML), large language models (LLMs) or other AI-assisted technologies are used in the provision of managed security services, the MSSP shall establish documented controls governing their use.

OPS – 08.2

Such controls shall address human oversight, validation of outputs, accuracy, reliability, accountability, traceability of AI-assisted decisions, protection of input and output data, management of AI-related risks, and procedures for identifying, handling and escalating erroneous, misleading, biased or unexpected outputs.

1756

13.8 Identity, Authentication and Access Control Management

13.8.1 IAM-01 Policies for Access Control to Information and for Management of Identities

13.8.1.1 Objective

Policies and procedures for controlling the access to information resources and for managing the different types of identities that are used to provide the managed security service are documented, communicated and made available to employees of the MSSP. The systematic application of those policies and procedures is intended to ensure that that all accesses to information have been duly authorised.

13.8.1.2 Requirements

The MSSP shall define roles, rights and authorities in policies and procedures for controlling access to information and other associated assets that are used to provide the service, according to ISP-02 and based on role-based access control and on the business and security requirements of the MSSP, in which at least the following aspects are covered: • Parameters to be considered for making access control decisions; • Granting and modifying access rights based on the “least-privilege” principle and on the “need-to-know” principle; • Use of a role-based mechanism for the assignment of access rights; • Definition of the different types of identities and role-based access supported, and assignment of access control parameters and roles to be considered for each type; • Segregation of duties between managing, approving and assigning access rights; • Dedicated rules for users with privileged access; • Requirements for the approval and documentation of the management of identities and access rights; • Review mechanisms of the access logs, including anomaly detection and real-time alerting of suspicious access activity • Procedure for enterprise-wide password reset in case of a major incident • Regular review of assigned identities and associated access rights; • Measures to be taken in the event of potential identity compromise, such as disabling and removing identities; • Assigning of unique usernames; • Events and periods of inactivity leading to disabling and removing identities, where appropriate; and • Specific measures for the management of identities used infrequently for emergency recovery and other such scenarios.	IAM-01.1
The MSSP shall define, document and implement procedures for managing identities assigned to a single person, and access rights to personnel that comply with the role, authority and rights policies and with the policies for managing identities.	IAM-01.2
The MSSP shall define, document and implement procedures for managing identities assigned to multiple persons, and associated access rights that comply with the role, authority and rights policies and with the policies for managing identities.	IAM-01.3
The MSSP shall define, document and implement procedures for managing identities assigned to non-human entities, and associated access rights to system components involved in the operation of the service that comply with the role, authority	IAM-01.4

and rights policies and with the policies for managing identities.	
When removing an identity, a review shall be done on the resources linked to the identity (list established in IAM-02.5) to take appropriate action, in case of parentless resources, a specific status “No access” shall be set.	IAM-01.5
The MSSP shall link the access control policy defined in IAM-01.1 with the physical access control policy defined in PS-01.1, to guarantee that the access to the premises where information is located is also controlled	IAM-01.6

13.8.2 IAM-02 Disabling, reenabling and removing identities

13.8.2.1 Objective

Identities that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.

13.8.2.2 Requirements

The MSSP shall document and implement an automated mechanism to disable identities after a certain period of inactivity, as defined in the policy required in IAM-01.1, with exceptions for identities to be used in emergency recovery and similar scenarios, where extended periods of inactivity may be allowed.	IAM-02.1
The MSSP shall document and implement an automated mechanism to disable identities after a certain number of failed authentication attempts, following the policies defined according to IAM-01.1, with exceptions for identities to be used in emergency recovery and similar scenarios.	IAM-02.2
The MSSP shall document and implement a process to monitor stolen and compromised credentials and disable any identity for which an issue is identified, pending a review by an authorised person, and implement it on all identities under its responsibility to which privileged access rights are assigned.	IAM-02.3
Such processes shall include an exception mechanism for use in cases where all of the identities needed to manage the situation are potentially compromised.	IAM-02.4
Approval from authorised personnel or system components is required to re-enable identities that have been disabled.	IAM-02.5
The MSSP shall document and implement a mechanism to remove identities that have been disabled after a certain period of inactivity, as defined in the policy required in IAM-02.1.	IAM-02.6

13.8.3 IAM-03 Management of Access Rights

13.8.3.1 Objective

Policies and procedures are defined for managing and controlling the assignment of access rights to identities that are assigned for the provision of the managed security service.

13.8.3.2 Requirements

The MSSP shall document and implement procedures to grant, update, disable and remove access rights to managed security service information system resources to an identity under its responsibility.	IAM-03.1
These procedures shall be in conformity with the role, authorities and rights policies and with the policies for managing access rights	IAM-03.2
The MSSP shall document and implement a procedure to timely update or revoke the access rights of personnel when the role and responsibilities of the personnel change, within 48 hours of the role change for privileged access rights and within 14 days for other access rights.	IAM-03.3
If the MSSP defines emergency identities to be used when the main authentication technology is not available, then the MSSP shall define and enforce specific requirements related to these identities.	IAM-03.4
Approval from authorised personnel or system components is required to re-enable identities that have been disabled.	IAM-03.5

13.8.4 IAM-04 Regular Review of Access Rights

13.8.4.1 Objective

The fitness for purpose of the identities and their associated access rights are reviewed regularly.

13.8.4.2 Requirements

The MSSP shall review the identities under its responsibility and associated access rights at least once a year to ensure that they still correspond to the current needs.	IAM-04.1
The MSSP handles identified deviations timely, but no later than 7 days after their detection, by appropriately revoking or updating access rights.	IAM-04.2
The MSSP shall support clients with the review of the identities under their responsibility and associated access rights..	IAM-04.3

13.8.5 IAM-05 Privileged Access Rights

13.8.5.1 Objective

Privileged access rights and the identities to which they are granted are subject to additional scrutiny.

13.8.5.2 Requirements

Privileged access rights shall be tailored, limited according to a risk assessment and assigned as necessary for the execution of tasks (the principle of least privilege).	IAM-05.1
Activities of identities with privileged access rights shall be logged in order to facilitate the detection of any misuse of privileged access or function in suspicious cases.	IAM-05.2

The logged information shall be monitored for defined events that may indicate misuse.	IAM-05.3
The MSSP shall document and implement a procedure that, upon detection of potential misuse by this monitoring, informs the responsible personnel so that they can promptly assess whether misuse has occurred and take corresponding action.	IAM-05.4
Identities assigned to multiple persons under the responsibility of the MSSP shall be assigned only to MSSP personnel.	IAM-05.5
The assigned identities shall follow IAM-05 requirements.	IAM-05.6
The MSSP shall require strong authentication (for example: multifactor authentication or password less approach) for accessing the administration interfaces used by the client.	IAM-05.7

13.8.6 IAM-06 Authentication mechanisms

13.8.6.1 Objective

Adequate authentication mechanisms are used to grant access to any environment and when needed within an environment.

13.8.6.2 Requirements

The MSSP shall define, document and implement according to ISP-02 policies and procedures about authentication mechanisms, covering at least the following aspects: • The selection of mechanisms suitable for every type of identity and each level of risk; • The protection of credentials used by the authentication mechanism; • The generation and distribution of credentials for new identities; • Rules for the renewal of credentials, including periodic renewals, renewals in case of loss or compromise; and • Rules on the required strength of credentials, together with mechanisms to communicate and enforce the rules. • Whenever possible, password less authentication mechanism shall be used.	IAM-06.1
The access to all environments of the MSSP shall be authenticated, including non-production environments.	IAM-06.2
The access to all environments under the control of the MSSP that contain client data, including the production environment of the client, shall require strong authentication (for example multi-factor authentication).	IAM-06.3
Within an environment, user authentication shall be performed through passwords, digitally signed certificates or procedures or mechanisms that achieve at least an equivalent level of security.	IAM-06.4
For access to non-personal identities assigned to multiple persons, the MSSP shall implement measures that require the users to be authenticated with their identity assigned to a single person, before being able to access these identities assigned to multiple persons.	IAM-06.5
	IAM-06.6

All authentication mechanisms shall include a mechanism to disable an identity after a predefined number of unsuccessful attempts.	

13.8.7 IAM-07 Protection and strength of credentials

13.8.7.1 Objective

Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the subject associated to a specific identity has been authenticated.

13.8.7.2 Requirements

The MSSP shall document, communicate and make available to all service users under its responsibility rules and recommendations for the management of credentials, including at least: • Non-reuse of credentials; • Trade-offs between entropy and ability to memorize; • Recommendations for renewal of passwords; • Rules on storage of passwords; • Confidentially of personal (or shared) authentication and non-sharing of credentials; • Recommendations on password managers; and • Recommendation to specifically address classical attacks, including phishing, social attacks, and whaling.	IAM-07.1
Passwords shall be only stored using cryptographically strong hash functions (cf. CKM-01), except when passwords are stored for subsequent re-use in the plain text form, for example in a password manager.	IAM-07.2
In the latter case stored passwords shall be protected, using a cryptographically strong mechanism.	IAM-07.3
If cryptographic authentication mechanisms are used, they shall follow the policies and procedures from CKM-01.	IAM-07.4
When creating credentials, compliance with policies shall be enforced.	IAM-07.5
When a credential associated to an identity assigned to a single person is changed or renewed, the person associated to that identity shall be notified.	IAM-07.6
Any password reset procedure shall not be valid for more than 48 hours.	IAM-07.7
The password shall be changed by the user after the use of the reset procedure.	IAM-07.8
The MSSP shall raise users' awareness of the risks associated with choosing a password that is too easy to guess, or reusing passwords across different applications, particularly between personal and work email accounts.	IAM-07.9

13.8.8 IAM-08 General access restrictions

13.8.8.1 Objective

The assets in and around the managed security service are managed in a way that ensure that access restrictions are enforced between different categories of assets.

1799 #### 13.8.8.2 Requirements

The MSSP shall implement sufficient partitioning measures between the information system providing the managed security service and its other information systems.	IAM-08.1
The MSSP shall implement suitable measures for partitioning between the clients. Unless legally forbidden, the MSSP shall, in a timely manner inform a client, whenever personnel of the MSSP gain access to the client's data processed, stored or transmitted in the managed security service without the prior consent of the client, including at least: • Cause, time, duration, type and scope of the access; and • Enough details to enable subject matters experts of the client to assess the risks of the access	IAM-08.2

1800

1801

13.9 Cryptography and key management

13.9.1 CKM-01 Policies and Procedures for the use of Cryptography and Key management

13.9.1.1 Objective

Policies and procedures for cryptography and key management related to the managed security service, including technical and organisational safeguards, are documented, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.

13.9.1.2 Requirements

The MSSP shall define, document and implement policies with technical and organisational safeguards for cryptography and key management related to the managed security service, according to ISP-02, in which at least the following aspects are described: • Usage of strong cryptographic mechanisms and secure communication protocols, corresponding to the state of the art; • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys; • Consideration of relevant legal and regulatory obligations and requirements; and • Risk-based provisions for the use of encryption aligned with the data classification Schemes and considering the communication channel, type, strength and quality of the encryption.	CKM-01.1
Procedures and technical safeguards for secure key management in the area of responsibility of the MSSP shall include at least the following aspects: • Generation of keys for different cryptographic systems and applications; • Issuing and obtaining public-key certificates; • Provisioning and activation of the keys • Secure storage of keys including description of how authorised users get access; • Handling of compromised keys; and • Withdrawal and deletion of keys;	CKM-01.2
If pre-shared keys or wildcard certificates are used, the specific provisions relating to the secure use of these procedures shall be specified separately.	CKM-01.3

13.9.2 CKM-02 Encryption of data in motion

13.9.2.1 Objective

Client data transmission and MSSP remote access over public networks both to, or by, the MSSP is protected in confidentiality, integrity, and authenticity.

13.9.2.2 Requirements

The MSSP shall select and implement strong cryptographic mechanisms for the transmission of client data both to, or by, the MSSP over public networks, in order to protect the confidentiality, integrity and authenticity of data.	CKM-02.1
The MSSP shall use strong cryptographic mechanisms to protect the communication during remote access to the production environment, including personnel authentication.	CKM-02.2

13.9.3 CKM-03 Encryption of data at rest

13.9.3.1 Objective

The MSSP has established procedures and technical safeguards to prevent the disclosure of client data during storage.

13.9.3.2 Requirements

The MSSP shall select and implement procedures and technical safeguards, including encryption, to protect the confidentiality of client data during storage, according to ISP-02.	CKM-03.1
The MSSP shall notify clients of security relevant updates of these procedures and technical safeguards and to changes in the storage of client data that may affect the confidentiality of the data.	CKM-03.2
The procedures for the use of private and secret keys, including a specific procedure for any exceptions, shall be contractually agreed with the client.	CKM-03.3

13.10 Communication security

13.10.1 CS-01 Technical safeguards

13.10.1.1 Objective

The MSSP has implemented appropriate technical safeguards in order to detect and respond to network-based attacks as well as to ensure the protection of information and information processing systems.

13.10.1.2 Requirements

The MSSP shall document, communicate and implement technical safeguards that are suitable to promptly detect and respond to network-based attacks and to ensure the protection of information and information processing systems, in accordance with ISP-02, and based on the results of a risk analysis carried out according to RM-01.	CS-01.1
The MSSP shall feed into a Security Information and Event Management (SIEM) system, relevant data from these technical safeguards	CS-01.2

13.10.2 CS-02 Network topology documentation

13.10.2.1 Objective

A map of the network topology is created and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery from malfunctions.

13.10.2.2 Requirements

The MSSP shall maintain up-to-date documentation describing the logical structure of the network used to provision or operate the managed security service.	CS-02.1

The documentation shall cover, at least, how the subnets are allocated, how the network is zoned and segmented, how it connects with third-party and public networks, and the geographical locations in which the client data is stored.	CS-02.2
In liaison with the inventory of assets (cf. AM-01), the documentation shall include the equipment that provides security functions and the servers that host the data or provide sensitive functions.	CS-02.3
The MSSP shall perform a full review of the network topology documentation at least once a year.	CS-02.4

13.10.3 CS-03 Security requirements to connect within the MSSP´s network

13.10.3.1 Objective

The establishment of connections within the MSSP's network is subject to specific security requirements.

13.10.3.2 Requirements

The MSSP shall define, document and implement according to ISP-02 specific security requirements to connect within its network, including at least: • When the clients are to be logically or physically segregated; • What communication relationships and what network and application protocols are permitted in each case; • How the data traffic for administration and monitoring are segregated from each other at the network level; • What internal, cross-location communication is permitted and • What cross-network communication is allowed.	CS-03.1
The MSSP shall establish and maintain an accurate representation of the technical and logical structure of client's systems based on its network topology documentation (cf. CS-02) and asset inventory (cf. AM-01).	CS-03.2

13.10.4 CS-04 Monitoring of connections within the MSSP´s network

13.10.4.1 Objective

The network traffic exchanged with the managed security service, internal and external, is monitored to respond appropriately and timely to threats.

13.10.4.2 Requirements

The MSSP shall distinguish between trusted and untrusted networks, based on a risk assessment according to RM-01.	CS-04.1
The MSSP shall separate trusted and untrusted networks into different security zones for internal and external network areas (and DMZ, if applicable).	CS-04.2
The MSSP shall design and configure both physical and virtualized network environments to restrict and monitor the connection to trusted or untrusted networks according to the defined security requirements (cf. CS-02).	CS-04.3

The MSSP shall review at least annually the design and implementation and configuration undertaken to monitor the connections in a risk-oriented manner, with regard to the defined security requirements.	CS-04.4
The MSSP shall assess the risks of identified vulnerabilities in accordance with the risk management procedure (cf. RM-01).	CS-04.5
Follow-up measures shall be defined and tracked	CS-04.6

13.10.5 CS-05 Networks for administration

13.10.5.1 Objective

Administrative and operational management duties are performed on networks segregated from other networks to prevent unauthorised traffic and to maintain separation of duties.

13.10.5.2 Requirements

The MSSP shall define, document and implement separate networks for system administration and the operation of management consoles.	CS-05.1
The MSSP shall logically or physically separate the networks for system administration from any other network.	CS-05.2
The MSSP's information system administration workstations must under no circumstances be connected to the internet.	CS-05.3
In the event that administrative tasks require an internet connection, the service provider may implement workarounds such as: • Providing a separate workstation for tasks requiring an internet connection • Providing access to a remote virtualized infrastructure for office applications from an administration workstation	CS-05.4

13.10.6 CS-06 Data Transmission Policies

13.10.6.1 Objective

Policies are defined to protect the transmission of data against unauthorised interception, manipulation, copying, modification, redirection or destruction, and malware intrusion.

13.10.6.2 Requirements

The MSSP shall define, document and implement policies and procedures with technical and organisational safeguards to protect the transmission of data against unauthorised interception, manipulation, copying, modification, redirection or destruction, and malware intrusion according to ISP-02.	CS-06.1
The policies and procedures shall include references to the classification of assets (cf. AM-05).	CS-06.2

13.11 Change and Configuration Management

13.11.1 CCM-01 Policies for changes to ICT systems

13.11.1.1 Objective

Policies and procedures are documented, communicated and implemented to control changes to ICT systems supporting the managed security service.

13.11.1.2 Requirements

The MSSP shall define, document and implement policies and procedures for change management of the ICT systems supporting the managed security service according to ISP-02, covering at least the following aspects: • Criteria for risk assessment, categorization and prioritization of changes and related requirements for the type and scope of testing to be performed, and necessary approvals; • Requirements for the performance and documentation of tests; • Requirements for segregation of duties during planning, testing, and release of changes; • Requirements for the proper information of clients about the type and scope of the change as well as the resulting obligations to cooperate in accordance with • the contractual agreements; • Requirements for the documentation of changes in the system, operational and user documentation; • Requirements for the implementation and documentation of emergency changes, which shall, to the extent possible in the emergency, comply with the same level of cybersecurity as normal changes; and • Requirements for the handling of a change's unexpected effects, including corrective actions.	CCM-01.1

13.11.2 CCM-02 Risk Assessment, Categorisation and Prioritisation of Changes

13.11.2.1 Objective

Changes are categorised and prioritised according to potential security effects.

