ETSI TR 103 305-4 V3.1.1 (2022-11)

Cyber Security (CYBER);
Critical Security Controls for Effective Cyber Defence;
Part 4: Facilitation Mechanisms

Reference
RTR/CYBER-0077

Keywords
cyber security, cyber-defence, information assurance

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 4 of a multi-part deliverable covering the Critical Security Controls for Effective Cyber Defence. Full details of the entire series can be found in part 1 [i.1].

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The Critical Security Controls represent perhaps the most valuable cyber defence mechanism worldwide and across multiple ICT sectors because of the many facilitation mechanisms which have been developed to assist with their implementation and use. The present document is an evolving repository for some of the most important facilitation mechanism for the Critical Security Controls.

Introduction

The Critical Security Controls ("the Controls") exist within a larger cyber security ecosystem that relies on the Controls as critically important defensive measures. There are a variety of facilitation mechanisms for their use. The present document provides a placeholder for reference information for several especially useful mechanisms: Hardened Images, Mappings and Compliance, Guide for Small- and Medium-Sized Enterprises, and Risk Assessment Method. The addition of the Community Defence Model enhances the understanding of the Critical Security Controls and confirms the relative value of individual Control Safeguards. The Control benchmarks provide extensive configuration guidelines for more than 100 systems on more than 25 vendor products.

1 Scope

The present document is an evolving repository for diverse facilitation mechanism guidelines for Critical Security Control implementations.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.2] Center for Internet Security: "CIS Hardened Images".

NOTE: Available at https://www.cisecurity.org/services/hardened-virtual-images/.

[i.3] Center for Internet Security: "Mappings and Compliance".

NOTE: Available at https://www.cisecurity.org/cybersecurity-tools/mapping-compliance/.

[i.4] Center for Internet Security: "CIS Controls Implementation Guide for SMEs".

NOTE: Available at https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf.

[i.5] Center for Internet Security: "CIS Risk Assessment Method (RAM)".

NOTE: Available at https://learn.cisecurity.org/cis-ram.

[i.6] Mappings to the CIS Critical Security Controls.

NOTE: Available at https://www.cisecurity.org/wp-content/uploads/2017/03/Poster_Winter2016_CSCs.pdf.

[i.7] ETSI TR 103 305-5: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement".

[i.8] Center for Internet Security: "CIS Community Defense Model, Version 2.0".

NOTE: Available at https://www.cisecurity.org/white-papers/cis-community-defense-model-2-0/.

[i.9] Center for Internet Security: "CIS Community Defense Model for CIS Controls v7.1".

NOTE: Available at https://www.cisecurity.org/white-papers/cis-community-defense-model/.

[i.10] MITRE, ATT&CK®.

NOTE: Available at https://attack.mitre.org/.

[i.11] Center for Internet Security: "CIS Benchmarks™".

NOTE: Available at https://www.cisecurity.org/cis-benchmarks/.

[i.12] Center for Internet Security: "CIS WorkBench".

NOTE: Available at https://workbench.cisecurity.org/.

[i.13] ETSI TS 103 523: "CYBER; Middlebox Security Protocol".

[i.14] GSMA: "FS.31 GSMA Baseline Security Controls".

NOTE: Available at https://www.gsma.com/security/resources/fs-31-gsma-baseline-security-controls/.

[i.15] Center for Internet Security: "CIS Controls v8 Mapping to GSMA FS.31 Baseline Security Controls v2.0".

NOTE: Available at https://www.cisecurity.org/white-papers/cis-controls-v8-mapping-to-gsma-fs-31-baseline-security-controls-v2-0/.

[i.16] Cloud Security Alliance (CSA): "Cloud Controls Matrix".

NOTE: Available at https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.

[i.17] Center for Internet Security: "CIS Critical Security Controls Mapping to Cloud Security Alliance Cloud Control Matrix".

NOTE: Available at https://www.cisecurity.org/white-papers/cis-controls-mapping-to-cloud-security-alliance-cloud-control-matrix/

[i.18] NIST: "Open Security Controls Assessment Language (OSCAL)".

NOTE: Available at https://github.com/usnistgov/OSCAL/releases/tag/v1.0.0.

[i.19] NIST: "OSCAL Concepts, Layers and Models".