13.11.2.2 Requirements

The MSSP shall categorise and prioritise changes considering the potential security effects on the system components concerned.	CCM-02.1
The categorisation and prioritisation of the changes shall be based on a risk assessment performed in accordance with RM-01 with regard to potential effects on the system components concerned that are used to provide the managed security service.	CCM-02.2
If the risk associated to a planned change is high, then appropriate mitigation measures shall be taken before deploying the change in the service's production environment.	CCM-02.3

13.11.3 CCM-03 Performing and Logging Changes

13.11.3.1 Objective

Changes to the managed security service are performed through authorised accounts and traceable to the person or system component who initiated them.

13.11.3.2 Requirements

The MSSP shall define roles and rights according to IAM-01 for the authorised personnel or system components who are allowed to make changes to the managed security service in the production environment.	CCM-03.1
All changes to the managed security service in the production environment shall be logged.	CCM-03.2
All changes to the managed security service in the production environment shall be traceable back to the individual or system component that initiated the change.	CCM-03.3

13.12 Procurement Management

13.12.1 PM-01 Policies and Procedures for Controlling and Monitoring Third Parties

13.12.1.1 Objective

Policies and procedures are defined to supervise the activities of third parties who contribute to the provision of the managed security service.

Where a supplier, subcontractor or third party provides a subservice used for the design, operation, management or delivery of the Managed Security Service submitted for certification, the treatment of that subservice for evaluation purposes shall follow the rules on subservices and dependency analysis set out in Chapter II.

13.12.1.2 Requirements

The MSSP shall define, document and implement policies and procedures according to ISP-02 for controlling and monitoring third-parties whose products or services contribute to the provision of the managed security service. Such policies and procedures shall address, as applicable, the aspects listed below and may rely on alternative assurance mechanisms, including supplier self-assessments, self-declarations, certifications, attestations, or other equivalent evidence where direct verification, monitoring, or contractual enforcement is not reasonably feasible. The policies and procedures shall cover at least the following aspects: • Requirements for the assessment of risks resulting from the procurement of third-party products and services; • Information security requirements for the processing, storage, or transmission of information by third parties based on industry accepted standards; • Information security awareness and training requirements for third-party staff; • Applicable legal and regulatory requirements; • Requirements for dealing with vulnerabilities, information security incidents, and malfunctions; • Specifications for the contractual agreement of these requirements, to the extent permitted by the nature of the commercial relationship and the contractual arrangements available from the third party; • Specifications for the monitoring of these requirements; and • Specifications for applying these requirements also to service providers used by the third-parties, insofar as the services provided by these service providers also contribute to the provision of the service. •	PM-01.1
The MSSP shall contractually require its subservice providers to provide regular assurance information by independent auditors or CABs on the suitability of the design and operating effectiveness of their service-related internal control system with respect to the applicable service requirements.	PM-01.2
The assurance information shall cover the complementary subservice organisation controls that are required, together with the controls of the MSSP, to meet the applicable service requirements with reasonable assurance.	PM-01.3
In case the subservice providers are not able to provide compliance assurance information, the client shall reserve the right to audit them using qualified personnel under an internationally recognised audit framework to assess the suitability and effectiveness of the service-related internal and complementary controls.	PM-01.4

13.12.2 PM-02 Risk Assessment of Suppliers

13.12.2.1 Objective

Suppliers of the MSSP undergo a risk assessment to determine the security needs related to the product or service they provide for the managed security service.

13.12.2.2 Requirements

The MSSP shall perform a risk assessment of its suppliers in accordance with the policies and procedures for the control and monitoring of third parties before they start contributing to the provision of the managed security service, or, for existing suppliers without undue delay after their involvement in the service has been identified. The assessment shall include the identification, analysis, evaluation, handling, and documentation of risks concerning the following aspects: • Protection needs regarding the confidentiality, integrity, availability, and authenticity of information processed, stored, or transmitted by the third-party; • Impact of a protection breach on the provision of the managed security service; and • The MSSP's dependence on the supplier or service provider for the scope, complexity, and uniqueness of the purchased product or service, including the consideration of possible alternatives.	PM-02.1
Following the risk assessment of a subservice provider, the MSSP shall define for every applicable service requirement a list of complementary subservice organisation controls to be implemented by the subservice provider.	PM-02.2
The MSSP shall ensure that the subservice provider has implemented the complementary subservice organisation controls.	PM-02.3
The MSSP shall ensure that the subservice provider has made available to the MSSP assurance information supporting the assessment of their suitability and operating effectiveness for the targeted evaluation level.	PM-02.4
The adequacy of the risk assessment and of the definition of complementary subservice organisation controls shall be reviewed regularly, at least annually.	PM-02.5
When the MSSP relies on products from a supplier to operate the managed security service, the MSSP shall not allow this supplier to access any client data and managed security service derived data, unless they: • Perform a risk assessment according to RM-01 on the possible exposure of client data, managed security service derived data or client account data; and • Inform their clients of these possible accesses in contractual documentation.	PM-02.6
The MSSP shall ensure that all operations requiring access to client data, managed security service derived data or client's account data are performed or supervised by personnel who have been authorized.	PM-02.7

13.12.3 PM-03 Directory of Suppliers

13.12.3.1 Objective

A directory of suppliers who contribute to the delivery of the managed security service, is available to facilitate their control and monitoring.

13.12.3.2 Requirements

The MSSP shall maintain a directory for controlling and monitoring the suppliers who contribute to the delivery of the service, containing at least the following information: • Company name; • Address; • Locations of data processing and storage; • Responsible contact person at the supplier; • Responsible contact person at the MSSP; • Description of the product or service; • Beginning of service usage; and • Proof of compliance with contractually agreed requirements.	PM-03.1
The MSSP shall verify the directory for completeness, accuracy and validity at least annually.	PM-03.2

13.12.4 PM-04 Monitoring of compliance with requirements

13.12.4.1 Objective

Monitoring mechanisms are in place to ensure that third parties comply with their regulatory and contractual obligations.

13.12.4.2 Requirements

The MSSP shall monitor the compliance of its suppliers with information security requirements and applicable legal and regulatory requirements in accordance with policies and procedures concerning controlling and monitoring of third parties, including at least a regular review of the following assurance information, as provided by suppliers under contractual agreements: • Reports on the quality of the service provided; • Certificates of the management systems' compliance with international standards; • Independent third-party reports on the suitability and operating effectiveness of their service-related internal control systems; and • Records of the third parties on the handling of vulnerabilities, information security incidents and malfunctions**.**	PM-04.1
The MSSP shall monitor the compliance of its subservice providers with the complementary subservice organisation controls applicable to them following the risk assessment, ensuring that the depth and extent of monitoring activities are commensurate with the level of risk associated with each subservice provider. (cf. PM-02).	PM-04.2
The frequency of the monitoring shall be based on the risk assessment conducted by the MSSP (cf. PM-02).	PM-04.3
The results of the monitoring shall be considered in the review of the third party's risk assessment.	PM-04.4
Identified violations and deviations shall be analysed, evaluated and treated in accordance with the risk management procedure (cf.RM-01).	PM-04.5
The MSSP shall document and implement a procedure to review, at least once a year, non-disclosure or confidentiality requirements regarding suppliers contributing to the provision of the managed security service.	PM-04.6

	When a change in a third-party contributing to the provision of the managed security service significantly adversely affects its level of security, the MSSP shall inform all of its clients without undue delay.	PM-04.7
	The MSSP shall monitor the compliance of its subservice providers with the complementary subservice organisation controls applicable to them following the risk assessment (cf. PM-02).	PM-04.8

1898

13.13 Information Security Incident Management

13.13.1 IM-01 Policy for Information Security Incident Management

13.13.1.1 Objective

A policy is defined to respond to information security incidents related to the managed security service in a fast, efficient and orderly manner.

13.13.1.2 Requirements

The MSSP shall define, document and implement policies and procedures according to ISP-02 containing technical and organisational safeguards to ensure a fast, effective and proper response to all known information security incidents related to the managed security service, including: • Guidelines for the classification, prioritisation, and escalation of information security incidents; • Description of events that trigger the incident management and that activate business continuity processes; • Identification and definition of communication channel with the clients and the Authorities and procedures as to how the data of a potentially impacted systems can be collected in a conclusive manner in the event of an information security incident.	IM-01.1
The information security incident management policy shall be coherent with the service continuity and disaster recovery plan. The policy shall include: • a categorisation system for incidents that is consistent with the event assessment and classification; • effective communication plans including for escalation and reporting; • assignment of roles to detect and appropriately respond to incidents to competent employees; • documents to be used in the course of incident detection and response such as incident response manuals, escalation charts, contact lists and templates.	IM-01.2
The incident response procedures shall include the following stages: • incident containment, to prevent the consequences of the incident from spreading; • incident eradication, to prevent the incident from continuing or reappearing, • recovery from the incident, where necessary.	IM-01.3
The MSSP shall test at planned intervals their information security incident management policy and procedures.	IM-01.4

13.13.2 IM-02 User's Duty to Report Information Security Incidents

13.13.2.1 Objective

Users are aware of their obligations to report information security incidents related to the managed security service.

13.13.2.2 Requirements

The MSSP shall inform personnel, clients and external business partners of their contractual obligations to report all information security events that become known to them and are related to the managed security service.	IM-02.1

The MSSP shall put in place a simple mechanism allowing their employees, suppliers, and clients to report suspicious information security events.	IM-02.2
The MSSP shall regularly train their employees how to use the reporting mechanism.	IM-02.3
The MSSP shall analyse the reported events and any abnormal system activity (cf OPS-04.9) and assess whether they constitute incidents and, if so, determine their nature and severity.	IM-02.4
The MSSP shall not take any negative action against those who report in good faith, events that do not subsequently turn out to be information security incidents.	IM-02.5
The MSSP shall make the information security incident reporting mechanism known as part of its communication to personnel, clients and external business partners.	IM-02.6
The MSSP shall define, publish and implement a single point of contact to receive reports of information security events and vulnerabilities.	IM-02.7

13.13.3 IM-03 Handling of Information Security Incidents

13.13.3.1 Objective

A methodology is defined and applied to handle information security incidents in a fast, efficient and orderly manner.

13.13.3.2 Requirements

The MSSP shall classify and prioritise information security events that could constitute an information security incident, and perform root-cause analyses for these events, using their subject matter experts and external security providers where appropriate.	IM-03.1
The MSSP shall maintain a catalogue that clearly identifies the information security incidents that affect client data and use that catalogue to classify information security incidents.	IM-03.2
The incident classification mechanism shall include provisions to correlate information security events.	IM-03.3
In addition, these correlated information security events shall themselves be assessed and classified according to their criticality.	IM-03.4
The MSSP shall respond to incidents in accordance with the procedures specified in IM-01.3 and in a timely manner.	IM-03.5
The MSSP shall log incident response activities in accordance with the procedures referred to in IM-01.3, and record evidence.	IM-03.6

13.13.4 IM-04 Documentation and Reporting of Information Security Incidents

13.13.4.1 Objective

Information security incidents related to the MSS are documented and reported in a timely manner to clients, supervisory authorities and CSIRTs.

13.13.4.2 Requirements

The MSSP shall comply with reporting obligations as mandated by relevant legislative frameworks for network and information security incidents, including supervisory authorities and CSIRTs.	IM-04.1

The MSSP shall establish communication plans and procedures: a) with the Computer Security Incident Response Teams (CSIRTs) or, where applicable, the competent authorities, related to incident notification; b) for communication among staff members of the MSSP, and for communication with relevant stakeholders external to the MSSP.	IM-04.2
In accordance with contractual agreements between the client and MSSP, information shall be made available to the affected clients for final acknowledgment or, if applicable, as confirmation.	IM-04.3
The MSSP shall document the implemented measures after an information security incident related to the MSS has been handled.	IM-04.4
The MSSP shall make information on information security incidents and confirmed information security breaches related to the managed security service available to all affected clients.	IM-04.5

1921

13.14 Service Continuity

13.14.1 SC-01 Service Continuity Policies and Management Responsibility

13.14.1.1 Objective

Responsibilities are assigned inside the MSSP organisation to ensure that sufficient resources can be assigned to define and execute the service continuity plan for the managed security service and that related service continuity activities are supported.

13.14.1.2 Requirements

The MSSP shall define policies and procedures according to ISP-02 establishing the strategy and guidelines to ensure service continuity management for the managed security service.	SC-01.1
The MSSP shall name at least one member of the top management as the process owner of service continuity and emergency management for the MSS.	SC-01.2
The process owner shall be responsible for establishing the process within the company following the strategy as well as ensuring compliance with the guidelines. They are also responsible for ensuring that sufficient resources are made available for an effective process.	SC-01.3
The MSSP shall determine the service continuity requirements, taking into consideration relevant business requirements, service requirements, Service Agreement and risks	SC-01.4
The MSSP shall identify suppliers and subservice organisations whose disruption may affect delivery of the managed security service and shall assess, document and periodically review their continuity, recovery and resilience capabilities as part of service continuity planning activities.	SC-01.5

13.14.2 SC-02 Business Impact Analysis

13.14.2.1 Objective

The business continuity framework for the managed security service is based on a business impact analysis.

13.14.2.2 Requirements

The policies and procedures for business continuity management for the managed security service shall include the need to perform a business impact analysis to determine the impact of any malfunction of the managed security service.	SC-02.1
The business impact analysis resulting from these policies and procedures shall be reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes.	SC-02.2

13.14.3 SC-03 Service Continuity Plan

13.14.3.1 Objective

A service continuity framework for the managed security service is available, including a service continuity plan.

13.14.3.2 Requirements

The MSSP shall document and implement a service continuity plan to ensure continuity of the MSS, taking into account information security constraints and the results of the business impact analysis.	SC-03.1
The service continuity plan shall include: • criteria and responsibilities for invoking service continuity • procedures to be implemented in the event of a major loss of service • targets for service availability when the service continuity plan is invoked • service recovery requirements • procedures for returning to normal working conditions	SC-03.2
The service continuity plan and list of contacts shall be shared with the client and be accessible when access to the normal service location is prevented.	SC-03.3
The MSSP shall document the cause, impact and recovery when the service continuity plan has been invoked.	SC-03.5

13.14.4 SC-04 Service Continuity Tests and Exercises

13.14.4.1 Objective

The service continuity framework for the managed security service is tested on a regular basis.

13.14.4.2 Requirements

The service continuity plan for the managed security service shall be tested at regular intervals (at least once a year) or after an update.	SC-04.1
The tests shall be documented, and the results considered to review the service continuity plan and to define future operational continuity measures. The tests should involve clients and relevant third parties, such as subservice providers and suppliers.	SC-04.2

13.15 Compliance and Continuous Improvement

13.15.1 CCI-01 Identification of Applicable Compliance Requirements

13.15.1.1 Objective

The legal, regulatory and contractual requirements applicable to the information security and quality of the MSS are identified and documented.

13.15.1.2 Requirements

The MSSP shall determine and document the legal, regulatory and contractual requirements applicable to the information security and quality of the MSS.	CCI-01.1

13.15.2 CCI-02 Policy for Planning and Conducting Audits

13.15.2.1 Objective

Policies and procedures are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the managed security service.

13.15.2.2 Requirements

The MSSP shall define, document and implement policies and procedures, made in accordance with ISP-02, for planning and conducting audits that protect the operation of the MSS from interference by audits.	CCI-02.1
The audit activities shall be monitored and logged	CCI-02.2

13.15.3 CCI-03 Internal Audits

13.15.3.1 Objective

Subject matter experts regularly check the compliance of the internal controls to relevant and applicable legal, regulatory and contractual requirements related to the managed security service.

13.15.3.2 Requirements

The MSSP shall perform at regular intervals and at least annually internal audits by subject matter experts that ensure objectivity and the impartiality of the audit process, to check the compliance of the internal controls to the requirements defined in CCI-01, and to the applicable vertical service requirements at the targeted evaluation level.	CCI-03.1
Identified vulnerabilities and deviations shall be subject to risk assessment in accordance with the risk management procedure (cf. RM-01) and follow-up measures are defined and tracked (cf. OPS-05).	CCI-03.2
The MSSP shall document specifically deviations that are nonconformities from the applicable service requirements, including an assessment of their severity, and keep track of their remediation	CCI-03.3

13.15.4 CCI-04 Evaluation of the internal controls' performance

13.15.4.1 Objective

The top management of the MSSP shall be kept informed of the performance of the internal controls for the managed security service, to ensure its continued suitability, adequacy and effectiveness.

13.15.4.2 Requirements

The MSSP shall regularly inform its top management about the performance of the internal controls regarding information security and quality within the scope of the managed security service.	CCI-04.1
This information shall be included in the management review of the internal controls that is performed at least once a year.	CCI-04.2
The MSSP shall use this information to improve the information security and quality of the managed security service	CCI-04.3

14 HoLa – MSS Delivery process Requirements

Complementary to the Technical Security Requirements of Chapter 13, the MSS Delivery Process Requirements also apply uniformly across all MSSP service offerings and client engagements, providing a common foundation for security, resilience, and risk management within the delivery of the service.

The delivery of MSS is divided into 3 phases:

- **Setup phase:** Establishes foundational controls regarding organising the service, MSS agreements, scope, requirements, and service delivery arrangements before execution activities commence. This phase ensures mutual understanding between the MSSP and client regarding service objectives, constraints, responsibilities, and success criteria.

- **Execution Phase**: Encompasses the operational execution or delivery of the MSS according to the agreed scope and requirements. During this phase, the MSSP performs the core activities defined in each service profile as, for example: incident analysis, containment actions, threat hunting, or security monitoring, in coordination with the client.