NOTE: Available at https://pages.nist.gov/OSCAL/concepts/layer/.

[i.20] OSCAL community resources.

NOTE: Available at https://github.com/oscal-club/awesome-oscal.

[i.21] Center for Internet Security: "Critical Security Controls Navigator".

NOTE: Available at https://www.cisecurity.org/controls/cis-controls-navigator/.

[i.22] Nonprofit Cyber.

NOTE: Available at https://nonprofitcyber.org/.

[i.23] Center for Internet Security: "CIS Controls v8 Mapping to ISO/IEC 27002:2022".

NOTE: Available at https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-iso-iec2-27002-2022.

[i.24] Center for Internet Security: "CIS Critical Security Controls v8 Mapping to NIST 800-53 Rev. 5".

NOTE: Available at https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-800-53-rev-5.

[i.25] CIS Controls OSCAL Repository.

NOTE: Available at https://github.com/CISecurity/CISControls_OSCAL.

[i.26] ETSI Critical Security Controls OSCAL Repository.

NOTE: Available at https://forge.etsi.org/rep/cyber/103305_CSC/oscal/.

[i.27] ISO/IEC 27002:2022: "Information security, cybersecurity and privacy protection -- Information security controls.".

3 Terms of definitions, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

Critical Security Control (CSC): specified capabilities that reflect the combined knowledge of actual attacks and effective defences of experts

NOTE: See ETSI TR 103 305-1 [i.1].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CAS	Controls Assessment Specification
CDM	Community Defense Model
CSA	Cloud Security Alliance
CSC	Critical Security Control
DBIR	Data Breach Investigations Report
DIBR	Data Breach Investigations Report
FISMA	Federal Information Security Modernization Act
FS	Fraud and Security Group (GSMA)
GDPR	General Data Protection Regulation
ICT	Information Communications Technology
IG	Implementation Group
NOTE:	See ETSI TR 103 305-1 [i.1].
IT	Information Technology
JSON	JavaScript Object Notation
NPC	Non-Profit Cyber
PCI DSS	Payment Card Industry Data Security Standard
RAM	Random Access Memory
SME	Small- and Medium-sized Enterprises
STIG	Security Technical Implementation Guide
XML	Extensible Markup Language
YAML	Yet Another Markup Languag

4 Hardened Images

4.1 Description

One of the potentially most effective new means for implementing the Critical Security Controls (CSCs) - especially in a cloud data center environment is to use Hardened Images via major cloud computing vendors which have been facilitated by the Center for Internet Security [i.2]. Hardened Images are securely configured according to applicable CIS benchmarks. The Hardened Images include most major cloud data center platforms.

4.2 Virtual Image vs. Hardened Virtual Image

A virtual image is a snapshot of a Virtual Machine (VM) used to create a running instance in a virtual environment, thus providing the same functionality as a physical computer. Virtual images reside on the cloud and enable cost-effective performance of routine computing operations without investing in local hardware and software.

Hardening is a process of limiting potential weaknesses that make systems vulnerable to cyber attacks. Examples include:

- Disabling unnecessary ports/services
- Eliminating unneeded programs and internal root accounts
- Limiting/denying visitor access

More secure than a standard image, hardened virtual images reduce system vulnerabilities to help protect against denial of service, unauthorized data access, and other cyber threats.

4.3 Benefits of Hardened Images

The available images are hardened to meet the Critical Security Control benchmarks, secure configuration standards that are collaboratively developed and used by thousands worldwide. The benchmarks are vendor-agnostic and securely configured, regardless of the cloud platform chosen. Benefits include:

- Conformance to recommended cybersecurity best practices
- Flexible deployability across networks by administrators
- Elimination of initial investments in hardware
- Ability to scale virtual resources and security quickly
- Inclusion of reports showing conformance to applicable benchmarks

5 Compliance Control Mappings and Navigation

5.1 Description

A broad array of national government agencies, regional authorities, and industry sector organizations have published cyber security compliance "frameworks" - frequently in the form of their own imposed controls. The Critical Security Controls can support most of these framework requirements, and continuing efforts exist to maintain and publish mappings from the Controls to all the diverse frameworks. See Critical Security Controls: Mapping and Compliance [i.3]. As a result, the Critical Security Controls have become not only a common bridge among other security control sets globally, but the means to comply with them because of the large collection of tools in the marketplace available for implementation, including those described in the present document.