- **Closure phase:** Ensures proper completion and closure of MSS activities, documentation of outcomes, knowledge transfer, and systematic improvement of future service delivery. This phase captures lessons learned, validates that the MSS objectives were met, and establishes a foundation for continuous improvement.

The requirements listed below cover the three phases of the delivery of MSS; they are built as follows:

- A cybersecurity objective to achieve
- Detailed requirements designed to achieve the security objective
- Evaluation guidelines

There are many cross-references between requirements and themes between this annex and the General requirements and the annexe(s) carrying on the vertical requirements. In some cases, requirements present in the horizontal baseline can be extended in the Vertical Layer according to the specificities of the delivered MSS.

14.1 Service Setup

The following requirements support the setup phase of the service. The scope encompasses the early exchanges of the MSSP with the client, the signature of the contract, and all interactions in between.

The requirements of the service setup phase depend on the specific client and the terms of the Service Agreement. These requirements can be extended, that is further developed and contextualised, in the vertical service profile according to the type of delivered MSS.

14.1.1 SET-01 Service suitability assessment

14.1.2 Objective

Assess whether the MSSP is able to perform the service based on the information provided by the client. In the case the MSSP intends to use subcontractors, this assessment shall also take place for the subcontractors.

14.1.3 Requirements

The MSSP shall define, for the MSS, the information necessary to enable the proper delivery of the service. All information hereafter is to be provided in written form.	SET-01.1
As a first step in establishing the service contract, the MSSP and the client shall establish an agreement on the scope of the MSS to be delivered, the objectives, criteria, and any specific arrangements for the service.	SET-01.2
These arrangements shall address as applicable: • Service level and performance requirements • Roles and responsibilities • Communication and escalation processes • Incident management and notification requirements • Access control and identity management • Information security and data protection requirements • Reporting and review mechanisms • Change and configuration management coordination • Technical integration requirements • Legal, regulatory, and compliance obligations • Business continuity and disaster recovery alignment • Service transition (onboarding/offboarding) • Confidentiality and information sharing restrictions • Third-party service dependencies	SET-01.3
The MSSP shall inform the client of its ability to provide the service as described in the agreement and report on its availability (number of experts, duration of the provided service).	SET-01.4
The MSSP shall provide the client with information on whether subcontractors will be involved in the delivery of the service, and if applicable which subcontractors will be involved, and for which part of the service.	SET-01.5
The MSSP shall make sure that the provided arrangements are consistent with its Service Agreement	SET-01.6

2010

2011 ### 14.1.4 SET-02 Service Agreement

2012 ### 14.1.5 Objective

2013 Define and contractually commit the MSSP in the Service Agreement to MSS scope and contracted
2014 service.

2015 ### 14.1.6 Requirements

The MSSP shall establish a Service Agreement with the client.	SET-02.1
The Service Agreement shall be signed by a legal representative of the MSSP and a legal representative of the client organisation, or by any person authorised to bind the MSSP and the client organisation.	SET-02.2
The Service Agreement shall include at minimum: • Description of the services to be provided, including the approach, objectives, scope; • Expected deliverables, including kick-off and closure documents; • Technical (tools and equipment) and organisational means deployed by the MSSP to deliver the service; • Lines of communication, for example phone numbers, e-mail addresses, emergency contact means, secure messaging platforms; • Requirements regarding skills and training, and where appropriate certifications, required from the MSSPs' employees; • Requirements regarding the verification of the background of the MSSPs' employees; • An obligation on MSSP to handle vulnerabilities that present a risk to the security of the network and information systems of the client; • Agreement and requirements if subcontracting is used (or for which part of the service); • Requirements regarding compliance of the MSSP to applicable legislation with regards to confidentiality of information; • Obligations on the MSSP at the termination of the contract, such as retrieval and disposal of the information obtained; • Information with regard to the migration of data following the termination of the contractual relationship, including the client's responsibilities and obligations to cooperate for the provision of the data.	SET-02.3

2016

14.2 Execution of the service

This phase involves the operational implementation and delivery of the MSS in line with the agreed scope and requirements.

In the HoLa, this phase includes general requirements concerning the start of the service and the service deployment plan as well as requirements about reporting to the client. These requirements don't depend on the service profile and can be applied to all MSS.

However, they are largely dependent on the Service Agreement and on client-specific needs.

14.2.1 EXE-01 Kick-off meeting

14.2.2 Objective

Once the contract is signed between the client and the MSSP, a kick-off meeting is held to officially launch the service

14.2.3 Requirements

The service shall not begin until after a formal opening meeting, during which the relevant representatives of the MSSP and the client confirm their agreement on all the terms of the service. The kick-off meeting agenda shall include at least topics on: • The scope, objective and general process of the provided MSS; • Expected deliverables and relative timeframe; • Agreement on communication methods and frequency of update calls and reporting meetings; • Contact persons; • Subcontracting.	EXE-01.1

14.2.4 EXE-02 Service Start

14.2.5 Objective

14.2.6 Initiation and execution of the service in the Operational Environment Requirements

The MSSP shall provide the client with a scoping note including: • The activities to be carried out; • Means of delivery; • The information to be collected in the context of the service; • The client-side personnel required for the proper delivery of the service by the MSSP; • Roadmap/timeline of the delivery of the service.	EXE-02.1
The scoping note shall be validated and signed by the client. The final decision and the responsibility of the scoping note belong to the client.	EXE-02.2
The MSSP shall plan the initiation and execution of the service in the operational environment, including dates, , deliverables and methods of deployment.	EXE-02.3

The MSSP shall take into account the change management policy (cf. CCM-01) and the change management policy of the client regarding the recording of any change.	EXE-02.4

14.2.7 EXE-03 Continuous service reporting

14.2.8 Objective

Manage changes affecting the service, and breaches of contractual objectives and report to the client.

14.2.9 Requirements

The MSSP shall provide timely notification and updates regarding major security, architectural, or operational changes that may affect the confidentiality, integrity, availability, or overall performance of the services provided to the client.	EXE-03.1
The MSSP shall document all changes in the service. Documentation shall also include rollback procedures	EXE-03.2
The MSSP shall perform a security and compliance impact assessment before applying any changes.	EXE-03.3
The changes shall be tested prior to initiation and execution of the service in the operational environment.	EXE-03.4
The MSSP shall monitor compliance with all contractual service objectives. Any failure to meet agreed service objectives shall be: • detected and recorded, • classified according to severity and impact, • escalated to authorized personnel, • communicated to the affected client • investigated through root cause analysis and • remediated through corrective actions.	EXE-03.5
Critical or repeated breaches of the contractual objectives shall trigger management review.	EXE-03.6
Records of breaches of objectives, investigations, communications, and remediation activities shall be retained in accordance with audit and regulatory requirements.	EXE-03.7
The MSSP shall organise regular meetings according to the procedure and cadence defined in the Service Agreement. These meetings shall include discussions on the following topics: • Progress of the service, with suitable visual support and metrics; • Any difficulties encountered; • New documentation or information needs; • Meetings required or held with stakeholders within customer organisation and relevant updates; • Any planned changes in the MSSP's team; • Any planned changes to the terms of the service. • Any breaches of the service contractual objectives	EXE-03.8

14.2.10 EXE-04 Incident notification to the client

14.2.11 Objective

Inform the client about incidents that affect the MSSP.

14.2.12 Requirements

The MSSP shall provide the client with documentation covering: a) the scope of incidents that the MSSP will report to the client; b) the level of disclosure of the detection of incidents and the associated responses; c) the target timeframe in which notifications of incidents will occur; d) the procedure for the notification of incidents (cf. IM-03, IM-04); e) contact information for the handling of issues relating to incidents; f) any remedies that can apply if certain incidents occur.	EXE-04.1
The MSSP shall notify the client of any incidents relevant to the client following the procedure provided in EXE-04.1	EXE-04.2

14.3 Service closure

The Service closure phase ensures the proper completion of MSS activities, including the documentation of results, knowledge transfer, and the structured enhancement of future service delivery. This phase captures service closure confirms that MSS objectives have been achieved, and details process on transition and secure data destruction or return.

14.3.1 CLS-01 Formal service closure

14.3.2 Objective

Ensure appropriate service closure documentation is created and a closure meeting is held with the customer.

14.3.3 Requirements

Upon completion of the MSS assignment, the MSSP shall provide the customer with formal closure documentation, that officially records the resolution and completion of all activities related to the service in accordance with the contract. The content of this documentation depends on the service profile and contractual specification (cf. C-RES-CR).	CLS-01.1
A closing meeting shall be organised with the customer following the delivery of the final service report. During the meeting, the MSSP shall provide the customer with an opportunity to share feedback on the service delivery.	CLS-01.2

14.3.4 CLS-02 Transition management

14.3.5 Objective

Ensure a secure, orderly and complete transition when the MSS is terminated, completed as planned or transferred to another provider or the customer.

14.3.6 Requirements

The MSSP and the customer shall agree on a handover plan with specific timelines	CLS-02.1
The handover plan shall include at least the following, when applicable: • Type, scope and format of the data the MSSP provides to the customer; • Transfer of documentation, artefacts; • Delivery methods of the data to the customer; • Secure handover of credentials, configurations; • Removal of access; • Risk assessment of transition if it applies; • Protection of sensitive information during transition; • Evidence of completion.	CLS-02.2

14.3.7 CLS-03 Destruction or return of assets and collected data

14.3.8 Objective

Customer data is securely deleted upon termination of the managed security service contract

14.3.9 Requirements

The MSSP shall implement procedures for deleting its customer's data upon termination of the managed security service contract in compliance with the contractual agreements between them.	CLS-03.1
The customer’s data deletion shall include all data, as well as related metadata and service derived data, such as data stored in data backups in accordance with the customer’s data retention policy and except as required by a valid court order.	CLS-03.2
The customer’s data deletion procedures shall prevent recovery by state-of-the-art forensic means.	CLS-03.3
The MSSP shall document the deletion of the customer’s data, including metadata and service derived data, in a way allowing the customer to track the deletion of its data.	CLS-03.4
The report of destruction or return shall clearly identify the information destroyed or returned, as well as the method of destruction or return used.	CLS-03.5
The destruction or return of assets and collected data shall be performed in a timely manner.	CLS-03.6

15 ANNEX III: VERTICAL LAYER

Explanatory note: This Annex establishes the specific technical, operational, and competence requirements tailored to the unique risk profiles of specific Managed Security Service domains. While the Horizontal Layer (Annex II) acts as a universal baseline, the Vertical Layers dictate the specific object of certification (the service profile) and establish the requirements necessary to achieve the 'substantial' or 'high' assurance levels. At the time of entry into force, this Annex contains the requirements for the Incident Management lifecycle, specifically limited to the Incident Response service profile.
For the purposes of this review cycle, the detailed technical security requirements and operational controls for this Layer have been structured as distinct, self-contained chapters. This structural separation is intended to clearly distinguish the highly prescriptive technical and methodological evaluation criteria from the core legal, administrative, and procedural framework of the Scheme. This format facilitates a focused technical review by the experts and ensures the technical controls can be evaluated as a cohesive, modular framework.

15.1 GENERAL PRINCIPLES OF VERTICAL LAYERS

1. The Vertical Layers requirements shall complement the baseline requirements of the Horizontal Layer (Annex II) by setting out precise criteria to address the distinctive characteristics and operational demands of specific Managed Security Services and related service profiles.

2. Additional service profiles on incident response lifecycle may be introduced through the update of the Scheme in accordance with CHAPTER IX: UPDATE OF THE SCHEME, where they fall within the MSS scope and mandate of this Scheme. Additional Vertical Layers should be requested by the commission and will be added as annex in this Scheme.

3. A Conformity Assessment Body (CAB) shall only evaluate the requirements of a specific service profile housed in this Annex after, or in conjunction with, the successful evaluation of the Horizontal Layer.

4. The assurance level of an EUMSS certificate (‘basic”, 'substantial' or 'high') shall be granted at the level of the certified service profile within this Annex. The evaluation of the service profile shall include the applicable Horizontal Layer requirements in Annex II and the applicable service-profile-specific requirements in this Annex.

5. Where this Annex defines assurance-level-specific requirements or reinforcements for a service profile, those requirements shall apply in addition to the Horizontal Layer baseline requirements and shall be assessed with the depth and rigour corresponding to the requested assurance level.

15.2 VERTICAL LAYER A: INCIDENT MANAGEMENT LIFECYCLE

1. This Vertical Layer covers the family of Managed Security Services designed to support the preparedness for, prevention, detection, analysis, mitigation of, response to, and recovery from cybersecurity incidents.

2. In this version of the Scheme, only Service Profile A.1 — Incident Response is available for certification. Future service profiles on incident management lifecycle shall become available for certification only once introduced through the update process defined in CHAPTER IX: UPDATE OF THE SCHEME and once the applicable requirements and evaluation approach have been defined.

3. The specific service profiles currently defined and available for certification under this Vertical Layer are:

   a) service profile A.1: Incident Response Services.

   b) [Reserved for future use: Governance and Preparation Services]

   c) [Reserved for future use: Protection Services]

   d) [Reserved for future use: Detection Services]

   e) [Reserved for future use: Recovery and Post-Incident Support]

15.3 SERVICE PROFILE A.1: INCIDENT RESPONSE

15.3.1 Scope and Definition, and Interrelationships

1. **The Incident Response service profile shall comprise a set of structured activities through which the Managed Security Service Provider (MSSP) carries out or provides assistance with the confirmation, analysis, containment, eradication, and reporting of information security incidents, in coordination with the client organisation.**

2. **While the Incident Response service profile interacts with adjacent domains (such as Digital Forensic Investigation, Crisis Management, Threat Hunting, Cyber Threat Intelligence, Security Monitoring, and Legal/Regulatory Reporting), the requirements herein establish the minimum necessary integration with these domains, which may be subject to separate future service profiles.**

15.3.2 Structure of Incident Response service profile Controls

To ensure structural consistency, the controls for the Incident Response Service Profile shall be built upon three distinct operational phases adapted from ISO 20700:2017:

a) Setup Phase (D-RES): Establishes foundational controls regarding Service Agreement, scope, expectations, and service delivery arrangements before execution activities commence.

b) Execution Phase (E-RES): Encompasses the operational execution and delivery of the incident response service according to the agreed scope.

c) Closure Phase (C-RES): Ensures proper completion, documentation of outcomes, knowledge transfer, and systematic improvement of future service delivery.

16. VeLa-IM: Incident Response Service Profile - Set-up Phase Requirements

16.1 Service Agreement Modalities and Statement of Work (SET-RES-SL)

Define and contractually commit the MSSP in the Service Agreement to incident response scope, resource availability, response time, and timelines specific to the incident response service.

16.1.1 Assurance Level Basic

16.1.1.1 Requirements

SET-RES-SL-01 (B)

In addition to elements listed in **HOLA-SET-02**, the Service Agreement shall specify the following:

(a) Service Scope and Modalities: The Service Agreement shall set out in writing a clear and complete description of the incident response services to be provided, including the approach, objectives, scope, and typical response activities.
(b) Service Tooling and Technologies: The Service Agreement shall identify the principal categories of tools and technologies to be used in the delivery of incident response activities or reference a dedicated section in the statement of work in which these are specified.
(c) Incident notification procedures: Where applicable, the Service Agreement shall provide the procedures to be followed by clients for reporting security incidents.
(d) Lines of communication: Where applicable, the Service Agreement shall describe which lines of communication are used for incident notification, among other; contact numbers, mail addresses, emergency contact lines, or secure messaging platforms.
(e) Points of Contact: Where applicable, the Service Agreement shall document designated individuals or functional roles within the MSSP, responsible for receiving and processing incident notifications, initiated by the client.
(f) Confidentiality Provisions: The Service Agreement shall include provisions governing the confidentiality of information collected, processed, or generated during incident response activities, including restrictions on disclosure to third parties.

Where circumstances require the immediate commencement of incident response services and such commencement necessitates access to the client's information systems prior to the conclusion of a Service Agreement, an interim agreement shall be established setting out the scope of work and the actions to be undertaken. The interim agreement referred to in this paragraph shall not replace the obligation to draft a Service Agreement at a subsequent stage.

Where the service is delivered under a pre-existing contractual arrangement, the elements specified in **SET-RES-SL-01 (B), SET-RES-SL-02 (B),** and **SET-RES-SL-03 (B)** may be addressed collectively across the existing contractual documentation, so as to avoid duplicating obligations already provided for therein. In such cases, a traceable mapping shall be maintained that identifies, for each element, the specific contractual provision in which it is addressed.

SET-RES-SL-02 (B)

In addition to **HOLA-SET-02**, the statement of work shall include, where applicable, the following generic Service Agreement with specific numeric targets:

(a) Time to Acknowledge: An initial confirmation shall be transmitted within a maximum timeframe defined in the Service Agreement, following receipt of an incident notification.
(b) Time to Response: Where the client authorises commencement of incident response activities, such activities are initiated within a committed timeframe as defined in the Service Agreement. Where commencement of response activities is dependent on client authorisation and such authorisation is not received within a timeframe defined in the Service Agreement, the MSSP shall document the authorisation request, the attempts made to obtain a response, and the time elapsed.
(c) Capacity Limitations: Where, at the time of incident notification, the MSSP lacks the necessary capacity to commence activities within the timeframes specified in points (a) and (b), it informs the client immediately, at minimum within a timeframe specified in the Service Agreement.

The Service Agreement of paragraph 1 should be appropriate to the availability model established pursuant to **SET-RES-SL-B-03 (B)**, ensuring consistency between availability commitments and response time obligations.

The Service Agreement shall specify, for each Service Agreement defined pursuant to paragraph 1, the precise measurement points from which compliance is determined. At a minimum, the Service Agreement shall define:

(a) The event that constitutes receipt of an incident notification for the purposes of §1(a) (Time to Acknowledge), which may include, but is not limited to, registration of a support ticket, receipt of an electronic notification through the agreed communication channel, or first verbal contact through the designated contact mechanisms;
(b) The event that constitutes commencement of response activities for the purposes of §1(b) (Time to Response);

The mechanism for recording the timestamps of each measurement event, such that compliance determination is based on auditable, system-generated records rather than retrospective estimation

SET-RES-SL-03 (B)

The statement of work shall, at minimum, specify the service availability model under which incident response services are provided.