The Compliance Control Mappings are continually evolved with existing and newly available compilations. Following the release of the new version of the Controls [i.1] the number of identified control sets and mappings from different organizations, sectors, and countries, including health and electrical power systems, have increased significantly [i.6]. Additional sector compliance requirements of significance are the Payment Card Industry Data Security Standard (PCI DSS) within the banking industry, and the Federal Information Security Modernization Act (FISMA) requirements among government agencies.

5.2 Controls Mapping and Navigation

Because the number of Compliance mappings has become so complex and dynamic, a Critical Security Controls Navigator was developed to facilitate the mapping process [i.21]. This powerful tool enables a user or organization to facing compliance requirements based on a set of controls to select the control sets and implementation groups, and then see exactly the detailed mappings. This can then be followed by identifying levels of risk management, and then by obtaining widely available products, services, playbooks, benchmarks, and defence information for the Critical Security Controls in the present document and in the marketplace.

Especially significant mappings facilitated by the Navigator include:

- GSMA FS.31 Baseline Security Controls [i.14] and [i.15].
- Cloud Security Alliance Cloud Controls Matrix [i.16] and [i.17].
- Controls relating to privacy requirements, including the GDPR are contained in ETSI TR 103 305-5 [i.7].
- ISO/IEC 27002 Information Security Controls for cybersecurity and privacy protection [i.23] and [i.27].
- NIST 800-53, Security and Privacy Controls for U.S. Federal Information Systems except those related to national security [i.24].

6 Guide for Small and Medium-sized Enterprises (SMEs)

6.1 Description

Credit card breaches, identity theft, ransomware, theft of intellectual property, loss of privacy, denial of service have emerged as daily cyber security incidents. Victims with large budgets can take steps to mitigate these attacks. However, organizations with small budgets and limited staff are less able to respond. Common concerns of SMEs include:

- Theft of company information - External hackers and dissatisfied employees steal company information and customer lists.
- Website defacement - Hackers corrupt your website to benefit competitors.
- Phishing attacks - Email is designed to look like legitimate correspondence that tricks recipients into clicking on a link that installs malware on the system.
- Ransomware - Types of malicious software block access to a computer so that criminals can hold your data for ransom.
- Data loss due to natural events and accidents.

A guide for Small and Medium-sized Enterprises (SMEs) with a small number of high priority actions based on the Critical Security Controls can be especially useful and is available online [i.4]. The guide contains a small sub-set of the Controls specifically selected to help protect SMEs.

To help prioritize SME efforts, the Guide recommends using a phased approach. Phase 1 involves knowing what is on the SME network and understanding the cybersecurity baseline. Phase 2 focuses on protecting the SME security baseline through education and prevention. Phase 3 helps SMEs to prepare in advance for disruptive events. Each phase has specific questions to be answered, along with action items and tools that will helpachieve SME cyber security goals.

7 Control Assessment Mechanisms

7.1 Controls Assessment Specification (CAS)

The Critical Security Controls provide essential best practices that organizations can implement to improve their cybersecurity posture. In addition to implementing the CIS, it is also important that organizations measure their implementations to ensure that Safeguards are in place and working properly. The purpose of the CIS Controls Assessment Specification (CAS) is to provide a common understanding of what should be measured in order to verify that CIS Safeguards are properly implemented. The hope is that those developing related tools will then build these measures into their tools so that the CIS Controls are measured in a uniform way.

The focus of CAS is on "what to measure" rather than "how to measure". With the goal of being platform agnostic, a conscious effort was made to avoid addressing the "how to measure" in writing CAS, leaving those platform specific details to specific implementations of these measures. Tool developers will determine the "hows" that are appropriate for their tools and use cases.

7.2 Controls Workbench

The Controls Workbench [i.12] is a powerful tool that works in conjunction with the Assessment Specification to inform users and enterprises exactly which safeguards to implement to achieve desired or required levels of security and risk. The Controls Workbench provides a means to deal with the complexity and enables each implementation to select all the relevant jurisdiction, sector/national, context and risk variables to facilitate the relevant requirements.

7.3 Risk Assessment Method (RAM)

Risk assessment is a term used to describe the overall process or method where an organization identifies hazards and risk factors that have the potential to cause harm (hazard identification), and then analyses and evaluates the risk associated with that hazard in some systematic and quantifiable manner. The constantly evolving, enormous array of cyber security vulnerabilities and incidents today in the face of finite resources is perhaps the biggest challenge of most organizations. The Critical Security Controls are enormously useful, but their effective implementation is necessitating some kind of risk assessment method.

The Critical Security Controls user community has contributed to a Risk Assessment Method (RAM) [i.5] to help organizations plan and justify their implementation of Controls - whether those controls are fully or partially operating. Few organizations can apply all controls to all information assets, because - while reducing some risks - security controls also introduce new risks to efficiency, collaboration, utility, productivity, or available funds and resources.

Laws, regulations, and information security standards all consider the need to balance security against an organization's purpose and its objectives, and require risk assessments to find and document that balance. The risk assessment method described provides a basis for communicating cybersecurity risk among security professionals, business management, legal authorities, and regulators using a common language that is meaningful to all parties.

The RAM uses established information security risk assessment standards. Organizations can evaluate risks and safeguards using the concept of "due care" and "reasonable safeguards" that the legal community and regulators use to determine whether organizations act as a "reasonable person".

8 Community Defense Model

8.1 Description

Organizations typically want to understand the effectiveness of the Critical Security Controls against the most prevalent types of attacks. The Community Defense Model (CDM) [i.12] facilitates this understanding based on currently available threat data from industry reports.

The CDM makes use of the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework which enables expression of any attack type as a set of attack techniques, known as attack patterns [i.10].

For each of the five most prevalent attack types, such as ransomware, the corresponding attack patterns can be collected through analysis of industry threat data. The Controls Safeguards which defend against each of the techniques found in those attack patterns can then be tracked. This methodology allows measurement of which Safeguards are most effective overall for defense across attack types.

The CDM results during the 2020-2021 period have increased confidence that conclusions from the first CDM were correct, see [i.9]. Based on additional industry threat data sources, the use of the updated version 8 of the Controls [i.1] and version 8.2 of the MITRE ATT&CK framework, it was possible to verify that the Controls are effective at defending against 86 % of the ATT&CK (sub-)techniques found in the ATT&CK framework. More importantly, the Controls are highly effective against the top five attack types found in industry threat data. The Controls, and specifically IG1, are a robust foundation for an organization's cybersecurity program.

The results also confirm that establishing and maintaining a secure configuration process (Safeguard 4.1) is a linchpin Safeguard for all five attack types, which reinforces the importance of configurations, such as those found in the CIS Benchmarks™ [i.11].

8.2 Model process

The CDM is comprised of a series of seven steps.

1) **Create master mapping.** A master mapping is created from the latest version of the Critical Security Controls to Enterprise ATT&CK v8.2, mapping the CIS Safeguards to the ATT&CK (sub-) techniques. ATT&CK mitigations were used as a guide to map at the ATT&CK (sub-)technique level.

2) **Analyse security function.** Analyse the security function of the Control Safeguards against ATT&CK (sub-)techniques using the master mapping in Step 1.

3) **Identify top five attack types.** Using multiple data sources, identify the five most prevalent attack types experienced by enterprises in 2020-2021: Malware, Ransomware, Web Application Hacking, Insider Privilege and Misuse, and Targeted Intrusions.

4) **Construct attack patterns.** For each attack type, use multiple data sources to create comprehensive attack patterns-the set of attacker techniques (e.g. ATT&CK (sub-)techniques) used in an attack type.

5) **Perform reverse mapping.** Use the master mapping of the Controls to ATT&CK (in Step 1) to map each ATT&CK (sub-)technique associated with an attack type back to the Safeguards.

6) **Analyse security value.** The reverse mapping allowed analysis of the security value of implementing the Safeguards against one or more attack types, meaning, how well do the CIS Controls defend against the top five attacks.

7) **Create visualizations.** The MITRE ATT&CK Navigator allows users to create interactive "layers" of ATT&CK. This tooling allowed to visualize each attack pattern individually and combined across all attack types. These layers can be found on the CIS WorkBench [i.12].