The service availability model referred to in paragraph 1 shall clearly specify one of the following service delivery models, or a combination thereof:

(a) Business hours: Services are accessible during regular business hours, defined at minimum as weekdays (Monday to Friday) from 09:00 to 17:00 Central European Time (CET);
(b) Continuous availability: Services accessible on a continuous basis, twenty-four hours per day, seven days per week, including weekends and public holidays
(c) Capability-driven availability: Service availability is determined by resource capacity or staff availability within the MSSP.

The service availability model may specify different availability arrangements for different sub-services or support tiers. The Service Agreement shall specify the availability arrangement for each component of the service delivered.

The Service Agreement shall specify the procedures and contact mechanisms for requesting incident response services outside of the defined availability hours, where applicable.

16.1.2 Assurance Level Substantial

16.1.2.1 Requirements

For response services certified at assurance level substantial, the MSSP shall ensure that: **SET-RES-SL-01 (S)**

(a) The operational functionality of the lines of communication shall be tested, at minimum on an annual basis, and documented evidence shall be maintained demonstrating that designated points of contact can be reached through specified channels.

(b) The incident notification procedures shall be reviewed periodically, and updated, at minimum annually or following any significant change to the service delivery model.

For response services certified at assurance level substantial, the MSSP shall maintain documented evidence demonstrating compliance with the service agreement specified pursuant to **SET-RES-SL-02 (B)**. **SET-RES-SL-02 (S)**

Where compliance with the service agreement specified pursuant to **SET-RES-SL-02 (B)** is not met, the MSSP shall implement and maintain a documented procedure to record the deviation, identify the underlying cause, and implement corrective measures to address the non-conformity and to prevent recurrence.

For response services certified at assurance level substantial, the following shall be ensured; **SET-RES-SL-03 (S)**

(a) Availability testing: The availability model shall be tested, at minimum on an annual basis, to verify that incident response services remain accessible in accordance with the documented service availability model, with outcomes of such testing documented and retained.

(b) Service continuity: For services operating under a continuous availability model pursuant to **SET-RES-SL-03 (B) §2(b),** a service continuity plan shall be maintained, informed by a risk analysis of the incident response service, that identifies risks to uninterrupted service delivery and defines the measures to mitigate those risks, including provisions for backup personnel and failover procedures. Periodic tests of the service continuity plan shall be conducted and documented evidence of such tests retained. Where a real incident necessitates activation of continuity measures, the MSSP shall retain evidence demonstrating that the plan was executed.

16.1.3 Assurance Level High

16.1.3.1 Requirements

For response services certified at assurance level high, documented evidence shall be maintained demonstrating that the procedures specified pursuant to **SET-RES-SL-01 (B) §1 (c)** and **(d)** are consistently followed, as well as tested and reviewed where necessary in accordance with **SET-RES-SL-01 (S).** **SET-RES-SL-01 (H)**

For response services certified at assurance level high, the documented evidence shall be maintained demonstrating compliance with the service agreement specified pursuant to **SET-RES-SL-02 (B)** . **SET-RES-SL-02 (H)**

For response services certified at assurance level high, the MSSP shall implement and maintain a documented capacity-planning procedure, demonstrating that staffing logic is based on historical incident volumes and Service Agreement commitments, relative to the declared availability model, and that documented arrangements for flexible scaling exist.

For instances where response time commitments specified under **SET-RES-SL-02 (B)** are not met, the MSSP shall have a procedure to conduct and document a root cause analysis identifying the underlying causes and implementing corrective actions to prevent recurrence.	
For response services certified at assurance level high, documented evidence of staffing sufficiency and availability testing shall be maintained, pursuant to **SET-RES-SL-03 (S)**.	**SET-RES-SL-03 (H)**

2137

2138

16.2 Incident Classification Scale (SET-RES-SS)

Ensure that the MSS includes a documented basis for evaluating, categorising, and prioritising incidents, such that response actions, resource mobilisation, escalation thresholds, and service level commitments can be consistently determined and verified.

16.2.1 Assurance Level Basic

16.2.1.1 Requirements

SET-RES-SS-01 (B)

Where the service includes the classification of security events and incidents, the statement of work shall include an incident classification scale (ICS) that defines how typical security events and incidents are evaluated, documented, categorised, and prioritised.

The ICS shall define classification factors used to evaluate incident severity. At a minimum, the ICS shall address:

(a) Incident Type: Categorisation of the incident by nature – such as malware infection, ransomware, data breach, denial of service, unauthorised access, or insider threat – informed, where applicable, by established taxonomies.
(b) Technical Impact: Assessment of the compromise to the confidentiality, integrity, or availability of information systems
(c) Business Impact: Assessment of the expected or observed impairment to business operations, services, or capabilities, considering the duration of the disruption and estimated time to recovery.
(d) Scope of Compromise: Assessment of the expected number and type of affected assets, users, or organisational units.
(e) Data and Information Impact: Assessment of whether the compromise affects sensitive, personal, or classified data, including the nature and volume of data potentially exposed, exfiltrated, or rendered unavailable.

The ICS shall define at least three (3) classification levels that represent the overall assessment of incident severity by the MSSP based on the classification factors. Each level shall have at minimum:

(a) Name: Clear designation – e.g., Critical, High, Medium, Low; or Priority 1, Priority 2, Priority 3, Priority 4.
(b) Definition: Concise description of the characteristics and threshold criteria that distinguish this level from other levels.
(c) Typical Impact Description: Brief description of the typical adverse consequences associated with incidents at this level, as well as typical response actions.
(d) Typical Response: Description of the response actions, resource mobilisation and escalation steps associated with this level, mapped to the service level commitments established pursuant to **SET-RES-SL-02 (B)**

The ICS shall be accessible to all personnel involved in incident triage and response activities, including service delivery personnel and client staff.

16.2.2 Assurance Level Substantial

16.2.2.1 Requirements

SET-RES-SS-01 (S)

For response services certified at assurance level substantial, it shall be demonstrated that the ICS is specified to the context of the client and the specificities of the response engagement.

At minimum, such specification shall be:

(a) Conducted prior to the commencement of incident response activities and documented in the statement of work, unless circumstances require the immediate commencement of incident response services in accordance with **SET-RES-SL-01 (B) §2**;
(b) Based on information gathered from the client regarding their operational context, which shall include, where applicable and proportionate to the engagement:
- The architecture and principal components of the information systems in scope of the engagement;
- The location and hosting arrangements of the information systems in scope of the engagement;
- The means of monitoring and, where applicable, detecting security incidents of the client;
- The specific features, constraints, and interconnections of the information systems in scope of the engagement;
- The data categories processed and their sensitivity classification;

(c) Documented with sufficient detail to justify the assigned severity level;
(d) Recorded with a timestamp indicating when the severity determination was made.

Where the client maintains its own incident classification Scheme, paragraph 1 is considered fulfilled by aligning the service's incident classification scale with the client's Scheme. Where the client does not maintain such a Scheme, paragraph 1 can also be fulfilled by a classification approach based on industry-standard frameworks, subject to client confirmation before the commencement of incident response activities.

For response services certified at assurance level substantial, documented evidence of ICS classification determination shall be maintained, across a representative sample of incident case files.

16.2.3 Assurance Level High

16.2.3.1 Requirements

SET-RES-SS-01 (H)

For response services certified at assurance level high, documented evidence of all ICS determinations shall be maintained, including initial classifications and any subsequent revisions made during the engagement.

For each ICS determination or revision, the documented evidence shall include:

(a) The classification level assigned or revised;
(b) The timestamp at which the determination or revision was made;
(c) The identity of the individual responsible for the determination or revision;
(d) The rationale or justification for the classification assignment, including specific factors that influenced the decision;
(e) In the case of classification revisions, a clear explanation of why the initial determination required correction and what additional information prompted the change.

16.3 Incident Roles, Responsibilities and Authorities (SET-RES-RR)

Ensure the Service Agreement explicitly defines roles, responsibilities, and escalation authorities specific to incident response activities, with clear coordinator designation and approval paths.

16.3.1 Assurance Level Basic

16.3.1.1 Requirements

SET-RES-RR-01 (B)

The statement of work shall document a defined set of roles, responsibilities, and decision-making authority for each phase of the incident response engagement, clearly distinguishing them from general organisational roles defined in **HOLA HR05**.

An incident coordinator or engagement manager shall be appointed for each engagement, who shall be responsible to oversee the activities throughout the incident response service, until the engagement is closed in accordance with **C-RES-CR-01 (B) §3.** The incident coordinator shall establish an incident response team (IRT) composed of appropriately skilled and trusted analysts required for the incident response functions and services to be provided in accordance with **SET-RES-SL-01 (B).**

In cooperation with the client, a decision-making authority matrix shall be included in the statement of work, specifying which IRT roles have the authority to isolate, disconnect, or shut down client assets. In addition, a dedicated crisis management team or steering committee shall be established and documented in the statement of work, comprising decision-making personnel from both the client and the MSSP. The documentation shall specify the team's composition, the function and role of each member, and the terms governing its operation, including activation criteria, availability, and the decisions reserved to the team – in particular those requiring a combined client–MSSP authorisation under the decision-making authority matrix.

Staffing requirements referred to in this requirement shall be defined with reference to the European Cybersecurity Skills Framework (ECSF), an equivalent framework or standard, or a documented internal competency framework demonstrating equivalent coverage of roles, responsibilities, knowledge, skills, competences, and proficiency levels relevant to the managed security service.

SET-RES-RR-02 (B)

The statement of work shall establish and document emergency escalation paths that define when and how incident response activities are escalated beyond the authority of the incident coordinator, including escalation to:

(a) MSSP Management: for decisions requiring authorisation beyond the incident coordinator's authority, as defined in **SET-RES-RR-01 (B) §4.**
(b) Client management: for decisions requiring client authorisation, as defined in **SET-RES-SL-01 (B) §1** and **SET-RES-RR-01 (B) §4.**
(c) External parties: when incident scope or severity requires specialised support, as defined in the statement of work.
(d) Competent authorities: for decisions requiring notification and reporting according to applicable legislation, including – but not limited to – Directive (EU) 2022/2555 and Regulation 2022/2554.

For each escalation level, the following information shall be defined and documented, at minimum:

(a) Escalation authority: Who has the authority to make the escalation decision;
(b) Escalation recipients: Specific roles or named individuals to be notified;
(c) Escalation timeframes: Maximum time between recognising escalation trigger and completing notification;

(d) Decision-making authority at escalated level: What decisions the escalated party is authorised to make;
(e) Escalation documentation requirements: Mandatory information to include in escalation notification.

For services operating under a continuous availability model pursuant to **SET-RES-SL-03 (B) §2(b),** out-of-business continuity and escalation arrangements shall be documented in the statement of work, including: **SET-RES-RR-03 (B)**

(a) Call roster structure for out-of-business hours operations (primary, secondary, escalation)
(b) Contact methods and expected response times
(c) Emergency activation procedures for off-shift personnel, in case of surges in workload and major incidents requiring specific expert skills or an extended IRT

Moreover, the statement of work shall define the actions to be taken where a rostered individual does not acknowledge activation within a defined interval or cannot be reached, including: the escalation path to secondary and subsequent contacts; the alternative contact methods to be attempted; and the maximum interval or number of attempts before escalation to the next contact.

16.3.2 Assurance Level Substantial

16.3.2.1 Requirements

For response services certified at assurance level substantial, it shall be demonstrated, through documented evidence – such as procedures and roster management systems – that incident response roles remain clearly assigned, current, and contactable . **SET-RES-RR-01 (S)**

For response services certified at assurance level substantial, the MSSP shall implement and maintain a documented procedure governing leadership oversight of high-impact actions, specifying the actions requiring oversight, the role responsible for providing it, and the conditions under which oversight must be obtained prior to action. The procedure described in this paragraph shall apply, at minimum, to actions under **E-RES-CO** and **E-RES-BS**.

The MSSP shall develop and maintain a competency matrix that maps the capabilities of the IRT analysts to incident response service categories and complexity levels. The competency matrix shall be reviewed and updated at minimum annually or when significant changes occur to service offerings, analyst staffing, or required capabilities. The assignment of personnel to specific engagements shall be informed by the competency matrix established pursuant to this paragraph, considering the nature and complexity of the engagement.

For response services certified at assurance level substantial: **SET-RES-RR-02 (S)**

(a) The operational functionality of the emergency escalation paths pursuant to **SET-RES-RR-02 (B)** shall be tested, at minimum on a semi-annual basis, and documented evidence of escalation decisions shall be maintained.
(b) Emergency escalation paths shall be reviewed and, where necessary, updated – at minimum annually or following any significant change to the service delivery model.

16.3.1 Assurance Level High

16.3.1.1 Requirements

SET-RES-RR-01 (H)

For response services certified at assurance level high, the competency matrix maintained under **SET-RES-RR-01 (S) §3** shall, at minimum, include:

(a) Role Inventory: The set of IRT roles to which personnel are allocated for incident response engagements, distinguishing at least lead/coordinator and analyst-tier positions.

(b) Seniority Levels: Defined seniority or experience tiers per role, with each tier substantiated in objective terms such as years of relevant operational experience or prior responsibility on incident engagements of equivalent severity.

(c) Technical skill Domains: The technical disciplines relevant to the MSSP's service offerings, with the minimum tier of competence required for each domain per role.

The matrix and its supporting documentation shall be reviewed at least annually, or upon material changes to service offerings, IRT staffing, or required capabilities, by an HR function operating independently from engagement leadership.

17. VeLa-IM: Incident Response Service Profile - Execution Phase Requirements

17.1 Case Initiation, Analyst Assignment & Readiness (E-RES-CI)

Ensure that every incident response engagement is formally logged in a case management system by the MSSP, assigned to appropriately qualified personnel, and prepared for structured triage before substantive response activities begin.

17.1.1 Assurance Level Basic

17.1.1.1 Requirements

Upon receipt of a client incident notification, a formal case file shall be created within a case management system, capturing the following minimum elements: (a) Unique Case Identifier: A system-generated or manually assigned case identifier that enables reference to the engagement throughout its lifecycle. (b) Client Identification: Client name, contract reference number, and (where applicable) specific units, functions or locations affected by the incident. (c) Initial Contact Information: Timestamp of initial client notification, notification channel used and identity of notifying individual or system. (d) Reported Incident Summary: Initial incident description as reported by the client or detected by monitoring systems, including (i) the suspected or confirmed incident type, (ii) affected systems, services, or data categories (iii) and preliminary business impact statement or incident classification level (ICS). (e) Assignment Information: Identity of the incident coordinator and team assigned to the case, the assignment timestamp, and contact information. (f) Information Classification: The information classification level assigned to the case, which shall be consistent with the client's information classification Scheme where one exists, or, in its absence, the MSSP's own documented classification Scheme. The case record creation specified in paragraph 1 shall occur within the response time commitments established in the Service Agreement during service availability hours as defined pursuant to **SET-RES-SL-03 (B).** Where the client or a competent authority of a Member State provides a designated platform for the recording of incident information, the use of that platform by the MSSP shall be considered to satisfy paragraph 1, provided that the platform supports the capture of the minimum elements specified therein. Where the designated platform does not support one or more of the required elements, the MSSP shall document such elements through supplementary means.	**E-RES-CI-01 (B)**
The MSSP shall maintain documented evidence of the qualifications, competencies and relevant experience of personnel eligible for assignment to the incident response team, verified at onboarding and reviewed periodically. At the start of each incident response engagement, the incident coordinator shall staff the IRT from the qualified personnel pool	**E-RES-CI-02 (B)**

in line with a standard staffing plan, and shall adjust its composition as the incident type, severity and technical complexity become apparent.

Documented qualifications referred to in paragraph 1 may include evidence of:

(a) Relevant Professional Certifications: Current professional certifications demonstrating competence in incident response, digital forensics, malware analysis, threat intelligence, or related cybersecurity disciplines.

Or a combination of:

(b) Technical Training Documentation: Completion records for technical training courses relevant to incident response activities.

(c) Practical Experience Documentation: Documented operational experience demonstrating hands-on capability in incident response tasks.

. Staffing requirements referred to in this requirement shall be defined with reference to the European Cybersecurity Skills Framework (ECSF), an equivalent framework or standard, or a documented internal competency framework demonstrating equivalent coverage of roles, responsibilities, knowledge, skills, competences, and proficiency levels relevant to the managed security service.

2180 ### 17.1.2 Assurance Level Substantial

2181 #### 17.1.2.1 Requirements

For response services certified at assurance level substantial, it shall be demonstrated that case initiation records are complete and consistent across incident engagements by conducting periodic quality reviews. **E-RES-CI-01 (S)**

The quality review process referred to in paragraph 1 shall include, at minimum:

(a) Sample Selection: Selection of a representative sample of incident case records from a six (6) month evaluation period, across all severity levels, and across multiple analysts or teams, if applicable.

(b) Completeness Verification: Verification that all mandatory data elements specified pursuant to **E-RES-CI-01 (B) §1** are populated for each sampled case record.

(c) Timeliness Verification: Verification that case records were created within response time commitments as specified pursuant to **E-RES-CI-01 (B) §2**.

Findings from quality reviews shall be documented, identify any gaps or inconsistencies, and implement corrective actions where case initiation practices deviate from documented procedures.