8.3 Model conclusions

The most recent CDM analysis affirms the prioritization of the Critical Security Controls and Implementation Groups. See Figure 8-1, below. In particular, CDM data backs the premise that all enterprises should start with essential cyber hygiene, or IG1, as a way to defend against the top five attacks. The key findings include:

- Implementation Group 1 (IG1) provides a viable defense against the top five attack types. Enterprises achieve a high level of protection and are well-positioned to defend against the top five attack types through implementation of essential cyber hygiene, or IG1. These results strongly reinforce the value of a relatively small number of well-chosen and basic defensive steps (IG1). As such, enterprises should aim to start with IG1 to obtain the highest value and work up to IG2 and IG3, as appropriate.

- Independent of any specific attack type, the Controls are effective at defending against a wide array of attacks. Specifically, the Controls are effective at defending against 86 % of the ATT&CK (sub-)techniques found in the ATT&CK framework. More importantly, the Controls are highly effective against the five attack types found in industry threat data. The bottom line is that the CIS Controls, and specifically IG1, are a robust foundation for your cybersecurity program.

- Establishing and maintaining a secure configuration process (CSC Safeguard 4.1) is a linchpin Safeguard for all five attack types. CSC Safeguard 4.1 is most effective in defending against the top five attack types, reinforcing the importance of secure configurations, such as those contained within the CIS Benchmarks.

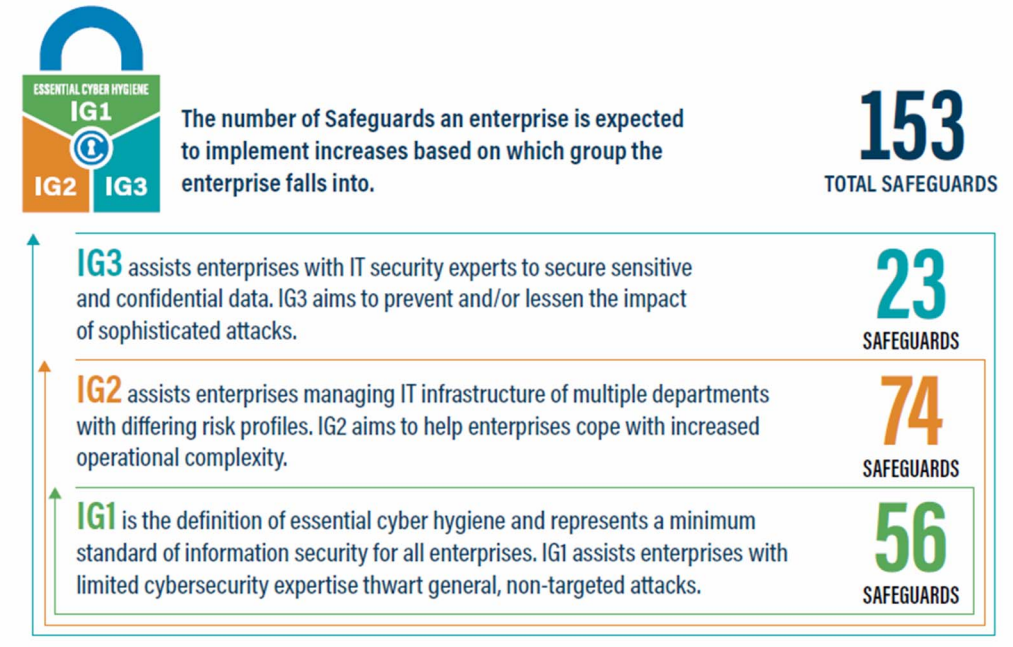

Figure 8-1: Critical Security Controls Implementation Group overview

8.4 Model features envisioned

Model features not addressed and planned for future development include:

- **Additional data sources.** Find additional data sources for the top attack types and patterns. This will help to further strengthen the analysis and provide additional insight to other sectors that may not be represented in the current data sources.

- **Re-categorization of top attack types.** During the writing of the most recent CDM (v2.0), and after analysis was completed, a 2021 major telecommunication service provider published a DIBR along with their new categorization for attack patterns (i.e. attack types). These attack patterns take a new approach to the way that attacks are viewed. Review of the DBIR categorization schemas is needed, as well as other data sources, to continually improve the categorization of attack types.