For response services certified at assurance level substantial, the pre-engagement verification performed by the incident coordinator pursuant to **E-RES-CI-02 (B) §1** shall be documented in or alongside the case record, and shall be made available to the client upon request. **E-RES-CI-02 (S)**

2182 ### 17.1.3 Assurance Level High

2183 #### 17.1.3.1 Requirements

For response services certified at assurance level high, the MSSP shall implement a documented procedure to ensure that case initiation under **E-RES-CI-01 (B)** is performed completely and consistently for all incidents within scope, including periodic review of **E-RES-CI-01 (H)**

case-initiation outputs against the documented procedure and corrective action for deviations.	
For response services certified at assurance level high, the documentation maintained pursuant to **E-RES-CI-02 (S)** shall, for each engagement, identify the elements declared under SET-RES-RR-01 (H) to which the assignment decision is traceable, including a documented derogation by the incident coordinator together with the rationale therefor where the engagement necessitates a role/tier combination not standardly mapped.	**E-RES-CI-02 (H)**

2184

17.2 Triage Procedure & Initial Incident Assessment (E-RES-TR)

Ensure that the MSSP executes a structured triage process that rapidly assesses incident scope, determines severity classification, and establishes the evidential and analytical basis for subsequent containment, evidence collection, and forensic analysis decisions.

17.2.1 Assurance Level Basic

17.2.1.1 Requirements

E-RES-TR-01 (B)

Where the service includes the receipt of events or incident reports from the client – notably, for services operating under a continuous-availability model, or for services with client-initiated incident notification arrangements established under **SET-RES-SL-01 (B)** – a structured triage procedure shall be documented and implemented for sorting, categorising, correlating, prioritising and assigning incidents.

The triage procedure referred to in paragraph 1 shall specify, at a minimum:

(a) Initial Data Gathering Steps: Systematic process for collecting preliminary information from the client and available technical sources, which can include log files, alert data, monitoring outputs from client systems, preliminary network traffic captures or endpoint telemetry.
(b) Severity Determination Criteria: Application of the incident classification scale (ICS) established pursuant to **SET-RES-SS-01 (B)** to assign preliminary severity level, based on the actual or projected adverse consequences on the client.
(c) Scope Assessment: Structured approach to estimating incident boundaries and affected assets, including the identification of initial compromise, estimation of time between initial compromise and detection, identification of lateral movement paths and suspected affected systems, accounts, or data, where applicable.

The triage procedure shall be documented in the statement of work or dedicated operational procedures and made accessible to all personnel conducting triage activities. Triage outcomes — including the preliminary severity classification and scope assessment — shall be recorded in the case file established pursuant to **E-RES-CI-01 (B).** A separate triage report is not required, provided that the basis for the initial severity determination shall be traceable from the case record.

17.2.2 Assurance Level Substantial

17.2.2.1 Requirements

E-RES-TR-01 (S)

For response services certified at assurance level substantial, the MSSP shall ensure that the triage procedure documented under **E-RES-TR-01 (B)** is initiated and applied completely and consistently for all incoming events and incident reports falling within the scope of the response service.

Paragraph 1 shall be demonstrated, for a representative sample of cases over the evaluation period, through:

(a) Data Gathering Evidence: Documentation showing that initial data gathering steps were executed in accordance with the defined procedure.
(b) Severity Determination Documentation: Documented assessment of classification factors pursuant to **SET-RES-SS-01 (B),** recorded severity level assignment, rationale explaining severity determination and analyst identity and timestamp.
(c) Scope Assessment Documentation: Documented scope estimates including affected systems enumeration, identified compromise vectors or lateral movement paths, and preliminary containment boundary assessment.

(d) Escalation Decision Documentation: Where escalation criteria were met, evidence of escalation occurring, and where criteria were not met, confirmation that the incident remained within standard response processes

17.2.3 Assurance Level High

17.2.3.1 Requirements

E-RES-TR-01 (H)

For response services certified at assurance level high, in addition to the requirements at substantial, the MSSP shall implement a documented procedure to monitor triage timeliness and completeness, identify deviations from the triage procedure documented under **E-RES-TR-01 (B),** and apply corrective measures to address recurring deviations.

In addition to **E-RES-TR-01 (S) §2**, this evidence shall include:

(a) Evidence Preservation: Triage inputs have been preserved in case files or evidence repositories, timestamped at time of collection or receipt,

(b) Triage Decision Traceability: Triage conclusions are traced back to specific evidence items, decision rationale explicitly references supporting evidence and an independent reviewer can reach the same conclusions given access to preserved triage inputs.

(c) Audit Trail Completeness: Complete audit trail exists for triage process including, which analyst accessed triage inputs and when, what analysis actions were performed, which triage decisions were made with timestamps, who was the decision-maker, and any modifications to triage conclusions are provided with a motivation for the change.

17.3 Collection Procedures (E-RES-CP)

Ensure that, where the incident response engagement requires the collection of technical data and digital artefacts, the MSSP identifies the relevant collection points within the agreed scope and acquires the information needed to meet the service objectives.

17.3.1 Assurance Level Basic

17.3.1.1 Requirements

E-RES-CP-01 (B)

Where applicable, a collection procedure for the acquisition of technical data and digital artefacts during incident response engagements shall be documented and implemented, scoped to the systems and information within the agreed scope of the engagement as defined in the service agreement.

The collection procedure referred to in paragraph 1 shall identify, for the target information system within the agreed scope:

a) Collection points: The equipment and locations holding information relevant to the service delivery.
b) Information to be collected; In accordance with the service agreement and as relevant to the incident the collection procedure shall cover the (i) technical and configuration information — such as equipment configurations, file-system information, services and processes; (ii) event logs; (iii) network traffic; and (iv) the contents of volatile and non-volatile storage media.
c) Collection methods: The methods used by the MSSP as appropriate to each information type, such as log extraction, network capture, and disk or memory imaging;
d) Sequence of operations: The order of collection, taking account of data volatility.

The MSSP shall be capable of collecting, where relevant to the incident and within the scope of the services agreed in the service agreement, information from the categories of systems typically found in the target environment, such as: system components (e.g. backup and file servers); network components (e.g. proxy servers, DNS servers, routers, wireless access points); security components (e.g. firewalls, encryption devices, antivirus systems, network sensors); business systems (e.g. web servers, databases); administration workstations; and user workstations, including desktop, laptop and mobile devices.

The MSSP shall, in collaboration with the client, identify any potential impact of the collection operations on the target information system, in particular any risk to availability, before those operations are carried out.

17.3.2 Assurance Level Substantial

17.3.2.1 Requirements

E-RES-CP-01 (S)

For response services certified at assurance level substantial, it shall be demonstrated, for a representative sample of engagements over the evaluation period, that collection operations were carried out in accordance with the documented procedure.

The demonstration shall include:

a) Collection records Identifying the collection points, information types collected, methods used and the sequence followed in accordance with **E-RES-CP-01 (B)** and **E-RES-CC-01 (S)**
b) Impact assessment: Documentation of the availability-impact assessment carried out with the client pursuant to **E-RES-CP-01 (B) §4**.

17.3.3 Assurance Level High

17.3.3.1 Requirements

For response services certified at assurance level high, it shall be demonstrated that collection is complete and reproducible against preserved collection records, and in accordance with the requirements of **E-RES-CC-01 (H).** The demonstration shall support independent verification, including retrieval of collection records for selected engagements, confirmation that information required by the service objectives was collected from the relevant in-scope collection points, and – where feasible – verification or re-acquisition of a preserved item to confirm the recorded method and result.	**E-RES-CP-01 (H)**

17.4 Evidence Chain of Custody (E-RES-CC)

Ensure that, where the incident response engagement includes the collection, acquisition or preservation of digital evidence, the MSSP retains a documented chain of custody for that evidence so that it may support legal, regulatory or disciplinary proceedings or substantiate the response actions performed.

17.4.1 Assurance Level Basic

17.4.1.1 Requirements

E-RES-CC-01 (B)

Where the service includes the collection, acquisition or preservation of digital evidence, a chain of custody (CoC) procedure shall be documented and implemented in alignment with ISO/IEC 27037 or an equivalent recognised standard, governing the identification, collection, acquisition and preservation of digital evidence throughout the incident response lifecycle, from initial identification through final disposition.

The chain of custody procedure referred to in paragraph 1 shall specify:

(a) Evidence Integrity and Duplication: Items designated as evidence shall be preserved in their original state. Where forensic analysis is required, authorised copies shall be produced from the originals using validated duplication methods, and all analysis shall be performed exclusively on such copies.
(b) Evidence Labelling: Standardized labelling measures for all evidence items, including unique evidence identifier, evidence type and description, source system or location, collection date and time and collector identity.
(c) Custody Transfer Logging: Measures for documenting the transfer of evidence custody.
(d) Evidence Storage Measures: Specifications for secure evidence storage and retention period, per **C-RES-ED-01 (B) §2(a) and §2(b),** including procedures for evidence disposition upon case closure or retention expiry, in accordance with **C-RES-ED-01.**

The chain of custody procedure shall include template CoC forms or database schemas capturing all required information elements of paragraph 2.

17.4.2 Assurance Level Substantial

17.4.2.1 Requirements

E-RES-CC-01 (S)

For response services certified at assurance level substantial, it shall be demonstrated that evidence items collected during incident response engagements have an associated chain of custody record documenting its complete lifecycle.

Paragraph 1 shall be demonstrated, for a representative sample of cases, through:

(a) Initial Collection Documentation: CoC record showing collection timestamp, the identity of collecting analyst, source system or location from which evidence was obtained, evidence description and type.
(b) Custody Transfer Documentation: Transfer logs in case evidence custody were transferred, which can include information on the reason for transfer, and confirmation signatures or acknowledgments.
(c) Storage Location Tracking: Documented storage locations, access controls restricting access to authorised personnel and controls ensuring media integrity.

17.4.3 Assurance Level High

17.4.3.1 Requirements

E-RES-CC-02 (H)

For response services certified at assurance level high, evidence storage facilities and chain of custody records shall be accessible for independent audit and validation activities.

The accessibility confirmation shall verify:

(a) Physical Evidence Storage Access: Evaluators can physically access evidence storage facilities, observe physical security measures and inspect stored physical media.

(b) Digital Evidence Repository Access: Evaluators can access digital evidence repositories with read-only access permissions, navigate evidence directory structures or schemas, and retrieve evidence files for verification.

(c) Chain of Custody Documentation Access: CoC forms, transfer logs, and custody records are organised and readily retrievable by case ID or evidence ID and such CoC documentation is complete.

Any limitations on evidence accessibility shall be documented and an assessment shall be conducted whether such limitations impede adequate audit and validation.

17.5 Analysis of Digital Artefacts (E-RES-DE)

Ensure that, where the analysis of digital artefacts is within the scope of the incident response engagement, the MSSP conducts structured analysis of digital artefacts collected during incident response – including malware samples, network traffic artefacts, and other artefacts relevant to incident scoping – to determine attack vectors, attacker tactics and techniques, lateral movement paths, and indicators of compromise (IOCs) that support containment, eradication, and threat intelligence development.

17.5.1 Assurance Level Basic

17.5.1.1 Requirements

E-RES-DE-01 (B)

Where the service includes the examination or analysis of digital artefacts, analysis procedures for the examination and interpretation of digital evidence collected during incident response engagements, including evaluation of potential digital artefacts to support investigation findings, shall be documented and implemented.

Analysis procedures shall be documented for each analysis type relevant to incident response services offered, addressing at minimum: the analytical methodology to be followed, the validated analysis tools to be used in the analysis, safe handling measures for potentially malicious artefacts – including analysis environment isolation and contamination prevention measures – and documentation measures for analysis findings and any limitations encountered.

Analysis procedures shall require that analysis activities address the key investigative questions appropriate to the incident, including determination of the attack vector, scope of compromise, data or systems affected, and indicators of compromise that can support detection of similar activity.

17.5.2 Assurance Level Substantial

17.5.2.1 Requirements

E-RES-DE-01 (S)

For response services certified at assurance level substantial, it shall be demonstrated that analysis activities produce documented analytical outputs that support investigation findings and response decisions.

The analytical output demonstration shall include, for a representative sample of incidents:

(a) Malware Capabilities Summary: For incidents involving malware, analysis reports, documenting: malware family identification, capabilities observed or identified, file system and registry modifications made by malware, network communications, persistence mechanisms, and anti-analysis or evasion techniques detected. Where available, malware families and attacker TTPs identified during analysis shall be mapped to established threat intelligence frameworks

(b) Indicators of Compromise (IOCs) Extracted: Structured IOC documentation, including file hashes for malicious files, malicious IP addresses and domains contacted, URLs used for malware download or C2 communication, file paths and registry keys created by malware and (where applicable) YARA rules or other detection signatures developed from analysis. IOCs should be documented in machine-readable formats (STIX, OpenIOC, CSV).

(c) Network Activity Patterns: For incidents with significant network component, analysis reports, documenting: network patterns, lateral movement paths, protocol abuse techniques, data exfiltration volumes and destinations, and timeline of network activity.

(d) Lateral Movement and Persistence Indicators: Documentation of attacker persistence and movement, including compromised accounts identified, credential dumping or theft evidence, lateral movement techniques observed, privilege escalation methods, and additional systems compromised from initial entry point.

Analysis outputs shall be incorporated into incident case files and (where applicable) provided to clients in closure reports or interim status updates, per **C-RES-CR-02 (B) §1(a).**

E-RES-DE-02 (S)

For response services certified at assurance level substantial, documented evidence shall be maintained to confirm that analytical conclusions are supported by technical evidence and that analysts followed documented analysis procedures.

Paragraph 1 shall be demonstrated, for a representative sample of cases over the evaluation period, through:

(a) Evidence-Based Conclusions: Analytical findings and conclusions are directly traceable to specific evidence artifacts, conclusions are supported by multiple corroborating evidence sources where available, and speculative statements are clearly identified as hypotheses requiring further investigation.
(b) Procedural Compliance: Analysis procedures documented pursuant to E-RES-DE-01 (B) §2 were followed, appropriate analysis tools were used for evidence type, and any procedural deviations are documented with justification.
(c) Peer Review Evidence: For complex or high-severity incidents, evidence that analysis findings underwent peer review or technical validation by senior analyst or subject matter expert, in accordance with the QMS of the MSSP, with reviewer sign-off or feedback incorporated into final analysis

17.5.3 Assurance Level High

17.5.3.1 Requirements

E-RES-DE-01 (H)

For response services certified at assurance level high, the analysis of digital artefacts can be re-executed on preserved evidence samples to verify that technical findings derived from digital artefacts and indicators, are reproducible and accurate to the extent possible taken into consideration the nature of the evidence, tooling, and analytical environment. .

The analysis re-execution validation shall:

(a) Evidence Sample Selection: Select preserved evidence samples suitable for re-analysis.
(b) Independent Analysis: Using the same analysis procedures and tools documented pursuant to E-RES-DE-01 (B) §2, independently re-perform analysis on selected evidence samples.
(c) Finding Comparison: Compare independent technical analysis findings against original MSSP technical analysis findings.
(d) Reproducibility Assessment: Confirm the extent to which key technical findings derived from digital artefacts and indicators are reproducible, assess whether any discrepancies exist, and investigate causes of any significant discrepancies. Where a finding cannot be reproduced, the reasons shall be documented.

Where re-execution validation identifies reproducibility issues, analytical methodology gaps, or tool accuracy concerns, such findings shall be documented and corrective actions recommended.

17.6 Containment Procedures & Client Authorisation (E-RES-CO)

The MSSP shall maintain pre-defined and client-approved containment playbooks that specify authorized containment actions by category and severity. During an active incident and where so provided by the service agreement, the MSSP shall execute containment actions in accordance with pre-approved playbooks without requiring real-time client authorization, except where actions would materially impact client business operations or system availability beyond thresholds defined in the service agreement. In such cases, the MSSP shall notify the client and seek expedited approval while implementing interim protective measures.

17.6.1 Assurance Level Basic

17.6.1.1 Requirements

E-RES-CO-01 (B)

Containment procedures shall be documented and implemented, which set out the criteria and steps for selecting, authorising and - where the agreed service scope includes execution - executing containment actions, taking account of the incident type and the intended duration of the containment measure.

Containment procedures shall define:

(a) Authorisation Measures: Delineation of containment actions by authorisation level, distinguishing between pre-approved actions that may be executed without explicit client approval, actions requiring explicit client approval prior to execution, and emergency actions that may be executed in exigent circumstances with retroactive client notification. Escalation paths for obtaining approvals shall be specified in accordance with **SET-RES-RR-02 (B)**

(b) Rollback and Recovery Provisions: For each category of containment actions, procedures shall be defined for reversing containment measures when the incident is resolved and validating that systems and services are restored to operational status.

(c) Evidence Preservation: In accordance with **E-RES-CC-01 (B),** measures to ensure that necessary data for analysis is collected before making any changes on the client systems, including capture of volatile data before containment actions that may alter system state. Where operational necessity would require containment before preservation, such deviation shall be documented.

Approval mechanisms for (§2) may include, but are not limited to, written confirmation, recorded verbal authorisation, or authenticated electronic acknowledgment. Where circumstances require immediate action and the designated client approver is not reachable within the timeframes established in the Service Agreement, the MSSP shall document the attempts made to obtain authorisation, proceed with the minimum containment actions necessary to prevent further harm, and obtain retroactive confirmation at the earliest opportunity.

In accordance with **SET-RES-SL-01 (B) §1** and **SET-RES-RR-02 (B),** containment procedures shall include communication measures specifying the information to be provided to the client before, during, and after containment execution.

Where containment capabilities are delivered through client capabilities or platforms or reside within the client's IT environment, the service may rely on those capabilities provided that the statement of work documents the containment actions available through each channel and the authorisation workflow for invoking them.

17.6.2 Assurance Level Substantial

17.6.2.1 Requirements

For response services certified at assurance level substantial, it shall be demonstrated that containment decisions are documented with supporting rationale, client authorisation is obtained where required, and containment actions are timestamped for audit purposes. **E-RES-CO-01 (S)**

The containment documentation shall include, for a representative sample of incidents:

(a) Containment Decision Documentation: For each containment action taken, documentation showing the specific containment action that was executed, the timestamp of containment action execution, the analyst executing containment action, and the rationale for the containment decision.
(b) Authorisation Records: Where containment actions required client approval per documented procedures: evidence of approval request, the client approval obtained with timestamp, and the identity of client representative providing approval. For pre-approved actions, documentation confirming that containment actions fall within pre-approved category.
(c) Effectiveness Assessment: Post-containment assessment of whether containment was effective, which can include evidence that the malicious activity ceased after containment, that systems were successfully isolated, or access revoked, and any containment bypasses or failures requiring additional containment actions.
(d) Rollback Documentation: Where containment actions were reversed after incident resolution, documentation showing the rollback timestamp, the authorisation, the validation that systems/services are functioning normally post-rollback, and the confirmation that rollback did not re-introduce vulnerability or risk.

The representative sample shall include incidents of varying severity levels and containment complexity.

For response services certified at assurance level substantial, containment actions shall align with authorised scope decisions and requests for out-of-scope actions were appropriately escalated for approval. **E-RES-CO-02 (S)**

The case file review shall verify:

(a) Scope Alignment: Containment actions taken were within the scope of actions authorised in the Service Agreement or dedicated annex, systems impacted by containment were within authorised asset scope, and actions taken align with client's acceptable impact tolerance.
(b) Out-of-Scope Handling: Where circumstances required containment actions outside normal authorised scope, evidence that out-of-scope actions were identified as requiring additional approval, escalated to appropriate authority per **SET-RES-RR-02 (B),** approved before execution (or executed under emergency authority with immediate post-notification), and documented with justification.

17.6.3 Assurance Level High

17.6.3.1 Requirements

For response services certified at assurance level high, containment decision records and authorisation audit trails shall be immutable and cannot be retrospectively altered without detection. **E-RES-CO-01 (H)**

The verification shall confirm:

(a) Immutable Logging: Containment actions are logged to systems that prevent modification of historical records, or containment logs are cryptographically signed or hashed to enable detection of modifications, or containment logs are replicated to independent secure log storage that maintains audit trail integrity.
(b) Timestamp Integrity: Timestamps on containment actions and authorisation records are reliable and cannot be backdated, and timestamp tampering would be detectable through cross-correlation with other audit sources.
(c) Authorization Record Integrity: Client approval emails, ticket approvals, or other authorisation records are preserved with integrity protection, and authorization records are retained in tamper-evident storage preventing deletion or modification.
(d) Audit Trail Completeness: Complete audit trail exists for containment activities, including: who initiated containment actions, when actions were executed, what authorisation was obtained, what systems were affected, and any changes to containment status.

17.7 Boundary-Safe Containment (E-RES-BS)

Ensure that containment actions by the MSSP are executed within authorised boundaries with technical requirements preventing inadvertent impact to out-of-scope systems, unauthorised containment actions, or destruction of forensic evidence through misconfigured or improperly targeted containment commands.

17.7.1 Assurance Level Basic

17.7.1.1 Requirements

E-RES-BS-01 (B)

Where the service includes the direct execution of containment, eradication or recovery actions on client systems (as distinct from advisory-only delivery in which the client performs the actions), boundary-safe execution procedures shall be documented and implemented, ensuring that containment actions are executed only on in-scope, authorised systems and that out-of-scope systems are protected from inadvertent containment impact.

Boundary-safe execution procedures shall ensure that in-scope systems are positively identified before containment actions are executed, out-of-scope systems are protected from inadvertent impact, and authorisation is tied to the identified in-scope system.

Boundary-safe procedures shall be incorporated into analyst training and standard operating procedures, with emphasis on preventing scope violations that can cause client business disruption or legal liability.

17.7.2 Assurance Level Substantial

17.7.2.1 Requirements

E-RES-BS-01 (S)

For response services certified at assurance level substantial, the use of privileged access management (PAM) systems or of equivalent technical measures that restrict analyst access to the authorised scope and log all containment actions in sufficient detail for post-event review. Such equivalent measures need not take the form of a dedicated PAM system: the native access-control and audit capabilities of the MSSP's service delivery platform may be accepted, provided they satisfy both of those conditions.

The demonstration shall include:

(a) PAM/Access Control Architecture: Documentation of access control architecture, including PAM system or equivalent access control platform in use, how analyst access is mediated through access controls, scope restrictions enforced by access controls, and credential management.
(b) Access Logging: Comprehensive logging of analyst access and actions, including access request and approval logs, session logs showing systems accessed and duration and audit trail suitable for detecting unauthorised access attempts or scope violations.
(c) Scope Enforcement Evidence: For a representative sample of containment actions, evidence that analysts accessing systems had authorised access, systems accessed were within authorised scope for that analyst/engagement, containment actions were logged with sufficient detail and no unauthorised out-of-scope access occurred (or where violations occurred, that they were detected and investigated).

17.8 Eradication Procedures (E-RES-ER)

Ensure that the MSSP develops and executes comprehensive eradication plans that systematically eliminate attacker presence, remove malware, neutralize persistence mechanisms, revoke compromised credentials, and address exploited vulnerabilities based on forensic analysis findings and threat intelligence.

17.8.1 Assurance Level Basic

17.8.1.1 Requirements

E-RES-ER-01 (B)

Eradication procedures shall be documented and implemented, specifying systematic approaches for the elimination of components of the incident, including malicious code, compromised accounts and passwords, or other compromised systems and information.

Eradication procedures shall address, at minimum, the following activities relevant to incident response services offered:

(a) Removal of malicious elements from all potentially affected systems, including on-premises and cloud-hosted environments, systems that are or will be restored from backups. This includes systems that are to be restored using hard disk reformatting, media wiping tools, firmware flashing, or physical destruction where warranted.
(b) Neutralization of persistence mechanisms established by the attacker.
(c) Credential reset and revocation for compromised accounts, prioritising privileged and widely-scoped accounts.
(d) Remediation or mitigation of exploited vulnerabilities, including patching, configuration hardening, and access control improvements as appropriate. Where warranted by the incident analysis, case-specific hardening recommendations shall be documented, addressing the particular attack vectors and systemic weaknesses identified during the engagement.
(e) Eradication verification: systematic validation that eradication is complete, using indicator-of-compromise sweeps, behavioural monitoring for a defined period, and system integrity checks against known-good baselines.

Where the statement of work does not include direct eradication actions, the MSSP shall advise the client on required actions and shall have insight into both the method used and the results, sufficient to give an expert opinion on whether the environment is deemed safe.

17.8.2 Assurance Level Substantial

17.8.2.1 Requirements

E-RES-ER-01 (S)

For response services certified at assurance level substantial, it shall be demonstrated that eradication plans are incident-specific, derived from forensic analysis findings, and incorporate platform-specific or threat-specific runbooks where applicable.

The eradication plan specificity demonstration shall include, for a representative sample of incidents:

(a) Analysis-Driven Planning: Eradication plan explicitly references forensic analysis findings, including IOCs from malware analysis per **E-RES-DE-01 (S) §2,** persistence mechanisms identified through forensic examination, compromised credentials identified in memory dumps or credential theft artifacts, and exploited vulnerabilities identified through root cause analysis.
(b) Tailored Eradication Steps: Eradication plans are customised to specific incident characteristics rather than generic incident types.

(c) Runbook Application: Where applicable, incident-specific eradication plan incorporates relevant runbooks, including specific runbooks selected based on affected systems, threat-specific runbooks selected based on attacker TTP or malware family, and runbook adaptations are documented where standard runbooks do not fully address incident specifics.
(d) Client Coordination: Eradication plans are developed in coordination with client, including client input on eradication prioritisation, client approval for high-impact eradication actions, and client resource allocation.

The representative sample shall include incidents of varying complexity to assess eradication planning adaptability.

E-RES-ER-02 (S)

For response services certified at assurance level substantial, documented evidence shall be maintained demonstrating that eradication plans were executed as documented and that deviations from planned eradication activities are recorded and justified.

Paragraph 1 shall be demonstrated, for a representative sample of cases over the evaluation period, through:

(a) Plan Execution: Documented eradication plan was followed, including eradication steps executed in documented sequence, all planned eradication actions were completed, and execution timestamps documented for each major eradication activity.
(b) Deviation Documentation: Where eradication execution deviated from the runbook, deviations are documented including the nature of deviation, the reason for deviation, the approver of deviation, and an assessment of whether deviation increased residual risk.
(c) Completeness Verification: Evidence that eradication verification activities documented pursuant to E-RES-ER-01 (B) were performed, including that IOC sweeps were conducted with results documented, system integrity checks were performed with findings documented, and overall eradication completeness assessment.
(d) Issue Escalation: Where eradication encountered significant obstacles or failures, issues were appropriately escalated and addressed through escalation per **SET-RES-RR-02 (B).**

For response services certified at assurance level substantial, a process to assess eradication execution quality shall be established to identify common deviation patterns and evaluate whether deviations indicate procedural gaps requiring correction.

2270

17.9 Eradication Sign-Off & Recovery Handoff (E-RES-ES)

Formally conclude the eradication phase with documented sign-off by the client, explicit acknowledgment of residual risks or limitations, and structured handoff to client recovery teams or managed security service (MSS) recovery services to ensure continuity between eradication and recovery phases.

17.9.1 Assurance Level Basic

17.9.1.1 Requirements

E-RES-ES-01 (B)

A formal sign-off process for eradication completion shall be documented and implemented, establishing clear transition point between eradication phase and recovery phase

The eradication sign-off process shall include:

(a) Eradication Completion Criteria: Defined criteria that must be met before eradication is considered complete, including all identified malware removed, all identified persistence mechanisms neutralized, all compromised credentials reset or revoked, all exploited vulnerabilities remediated or compensating controls implemented, post-eradication monitoring period completed without detecting residual attacker activity, and affected systems validated for integrity and readiness for recovery, and a defined post-incident observation period has been completed to confirm that no residual malicious activity persists

(b) Residual Risk Acknowledgment: Explicit documentation and client acknowledgment of any residual risks or uncertainties, which can include known limitations in eradication, uncertainty areas where complete eradication cannot be guaranteed, systems that are not yet eradicated, and recommended ongoing vigilance measures.

(c) Recovery Transition Planning: Handoff planning specifying responsibilities for recovery phase, which can include the recovery activities will be performed by MSSP (if so provided by the Service Agreement), which recovery activities are the client's responsibility, dependencies between MSSP eradication and client recovery, and possible coordination mechanisms between the client and the MSSP during recovery.

(d) Formal Client Approval: Explicit client acknowledgment and approval to transition from eradication to recovery, per **SET-RES-RR-01 (B) §4** and **SET-RES-SL-01 (B) §1.** The form of client approval shall be proportionate to the circumstances and may include recorded verbal confirmation where written approval cannot be obtained within operationally acceptable timeframes.

The eradication sign-off process may be integrated with broader incident closure procedures where eradication is the final technical phase before incident closure or may be a distinct milestone for incidents where eradication and recovery are separate phases with different teams or timelines.

17.9.2 Assurance Level Substantial

17.9.2.1 Requirements

E-RES-ES-01 (S)

For response services certified at assurance level substantial, eradication sign-off documentation shall include comprehensive summary of eradication activities, explicit residual uncertainty statements, recommendations for recovery, and formal client approval.

The sign-off documentation shall include, for a representative sample of incidents:

(a) Eradication Activity Summary: Comprehensive summary of eradication actions taken, including malware removal activities, persistence mechanism neutralization, credential resets, vulnerability remediation, and eradication timeline.

(b) Residual Uncertainty Statement: Explicit statement of limitations, uncertainties, or known residual risks, including detailed descriptions where eradication may be incomplete, an inventory of systems not yet eradicated, any limitations in vulnerability remediation, and ongoing monitoring recommendations for the client.

(c) Recovery Recommendations: Specific guidance for recovery phase, including recommendations on recovery approach, recovery prioritisation, recovery validation, and post-recovery hardening.

The representative sample shall include incidents with varying complexity and outcomes.

18. VeLa-IM: Incident Response Service Profile - Closure Phase Requirements

18.1 Incident Closure Reporting & Documentation (C-RES-CR)

Produce comprehensive closure documentation that captures incident timeline, root cause analysis, response effectiveness, remediation actions, and lessons learned to support both client understanding and allow for service improvement.

18.1.1 Assurance Level Basic

18.1.1.1 Requirements

C-RES-CR-01 (B)

In addition to **HOLA-CLS-01** and upon completion of each incident response engagement, an incident closure report shall be produced. The end of incident recovery shall be declared based on agreed criteria with the client, and incident-related documentation shall be completed.

The incident closure report referred to in paragraph 1 shall contain, at a minimum, the following elements:

(a) Executive Summary: An overview that provides non-technical stakeholders with information on the incident significance, business impact, key findings, and recommendations.

(b) Incident Timeline: A chronological account of significant events, including: the initial notification, acknowledgment and initial response, major investigative milestones, containment actions and timestamps, eradication activities and recovery completion.

(c) Root Cause Analysis (RCA): a technical analysis, conducted in accordance with the provider's documented RCA methodology, as agreed with the client, that identifies the fundamental cause(s) that enabled the incident to occur; the analysis draws on the information and evidence gathered during incident handling and on other relevant sources, including interviews with involved personnel, distinguishes the root cause(s) from contributing factors and symptoms, and summarises the findings, which inform the corrective and preventive actions.

(d) Scope of Compromise: Documentation of the extent of the incident's impact, which can include an overview of affected systems or applications, the number of user accounts or endpoints compromised, an overview of data that was accessed, modified, or exfiltrated.

(e) Remediation Actions Taken: Detailed documentation of response activities performed, which can include the immediate containment measures that were implemented, eradication steps that were performed, as well as recovery actions and compensating measures implemented pending permanent remediation.

(f) Lessons Learned: A summary of key insights derived from the incident, including process gaps identified, detection or response shortcomings, and recommended improvements to reduce the likelihood or impact of similar incidents.

(g) Evidence Package: The MSSP shall have the capability to deliver a structured evidence package compiled in accordance with the Statement of Work. At

minimum, the package shall comprise references to the evidence artefacts collected during the engagement and, where applicable, the chain of custody records associated with them; additional components hall be included where the Statement of Work so specifies.

The incident closure report referred to in paragraph 1 shall contain provisions for the formal closure of the service, requesting client acknowledgment that: all contractually committed activities have been completed to satisfaction, outstanding actions (if any) are clearly documented with ownership and timelines, and the client accepts formal closure of the incident response engagement.

Where the client does not provide the acknowledgment referred to above within the timeframe specified in the statement of work, or contests that the activities have been completed, the MSSP shall:

(a) Record the client's specific objections, outstanding items, or grounds for non-acknowledgment in the case file, together with the date of notification and the identity of the client representative;
(b) Determine, in cooperation with the client, the actions necessary to address the objections or outstanding items, the parties responsible for those actions, and the timeline for resolution; and
(c) Where the matter cannot be resolved at the engagement level, escalate it in accordance with the escalation paths established under **SET-RES-RR-02 (B)**

Notwithstanding paragraph 3 and 4, exceptional circumstances may arise in which a client does not want to receive an incident closure report. In those specific cases, the motivation of the client shall be sufficiently motivated and documented.

If so, required by the Service Agreement, the incident closure report shall also include the following elements: **C-RES-CR-02 (B)**

(a) Indicators of Compromise (IOCs): A comprehensive listing of technical indicators discovered during investigation. IOCs shall be documented in structured formats suitable for integration into security monitoring tools. Where regulatory or confidentiality restrictions apply, the MSSP shall document the restriction and deliver IOCs through an alternative secure channel agreed with the client.
(b) Recommendations for Prevention: Specific, prioritised recommendations to prevent recurrence of similar incidents. Recommendations shall be organised by priority, based on the risk reduction potential and implementation feasibility.
(c) Recovery Validation: Documentation demonstrating that affected systems and services have been restored to secure operational state and client confirmation of satisfactory recovery.
(d) Notification to Authorities: Where the incident analysis reveals indicators of state-sponsored or state-affiliated threat activity, or where other circumstances may give rise to notification obligations under applicable national or European legislation, the closure report shall document the MSSP's assessment of whether such notification obligations may apply to the client, the basis for that assessment, and the recommendation made to the client regarding the relevant reporting timelines and channels. The closure report shall confirm that the decision to notify, and the act of notification, rests with the client.

18.1.2 Assurance Level Substantial

18.1.2.1 Requirements

C-RES-CR-01 (S)

For response services certified at assurance level substantial, incident closure reports defined under **C-RES-CR-01 (B)** shall, before being delivered to the client, be reviewed and approved by a reviewer with sufficient competence and independence from the case author.

The review process shall verify, at minimum:

(a) The completeness of all required sections pursuant to **C-RES-CR-01 (B)** and **C-RES-CR-02 (B);**
(b) The technical accuracy of findings and analysis;
(c) The appropriateness and feasibility of recommendations;
(d) The removal of any confidential or unredacted client information not suitable for inclusion.

The review process under paragraphs 1 and 2 may be performed within existing quality-management arrangements subject to HOLA. The MSSP is not required to establish a separate quality-assurance programme to fulfil this requirement.

18.1.3 Assurance Level High

18.1.3.1 Requirements

C-RES-CR-01 (H)

For response services certified at assurance level high, documented evidence shall be maintained demonstrating sustained quality assurance performance, including evidence of quality review completion for all incident closure reports produced during this period.

For response services certified at assurance level high, the evaluator shall assess the quality and analytical rigour of root cause analyses across a representative sample of incident closure reports, verifying that:

(a) Evidence-Based Conclusions: Root cause determinations are directly supported by forensic evidence, log analysis, or other investigative artifacts documented in the report.
(b) Alternative Hypotheses: The analysis demonstrates consideration of alternative explanations for observed indicators and documents the rationale for ruling out alternative root causes.
(c) Contributing Factors Analysis: The report identifies and analyses contributing factors beyond the immediate technical cause, including process gaps, human factors, or systemic issues that enabled or exacerbated the incident.
(d) Lessons-Learned Integration: The closure report includes a dedicated lessons-learned section that identifies specific, actionable improvements derived from the incident, including detection gaps, response process shortcomings, and recommendations for the client's security posture. The lessons-learned section shall be consistent with the post-incident review conducted pursuant to **C-RES-LL-01**.