- **More specific analyses.** As future versions of the CDM are evolved, the analysis needs to perform greater in-depth analyses, to answer questions such as: "What is the specific 'point' in an attack where it can be thwarted completely?" and "What are the minimal set of Safeguards within IG1 that are needed to implement to stop that attack?"

- **More collaboration and correlation.** As the Security Best Practices continues to mature the mappings to ATT&CK, further incorporation of Benchmark mappings is needed [i.10].

- **More stakeholder engagement.** A broader array of stakeholder communities engaging in the CDM work will enable expanded application to those communities.

Additional needed capabilities include:

- Determining the most cost-effective way to obtain the security value of IG1

- Making the best security use of the existing cyber security capabilities of an organization

- If attack data that is unique to an industry sector or threat intelligence that is unique to a company, are used, which Safeguards should be implemented to achieve an appropriate defensive strategy?

- Will defenses be effective at multiple steps or tactics of the attack lifecycle?
- If the effectiveness of a specific Safeguard (or its absence) is known, can defenses be intelligently tailored to accommodate specific operational constraints (like the need to run legacy applications)?

9 Critical Security Control benchmarks

9.1 Description

The Critical Security Control benchmarks are best practices for the secure configuration of most major IT platforms [i.11]. They are available for more than 100 platforms across more than 25 vendor product families, and developed through a unique consensus-based process comprised of cybersecurity professionals and subject matter experts around the world. The benchmarks are consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry, and academia. They constitute a unique, openly-available and constantly evolving cyber security knowledge resource.

9.2 Benchmark development process

The initial benchmark development process defines the scope of the benchmark and begins the discussion, creation and testing process of working drafts. Using the WorkBench community website, [i.12] discussion threads are established to continue dialogue until a consensus has been reached on proposed recommendations and the working drafts. Once consensus has been reached in the CIS Benchmark community, the final benchmark is published and released online for free in PDF format. The release of new CIS Benchmarks can vary depending on the community as well as the major release schedule of the technology the benchmark supports. Monthly emails are distributed announcing new benchmarks and updates to existing benchmarks that have been released. Each community allows the user to view milestones associated with a particular CIS Benchmark to show where it stands in the development and update process.

9.3 Benchmark configuration profiles

The latest Benchmark configuration profiles are available on a dedicated website in multiple formats [i.11]. Most benchmarks include multiple configuration profiles. A profile definition describes the configurations assigned to benchmark recommendations. The Level 1 profile is considered a base recommendation that can be implemented fairly promptly and is designed to not have an extensive performance impact. The intent of the Level 1 profile benchmark is to lower the attack surface of an organization while keeping machines usable and not hindering business functionality. The Level 2 profile is considered to be "defense in depth" and is intended for environments where security is paramount. The recommendations associated with the Level 2 profile can have an adverse effect on an organization if not implemented appropriately or without due care. The STIG profile replaces the previous Level 3. The STIG profile provides all recommendations that are STIG specific. Overlap of recommendations from other profiles, i.e. Level 1 and Level 2, are present in the STIG profile as applicable. Every recommendation within each benchmark is associated with at least one profile. Applying benchmark guidance in a test environment to determine potential impact is recommended.

10 Critical Security Controls for middlebox defence

10.1 Description

This clause applies the Critical Security Controls [i.1] to network middleboxes - especially for those using ETSI Middlebox Security Protocols ETSI TS 103 523 [i.13].

10.2 Application of the Controls

The Critical Security Controls should be applied, as appropriate, to all network middleboxes and their management.

11 Open Security Controls Assessment Language (OSCAL)

11.1 Description

An Open Security Controls Assessment Language (OSCAL) has recently emerged [i.18]. The OSCAL architecture is organized in a stack of layers. Each lower layer in the stack provides information structures that are referenced and used by each higher layer. Each layer is composed of one or more models, which represent an information structure supporting a specific operational purpose. Each model in OSCAL is intended to build on the information provided by the model(s) in the lower layers. Each OSCAL model is represented in multiple, machine-readable formats (e.g. XML, JSON, YAML), which provide a serialization and encoding mechanism for representing and exchanging OSCAL data, also referred to as OSCAL content. Figure 11-1 depicts each layer and the corresponding model(s) for each layer [i.19].