18.2 Remediation Planning (C-RES-RP)

Ensure that, where the MSSP supports the client in remediating an incident, it does so in a steering capacity – i.e, planning, coordinating and tracking remediation activity against objectives agreed with the client - while responsibility for remediation decisions and their execution remains with the client, unless otherwise defined in the service agreement.

18.2.1 Assurance Level Basic

18.2.1.1 Requirements

C-RES-RP-01 (B)

Where the service includes support to remediation, a remediation planning and steering procedure shall be documented and implemented by the MSSP.
The procedure referred to in paragraph 2 shall provide for a remediation plan that includes, at minimum:

a) Objectives: Records the strategic remediation objectives agreed with the client's management and decomposes each into operational objectives and then technical actions;
b) Assignment: Assigns each technical action to one or more identified members of the MSSP or the client.
c) Continuity alignment: Incorporates the client's business continuity and disaster recovery objectives within the planning, when such information has been provided by the client.
d) Register: Maintains a remediation action register recording, for each action, the date and (where applicable) time, a description of the action, and any trade-offs made together with the party that authorised them.

If so provided by the service agreement, the MSSP shall coordinate the teams contributing to remediation – at the client, at the MSSP, and any third parties – to support the implementation of the plan.

18.2.2 Assurance Level Substantial

18.2.2.1 Requirements

C-RES-RP-01 (S)

For response services certified at assurance level substantial, it shall be demonstrated, for a representative sample of engagements, that remediation was steered in accordance with the documented procedure.

The demonstration shall include: a remediation plan showing that actions were assigned and remained traceable. If so provided by the service agreement, it shall also include a maintained action register per E-RES-RP-01 (B) §2, evidence of coordination among contributing teams and a periodic assessment of whether technical remediation objectives remain aligned with the defined strategic objectives.

18.3 Lessons-Learned Documentation & Process Improvement (C-RES-LL)

Capture actionable lessons learned from each incident response engagement and systematically feed identified improvements into service delivery procedures, personnel training, tool capabilities, and security requirements to prevent recurrence and enhance overall incident response effectiveness.

18.3.1 Assurance Level Basic

18.3.1.1 Requirements

In addition to **HOLA-CLS-01**, the statement of work shall define how insights from incident response engagements are captured, analysed, and translated into improvements to incident management, information security measures, and information security risk assessment and management review results The lessons learned process referred to in paragraph 1 shall specify, at a minimum the procedures for conducting structured reviews following incident closure. The lessons-learned process shall be documented in a dedicated procedure document and made accessible to all personnel involved in incident response activities.	**C-RES-LL-01 (B)**

18.3.2 Assurance Level Substantial

18.3.2.1 Requirements

For response services certified at assurance level substantial, the lessons learned process referred to in C-RES-LL-01 (B) shall include: (a) Improvement Identification Methodology: A structured approach to identifying improvement opportunities. (b) Improvement Integration Mechanism: The process shall define how identified improvements are fed into relevant organisational processes within the MSSP and recommendations for client security measure improvements, if so, required by the closure report.	**C-RES-LL-01 (S)**
For response services certified at assurance level substantial, it shall be demonstrated that identified improvement actions are tracked to completion through a documented tracking mechanism. The tracking mechanism referred to in paragraph 1 shall include: (a) Registry: A centralised registry or tracking system documenting all improvement actions, prioritised according to a documented rationale and with realistic target implementation dates. (b) Status Monitoring: Improvement action status shall be reviewed at defined intervals to track progress toward completion, reassess priorities as needed, and escalate overdue actions to management. (c) Verification: Upon completion of an improvement action, evidence shall be documented demonstrating implementation. For response services certified at assurance level substantial, documented evidence shall be maintained, demonstrating improvement action tracking, including evidence that actions are assigned, monitored, and progressed toward completion.	**C-RES-LL-02 (S)**

18.3.3 Assurance Level High

18.3.3.1 Requirements

For response services certified at assurance level high, documented evidence shall be maintained demonstrating improvement action tracking, including evidence that actions are assigned, monitored, and progressed toward completion. The lessons learned documentation process shall be reviewed and updated at predefined points, which shall include, at minimum, following each qualifying incident and at a defined recurring interval.	**C-RES-LL-01 (H)**

18.4 Evidence Disposition & Archival (C-RES-ED)

Ensure that incident response evidence is retained for legally and contractually required periods, securely archived with integrity protection and accessibility assurance, and disposed of securely and completely according to documented policy when retention requirements expire.

18.4.1 Assurance Level Basic

18.4.1.1 Requirements

C-RES-ED-01 (B)

In addition to **HOLA-CLS-03**, the statement of work shall define specific evidence retention and disposition procedures, governing the lifecycle management of incident response evidence from identification and collection through final disposition, ensuring that evidence is preserved by means of enforcing chain of custody.

The evidence retention and disposition procedures referred to in paragraph 1 shall specify:

(a) Minimum Retention Periods: The statement of work shall define minimum retention periods for incident response evidence, derived from the client's contractual requirements set out in the Service Agreement and from applicable national and European legal and regulatory obligations. Where these requirements conflict, the retention period shall be set proportionately, giving full effect to applicable national and European legislation..

(b) Archival Storage Requirements: The statement of work shall specify requirements for secure archival storage of incident evidence. Where the evidence may be required for legal, regulatory, or disciplinary proceedings, archival storage shall preserve the evidence in a manner that supports its admissibility, including integrity protection.

Secure Destruction Methods: The statement of work shall define approved methods for secure destruction of evidence upon retention expiry. The evidence retention and disposition procedures shall be documented in dedicated evidence handling procedures and made accessible to all personnel involved in incident response and evidence management activities.

18.4.2 Assurance Level Substantial

18.4.2.1 Requirements

C-RES-ED-01 (S)

For response services certified at assurance level substantial, it shall be demonstrated that evidence retention complies with documented retention policies and that destruction follows secure destruction procedures.

The requirements of paragraph 1 shall be demonstrated through:

(a) Retention Compliance Audit: Periodic audits (at minimum annually) shall be conducted to verify that incident evidence is being retained for required periods, evidence approaching retention expiry is identified and processed according to procedures, and no evidence has been destroyed prematurely.

(b) Destruction Records: Where evidence has been destroyed during the evaluation period, detailed destruction records shall be maintained that verify destruction in accordance with the procedure of **C-RES-ED-01 (B) §2(c)**

For response services certified at assurance level substantial, documented evidence shall be maintained, demonstrating retention compliance and secure destruction (if applicable).

18.4.3 Assurance Level High

18.4.3.1 Requirements

C-RES-ED-01 (H)

For response services certified at assurance level high, documented evidence shall be maintained, demonstrating retention compliance and secure destruction (if applicable).

The requirements of paragraph 1 shall be demonstrated through:

(a) Evidence Lifecycle Documentation: For a representative sample of archived evidence, complete lifecycle records of evidence shall exist.

(b) Premature Destruction Measures: Measures are implemented, that prevent evidence destruction before retention period expiry without proper authorisation and unauthorised premature destruction did not occur during the evaluation period.

For response services certified at assurance level high, documented evidence shall be maintained, demonstrating that archived evidence remains accessible and verifiable throughout the retention period.

The evidence accessibility and integrity verification referred to in paragraph 3 shall be demonstrated through:

(a) Retrieval Testing: Periodic testing (at minimum annually) is conducted to verify that archived evidence can be successfully retrieved from archival storage within operationally reasonable timeframes.

(b) Integrity Verification: Retrieved evidence is subjected to cryptographic integrity verification and verification results are documented. Any integrity verification failures shall trigger investigation and corrective action.

(c) Storage Monitoring: For evidence stored on physical media, media degradation monitoring is implemented and proactive measures are taken to ensure evidence remains accessible and intact.

19 ANNEX IV: ASSURANCE CONTINUITY AND CERTIFICATION LIFECYCLE

19.1 ASSURANCE CONTINUITY AND CERTIFICATION LIFECYCLE

Explanatory note: This annex defines the measures to put in place in order to guarantee that certified Managed Security Services remain in conformity with the Scheme requirements after the initial issuance of the certificate. It defines a 3-year certification lifecycle, detailing the surveillance, recertification, and special evaluation activities to be performed by the Conformity Assessment Body.

1. The objective of assurance continuity is to ensure the ongoing validity of the demonstration of fulfilment of the Scheme requirements, which shall cover three aspects:

    a) the continuous secure operation of the certified Managed Security Service over time;

    b) changes in the certified Managed Security Service infrastructure, processes, or scope over time;

    c) changes in the threat environment over time.

2. To maintain the validity of an EUMSS certificate, which shall not exceed a maximum period of 3 years, the Scheme requires three different types of evaluations: annual surveillance evaluations, recertification evaluations, and special evaluations.

19.2 ANNUAL SURVEILLANCE EVALUATIONS

Explanatory note: surveillance evaluation is an ISMS concept to handle revisions during the period of validity of the certificate.

1. The purpose of the annual surveillance evaluation is to confirm the continued conformity of the certified Managed Security Service, and, for certificates at the assurance levels 'substantial' or 'high', to confirm its continued operational effectiveness. At least one surveillance evaluation shall be performed every year.

2. During the annual surveillance evaluation for any EUMSS certificate and for all assurance levels, including 'basic', the evaluation team of the Conformity Assessment Body shall undertake evaluation activities consisting of at least a review of the technical documentation, or substitute evaluation activities with equivalent effect (such as structured interviews with key personnel), to

    a) perform an analysis of the minor changes made to the Managed Security Service since the last evaluation;

    b) for assurance level 'substantial' and 'high': verify the existence and implementation of modified security controls;

    c) select and evaluate a subset of requirements where observations or non-conformities were identified in previous evaluations.

3. For a Managed Security Service certified at the assurance level 'substantial' or 'high', in addition to the documentation and design review required in paragraph 2, the Conformity Assessment Body shall evaluate the ongoing operating effectiveness of the service. During the annual surveillance evaluation, the evaluation team shall:

    a) evaluate the operating effectiveness of a subset of the controls, explicitly including all controls related to incident management, vulnerability management, and change management;

    b) review the internal records of the provider to ensure that any vulnerabilities or incidents that did not reach the "materiality" threshold were adequately handled in accordance with the provider's internal procedures

4. For a Managed Security Service certified at the assurance level 'high', the annual surveillance evaluation shall additionally include targeted vulnerability assessments and a review of the service's continued resistance to skilled attackers. The focus of the surveillance activities should be on new or emerging risks, recent incidents reports in the market or recent trends in the legal or technical environment, minor changes in the service delivery or infrastructure of the provider along with a randomly chosen part of the ISMS of the provider. Where the annual review identifies major changes to the service delivery model or significant modifications to critical procedural, manual, and physical workflows—the Conformity Assessment Body shall perform targeted evaluation activities focused on these additions (along with a suspension of the certificate until these unnotified major changes have been assessed). Where relevant for IT systems, this shall include differential penetration testing. However, where the service relies heavily on physical, manual, or procedural activities and such technical testing is not appropriate, the Conformity Assessment

Body shall perform substitute evaluation activities with equivalent effect (such as process simulations, table-top exercises, or physical security inspections) to ensure the service's overall resistance to state-of-the-art attacks remains intact.

19.3 RECERTIFICATION EVALUATION

Explanatory note: Recertification needs to cover the effectiveness of all controls. If in surveillance evaluations the effectiveness assessment has only been performed on a minimal set of requirements, then the work to be done for recertification may be very significant. It is therefore recommended to carefully select the activities to be performed during these surveillance evaluations, in order to avoid deferring potential difficulties to the recertification evaluation

1. The purpose of the recertification evaluation is to confirm the continued conformity and effectiveness of the Managed Security Service as a whole to allow for the renewal of the certificate.

2. A recertification evaluation shall be planned and conducted to evaluate the continued fulfilment of all evaluation criteria before the 3-year expiry date of the current certificate.

3. The recertification activity shall include a review of the previous annual surveillance evaluation reports and the performance of the service over the most recent certification cycle, and shall be conducted using appropriate evaluation methods aligned with those defined for initial certification.

4. For the ‘basic’ assurance level, the certificate holder shall perform an updated internal audit and self-assessment against the requirements of the Scheme and provide the resulting reports to the Conformity Assessment Body.

5. Specific requirements for 'High' assurance**:** For a Managed Security Service certified at the 'high' assurance level, the recertification evaluation shall mandate a full, comprehensive penetration test of the IT systems and infrastructure used to provide the service (or substitute activities where relevant), establishing a new baseline of resistance against state-of-the-art cyberattacks.

   Where vulnerability assessment and/or penetration testing activities are considered necessary by the conformity assessment body, the MSSP shall provide the conformity assessment body with the results of such activities, including the scope, methodology, identified findings, and remediation status where applicable. The conformity assessment body shall review and evaluate such evidence as part of the recertification assessment.

6. Following a successful recertification evaluation, the Conformity Assessment Body shall issue a new certificate with a new end date, which shall not be more than 3 years after the recertification decision.

19.4 SPECIAL EVALUATION

Explanatory note: The objective of a special evaluation is to perform an evaluation focused on the measures taken by the provider of the service to fulfil the requirements for which nonconformities have been detected or on the changes made to their service or to their control framework.

1. The objective of a special evaluation is to perform a targeted assessment focused on the measures taken by the certificate holder to fulfil requirements following a major event, a material non-conformity, a major/material change within the service delivery of the provider or a critical security breach.

2. A special evaluation shall be performed when decided by the Conformity Assessment Body, particularly following a notification by the provider.

3. During a special evaluation, the evaluation team shall:

    a) perform an analysis of the material changes or non-conformities identified;

    b) assess the suitability of the design of the affected controls and the remediation plan submitted by the provider;

    c) evaluate the operating effectiveness of the remediated or updated controls to ensure the service remains in conformity or returns to conformity with the required assurance level.

19.5 SURVEILLANCE SCHEDULE

Explanatory note: This section specifies the frequencies of surveillance in accordance with their type.

1. A special evaluation shall be performed when decided by the Conformity Assessment Body, following a notification of major changes, material events, or a major non-conformity.

2. In accordance with section EVALUATION CRITERIA AND METHODS FOR MSS of this Scheme, after each special and annual evaluation, a review and certification decision shall take place, with the following possible outcomes:

    a) continuation of the certificate, without any change;

    b) suspension of the certificate, accompanied by guidance for customers of the provider and requirements for the provider to fix the identified non-conformities within a defined timeline;

    c) withdrawal of the certificate in the case of non-conformities that cannot be addressed;

    d) update of the certificate with a new scope, but retaining the original end date.

19.6 PARAMETERS FOR MAINTENANCE PROCESSES

Explanatory note: maintenance will be triggered according to the nature of the changes and events, that are defined in this section.

1. To ensure the agile delivery of Managed Security Services while maintaining certification integrity, providers shall establish a distinction between minor events and major (material) events:

a) Minor changes and events: Routine operational changes, standard patching, and non-critical vulnerabilities shall be handled directly through the internal change and vulnerability management processes defined by the provider. These do not require immediate notification to the Conformity Assessment Body. The effectiveness of these internal processes shall be evaluated by the Conformity Assessment Body during the annual surveillance evaluation.

b) Major changes and material events: Major architectural changes, the integration of substantial new third-party delivery components, critical vulnerabilities, or actual security breaches compromising the service infrastructure constitute material events; they shall be notified to the Conformity Assessment Body without undue delay, triggering a review and potentially a special evaluation or the suspension of the certificate.

20 ANNEX V: LIST OF INFORMATION REQUIRED UPON APPLICATION FOR CERTIFICATION IF SUBSERVICES ARE DEPLOYED

20.1 LIST OF INFORMATION REQUIRED UPON APPLICATION FOR CERTIFICATION IF SUBSERVICES ARE DEPLOYED

Explanatory note: This Annex lists all the information that the certificate holders need to make available at the beginning of the certification process. This is needed because TS 18072 expects the evaluator to list assurance documentation for every relevant subservice and assess its relevance, including validity period, framework, mapping and issuer competence/impartiality.

The applicant shall provide a description of all relevant subservices used for the design, operation, management or delivery of the Managed Security Service submitted for certification, including:

(a) the identity of the subservice organisation, where disclosure is not legally restricted;

(b) the role of the subservice in the certified service;

(c) whether the subservice is provided by an internal or external subservice organisation;

(d) whether the inclusive method or the carve-out method is proposed for the subservice;

(e) the requirements of this Scheme for which the applicant relies, in whole or in part, on the subservice;

(f) the assurance documentation available for the subservice, including its scope, period of validity or period covered, assurance level where applicable, and issuing organisation;

(g) any known non-conformities, deviations, exceptions or corrective actions affecting controls of the subservice relied upon for conformity with this Scheme.

21 ANNEX VI: CONTENT OF A CERTIFICATE

21.1 CONTENT OF A CERTIFICATE

Explanatory note: This Annex lists the required content of EUMSS certificates.

1. An EUMSS certificate shall at least contain:

(a) a unique identifier allocated by the Conformity Assessment Body issuing the certificate of conformity;
(b) information related to the certified Managed Security Service including the following:
(1) name of the Managed Security Service;
(2) the specific service profile of the Managed Security Service (e.g., Incident Response);
(3) the assurance level;
(4) name, address and contact information of the holder of the EUMSS certificate;
(5) link to the website of the holder of the EUMSS certificate where publicly available information is provided, including the supplementary cybersecurity information for the certified MSS in accordance with Article 55 of Regulation (EU) 2019/881 (Cybersecurity Act).
(c) Information related to the evaluation and certification of the Managed Security Service, including the following:
(1) name, address and contact information of the Conformity Assessment Body that issued the certificate of conformity;
(2) where applicable, name of the subcontractors that contributed to the evaluation;
(3) name of the responsible national cybersecurity certification authority;
(4) references to Regulation (EU) 2019/881 (Cybersecurity Act) and to the present Scheme;
(5) a reference to the certification report associated with the certificate;
(6) a reference to the certification assessment report associated with the certificate;
(7) the single applicable assurance level in accordance with section 1.4 ASSURANCE LEVELS.
(8) a reference to the standards used for the evaluation, including their versions; The certificate shall identify, where applicable, the evaluation method applied to each relevant subservice used by the certified Managed Security Service, distinguishing between the inclusive method and the carve-out method.
(9) the date of issuance of the certificate;
(10) the period of validity of the certificate.
(d) the mark and label associated with the certificate in accordance with section MARK AND LABEL.

2. The information shall be provided in an official language of the EU, and an English translation shall be available within the certificate.

22 ANNEX VII: CONTENT OF A CERTIFICATION REPORT

22.1 CONTENT OF A CERTIFICATION REPORT

Explanatory note: This Annex lists the required content of a certification report (to be made publicly available together with the certificate).

1. On the basis of the findings resulting from the evaluation, the Conformity Assessment Body establishes a certification report to be published together with the corresponding EUMSS certificate.

2. The certification report is the source of detailed and practical information about the Managed Security Service and shall therefore include all publicly available and sharable information of relevance to users and interested parties. Publicly available and sharable information can be referenced by the certification report.

3. The certification report shall at least contain the following sections:

(a) executive summary;
(b) identification of the Managed Security Service;
(c) description of the Managed Security Service and intended use;
(d) the assurance level;
(e) the supplementary cybersecurity information to be made publicly available, in accordance with Article 55 of Regulation (EU) 2019/881 (Cybersecurity Act);
(f) a summary of the evaluation plan, including a summary of the results of the evaluation; Where the certified Managed Security Service relies on subservices, the certification report shall include a summary of the dependency analysis performed by the Conformity Assessment Body. The summary shall identify:

I. the relevant subservices considered in the evaluation;
II. the evaluation method applied to each subservice, distinguishing between the inclusive method and the carve-out method;
III. the assurance documentation relied upon for each subservice;
IV. any assumptions made regarding controls implemented by subservice organisations;
V. any limitations, missing information, non-conformities, deviations or exceptions related to subservices that affected the evaluation conclusion or certification decision;
VI. the conclusion of the Conformity Assessment Body regarding the adequacy of the assurance obtained for the relevant subservices.

(g) summary of the review and certification decision;
(h) when available, the mark or label associated to the Scheme;
(i) bibliography.

4. The executive summary shall be a brief summary of the entire certification report. The executive summary shall provide a clear and concise overview of the evaluation results and shall include the following information:

(a) name of the certified Managed Security Service, enumeration of the service profile(s) that are part of the evaluation and the Managed Security Service;
(b) the name of the Conformity Assessment Body issuing the certificate and, where applicable, the list of subcontractors who contributed to the evaluation;
(c) completion date of evaluation;
(d) reference to all partial evaluation report(s) established by the evaluation team;
(e) brief description of the certification report results, including:
(1) the name and version of all components evaluated in the context of the certification;
(2) the name and version of all components that have been evaluated prior to the certification, together with a reference to their certificate or other relevant assurance information;
(3) assumptions about the operating environments;
(4) special configuration requirements;
(5) disclaimer(s).

5. The evaluated Managed Security Service shall be clearly identified, including the following information:

(a) the name and version number of the evaluated Managed Security Service;
(b) the service profile of the Managed Security Service (e.g. Incident Response);
(d) name and contact information of the holder of the EUMSS certificate;
(e) link to the website of the holder of the EUMSS certificate where publicly available information is provided, including the supplementary cybersecurity information for the certified Managed Security Service in accordance with Article 55 of Regulation (EU) 2019/881 (Cybersecurity Act).

6. The description of the Managed Security Service shall include:

(a) a description of the Managed Security Service architecture, including required hardware, software and subservices when applicable;
(b) a description of the Managed Security Services security policies that are relevant for the users, which may refer to the description of the information security management system component and of other components that define such security policies and processes;
(c) a description of the Managed Security Services control framework, including a mapping between the controls, the elements in which they are implemented and the risks identified on the Managed Security Service;
(d) the list of additional assumptions and requirements to the operating environments of the certified Managed Security Service for the compliant provision of the Managed Security Service;

7. A complete listing of the supplementary cybersecurity information to be made publicly available in accordance with Article 55 of Regulation (EU) 2019/881 (Cybersecurity Act) shall be provided. All relevant documentation shall be denoted by their version numbers.

8. The summary of the evaluation shall include:

(a) a description of the evaluation plan, including a list of the evaluation activities;
(b) the results of the evaluation activities;

(c) in the case of a maintenance evaluation, a summary of the nonconformities encountered since the previous evaluation.

9. The summary of the review and certification decision shall include the following information:

(a) confirmation of the attained assurance level as referred to in Article 52 in Regulation (EU) 2019/881 (Cybersecurity Act);

(b) detailed description of the assurance requirements, as well as the details of how the Managed Security Service meets each of them;

(c) date of issuance and period of validity of the certificate;

(d) unique identifier of the certificate.

10. The mark or label associated to the EUMSS may be inserted the certification report in accordance with the rules and procedures laid down in section MARK AND LABEL.

11. The bibliography section shall include references to all documents used in the compilation of the certification report. That information shall include the following:

(a) the security evaluation criteria, state-of-the-art documents and further relevant specifications used and their version;
(b) technical reference documentation;
(c) further documentation used in the evaluation effort.

12. In order to guarantee the reproducibility of the evaluation, all documentation referred to has to be uniquely identified with the proper release date, and proper version number.

13. Prior to publication of the Certification Report, the Conformity Assessment Body shall perform a documented exposure assessment to determine whether the disclosed technical, architectural, operational or security-related information could reasonably facilitate hostile intelligence gathering, attack planning, attack surface mapping or other forms of adversarial exploitation. Such assessment should consider the potential effects of AI-assisted OSINT, large-scale information aggregation, publicly available information correlation and hybrid threat activities. Where elevated exposure risks are identified, the Conformity Assessment Body shall consider appropriate abstraction, aggregation, redaction or other disclosure-limiting measures while preserving the transparency objectives of the Scheme.

14. The certification report shall be made available at least in English. Where the certification report is initially established in another official language of the Member State where the Conformity Assessment Body is established, an English translation of the certification report shall be provided alongside it to facilitate publication on the dedicated European cybersecurity certification website.

23 ANNEX VIII: CONTENT OF A CERTIFICATION ASSESSMENT REPORT

23.1 CONTENT OF A CERTIFICATION ASSESSMENT REPORT

Explanatory note: This Annex lists the required content of the confidential certification assessment report. Because this Scheme certifies the Managed Security Service and not the provider as an organisation, the report focuses strictly on the certified service, while necessarily including supporting information about the Managed Security Service Provider (MSSP). Unlike the public certification report, this document contains highly sensitive technical and operational data regarding the service delivery. It is strictly restricted to the conformity assessment body, the applicant, and the relevant national cybersecurity certification authority (NCCA) for supervisory purposes.

1. The certification assessment report shall be drafted in an official language of the Union agreed upon between the applicant and the Conformity Assessment Body, and accepted by the relevant national cybersecurity certification authority.

Given the cross-border nature of Managed Security Services, and to facilitate efficient certification processes, potential mutual assistance between national authorities, and peer assessments, the use of English as the language for the certification assessment report is strongly recommended, though not mandatory.

2. The certification assessment report shall contain all the information required for the public certification report set out in ANNEX VII: CONTENT OF A CERTIFICATION REPORT.

3. In addition, due to the detailed nature of the assessment, the certification assessment report shall contain the following extra requirements and confidential information:

(a) Evaluator Details and Signatures:

1. the names of the natural persons (evaluators, auditors, technical experts) involved by the conformity assessment body in performing the conformity assessment and their respective roles;

2. at least one qualified electronic signature identifying the name and title of the responsible person authorised to adopt the certification decision on behalf of the Conformity Assessment Body;

(b) Exhaustive Internal Documentation: An exhaustive, version-controlled list of all public and sensitive internal documents that were evaluated as part of the scope of the conformity assessment of the service, including at least:

1. templates of the Service Agreement and terms and conditions governing the service delivery to clients;

2. the results of the internal risk assessment and threat modelling related specifically to the service provision;

3. the list of internal operational playbooks, standard operating procedures (SOPs), and policies supporting the effective provision of the certified service;

4. the specific service platforms, sensors, software tools, and hardware devices used by the provider to securely deliver the Managed Security Service, as applicable;

    1. Detailed Evaluation Methodologies & Pentesting Justification: A detailed description of the evaluation methodologies employed, including: the rationale behind the selection of evaluation activities, the sampling methodology used across different client environments, and the specific test and simulation procedures utilized in accordance with CEN/CENELEC TS 18072;

    2. for assurance level high: where technical penetration testing is deemed not relevant or appropriate (e.g., because the certified service relies exclusively on procedural, manual, or physical activities), a formal justification for its omission and a detailed methodological description of the substitute evaluation activities with equivalent effect (such as process simulations, table-top exercises, social engineering assessments, or physical security inspections) undertaken to assess the service's resistance to skilled attackers;

    3. Where the Managed Security Service relies on subservices, the certification assessment report shall document the dependency analysis performed for each relevant subservice. The documentation shall include at least:

        I. the identified subservices and their role in the Managed Security Service;

        II. whether each subservice was evaluated using the inclusive method or the carve-out method;

        III. the requirements of this Scheme for which the applicant relies, in whole or in part, on the subservice; the assurance documentation used for the analysis, including its type, scope, period of validity or period covered, applicable framework, issuing organisation and, where available, mapping to the requirements of this Scheme;

        IV. the assessment of the competence and impartiality of the organisation that issued the assurance documentation, unless the subservice is certified under a Certification Scheme recognised for the purposes of this Scheme;

        V. the assumptions made regarding controls implemented by subservice organisations;

        VI. the conclusions regarding the adequacy of the assurance obtained;

        VII. any limitations, missing information, non-conformities, deviations, exceptions, corrective actions or compensating controls identified in relation to the subservice;

VIII. the impact of those elements on the evaluation conclusion and certification decision.

(d) Comprehensive Control Framework & Dependency Analysis: A detailed description of the control framework of the service.

(e) Detailed Activity Results & Operating Effectiveness: A comprehensive assessment of the evaluation activities performed by the evaluator, detailing:

1. the exact timing and duration of the activities to prove "operating effectiveness" over time (e.g., covering 6 months for 'substantial' or 12 months for 'high');

2. the specific, unredacted results of the activities, including identified vulnerabilities, technical penetration testing results, or the detailed outcomes of the approved substitute evaluation activities (e.g., physical breach simulations), accompanied by technical rationales;

(f) Non-Conformity and Remediation Tracking:

1. for every minor non-conformity identified, the agreed plan of corrective actions and their timescale;

2. for every major/material non-conformity, the exact date when corrective actions were completed, and the reference to the evaluation activities undertaken to verify effective remediation prior to issuance;

(g) Evaluation Administration:

1. a record identifying the time taken by the conformity assessment body (in person-days) to conduct the assessment;

2. the exact deadline within which the next annual surveillance evaluation must be conducted to maintain the validity of the certificate;

(h) Confidentiality Declaration: An explicit declaration stating that the certification assessment report contains highly sensitive proprietary information, is exempt from public disclosure under Article 50 of Regulation (EU) 2019/881 (Cybersecurity Act), and is intended strictly for the use of the conformity assessment body, the applicant, and the competent national cybersecurity certification authority

24 ANNEX IX: SCOPE AND TEAM COMPOSITION FOR PEER ASSESSMENTS

24.1 SCOPE OF THE PEER ASSESSMENT

Explanatory note: This Annex complements the chapter on peer assessment (Chapter VIII) by establishing the exact scope and team requirements for assessing Certification Bodies that issue EUMSS certificates at the 'high' assurance level.

1. The peer-assessed Conformity Assessment Body shall submit a complete list of certified Managed Security Services that may be candidates for review by the peer assessment team.

2. The selection of candidate services for the peer assessment shall comply with the following rules:

    a) the candidate services shall cover the technical scope of the Conformity Assessment Bodies accreditation and authorisation;

    b) the peer assessment team shall select and analyse at least two different Managed Security Service evaluations that were certified by the body at assurance level ‘high’;

    c) the sample shall encompass an assessment of how the Conformity Assessment Body evaluated both the foundational requirements of the Horizontal Layer (Annex II) and the specific requirements of the relevant Vertical Layer service profile (Annex III).

3. Where the Conformity Assessment Body has not yet issued the minimum number of certificates at assurance level 'high' to meet the requirements in paragraph 2, the peer assessment team shall decide whether to perform the peer assessment on the available Managed Security Services, or to postpone the peer assessment.

24.2 PEER ASSESSMENT TEAM COMPOSITION AND COMPETENCE

Explanatory note: Given the operational complexity of Managed Security Services, this Annex explicitly aligns the required competencies of the peer assessment team with the role profiles defined in the European Cybersecurity Skills Framework (ECSF), ensuring that the team possesses the right mix of audit, technical, and service-specific expertise (such as Incident Response and Penetration Testing).

1. The peer assessment team shall consist of at least two experts, each selected from a different Conformity Assessment Body established in different Member States that issues EUMSS certificates at assurance level ‘high’.

2. Each member of the assessment team shall have at least two years of experience carrying out certification or conformity assessment activities within a Conformity Assessment Body.

3. To ensure that the peer assessment team is capable of accurately evaluating the Conformity Assessment Bodies technical competence, the team shall collectively demonstrate expertise aligned with the following relevant role profiles of the European Cybersecurity Skills Framework (ECSF):

   a) Cybersecurity Auditor (ECSF Profile 2.6): Expertise necessary to assess the Conformity Assessment Bodies procedures for evaluating the provider's Information Security Management System (ISMS), evidence reuse methodologies, and overall compliance with the Horizontal Layer.

   b) Penetration Tester (ECSF Profile 2.12): Expertise necessary to evaluate the Conformity Assessment Bodies technical capacity to perform or validate vulnerability assessments, penetration testing, and substitute equivalent activities (such as physical/procedural attack simulations) required for the 'high' assurance level.

   c) Cyber Incident Responder (ECSF Profile 2.2) or relevant Domain Expert: Expertise related to the specific service profile under review (e.g., Incident Management), ensuring the team can judge the Conformity Assessment Bodies competence in evaluating the technical and operational capabilities of the specific Managed Security Service.

4. In the case of a delegation of certificate issuance or prior approval of certificates as referred to in Article 56(6) of Regulation (EU) 2019/881 (Cybersecurity Act), an expert from the national cybersecurity certification authority related to the concerned Conformity Assessment Body shall, in addition, participate in the team of experts selected in accordance with paragraph 1 of this Section.

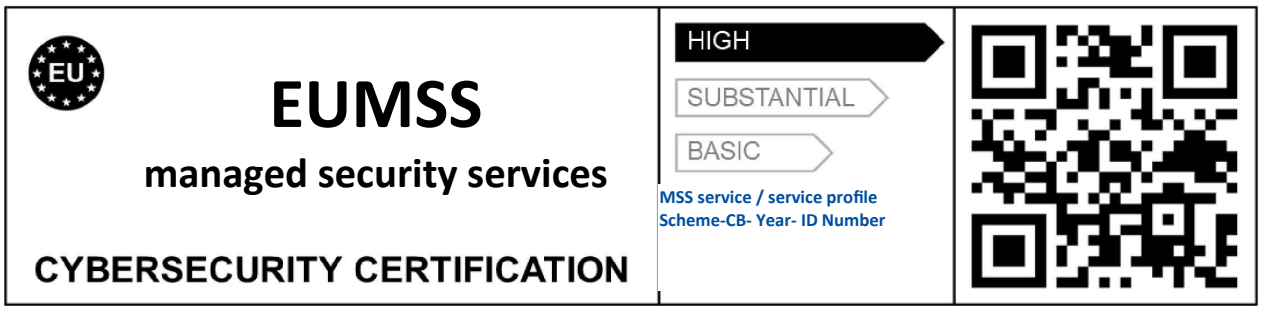
5. The national cybersecurity certification authority monitoring and supervising the peer-assessed Conformity Assessment Body, and at least one national cybersecurity certification authority whose Conformity Assessment Body is not subject to the peer assessment, shall participate in the peer assessment as an observer. ENISA may also participate in the peer assessment as an observer.

6. The peer-assessed Conformity Assessment Body shall be presented with the composition of the peer assessment team prior to the execution of the assessment. In justified cases, it may challenge the composition of the peer assessment team and ask for its review, particularly in cases of potential conflicts of interest.

25 ANNEX X: MARK AND LABELS

25.1 MARK AND LABELS

1. The form of mark and label:



2. If the mark and label are reduced or enlarged, the proportions given in the drawing above shall be respected.

3. Where physically present, the mark and label shall be at least 5 mm high.

26 ANNEX XI: ACCEPTABLE ISMS STANDARDS FOR HOLA

26.1 ACCEPTABLE ISMS STANDARDS FOR HOLA

1. ENISA may create guidance with the list of acceptable ISMS standards for the EUMSS Scheme.

2. Only standards, which fulfil the following requirements may be on this list:

a) The standard is a generic ISMS requirements standard.

b) The standard was developed in an open fashion, including participations by relevant stakeholders.

c) The standard can be obtained by all market actors under the same conditions.

d) The standard (including previous version) has been under operation by other organizations for at least 3 years.

3. ENISA shall inform the ECCG about the standards on the list and take its feedback on entries into account before publishing the List.

27 ANNEX XII: TERMINOLOGY

27.1 TERMINOLOGY

TBD

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity Certification Schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union