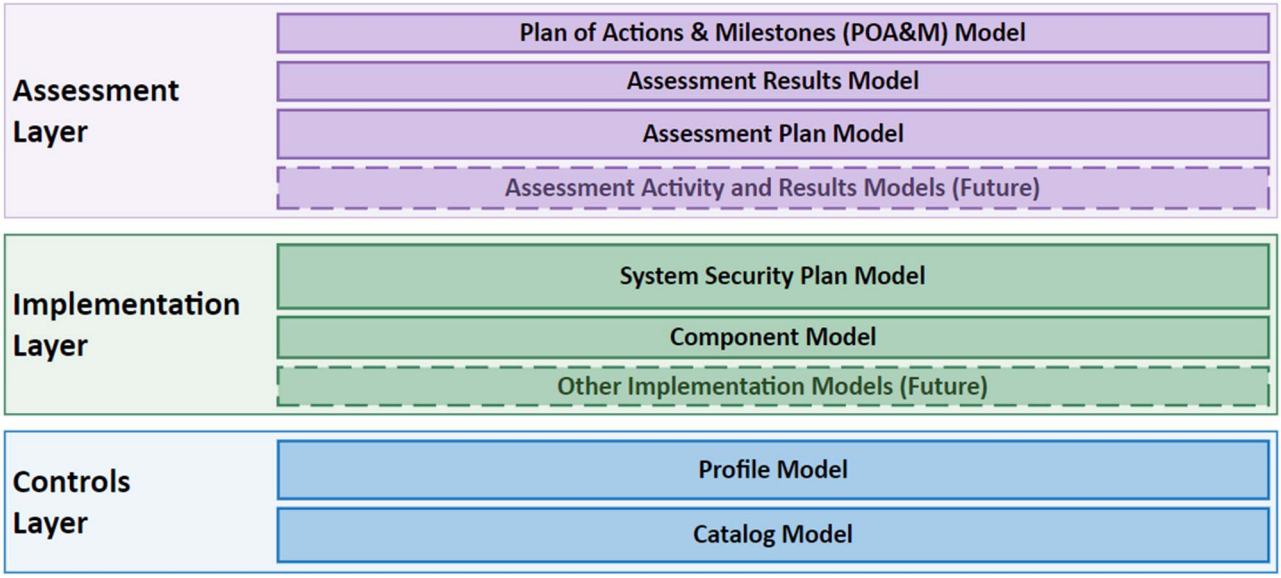

Figure 11-1: OSCAL layers and models (from NIST OSCAL webpage [i.19])

OSCAL open resources worldwide are emerging that include enterprise and national cybersecurity controls, and includes a catalog of diverse cybersecurity control specifications [i.20].

11.2 OSCAL serializations for the Critical Security Controls

OSCAL serializations of the CIS Critical Security Controls and including a variety of OSCAL Catalogs for the main CIS Controls document, Controls Assessment Specification, and mapping documents are available in repository with a permanent uuid [i.25]. This enables automated ingestion of Controls and assessments against those frameworks and mappings in between frameworks regardless of version.

OSCAL serializations of the ETSI Critical Security Controls and including a variety of OSCAL Catalogs for the ETSI TR 103 305-1 [i.1] are available in a repository with a permanent uuid [i.26].

12 Global Controls Collaboration

12.1 Description

The continuing development and implementation of the Critical Security Controls can be significantly enhanced through global collaboration among organizations dedicated to this objective. This collaboration was advanced through the creation of Non-profit Cyber (NPC) [i.22]. Cybersecurity non-profit organizations are essential resources improving cyber defense for every enterprise, in every dimension, and for the ecosystem as a whole. They create guidance, standards, and best practices, conduct research, educate individuals and businesses, build and share great tools, and operate important infrastructure. Non-profits are often natural "integration engines," bringing together knowledgeable individuals and ideas across technical disciplines, the public and private sectors, industry sectors, worldwide. Such organizations are also venues where individuals or small enterprises can have impact equal to the largest enterprises.

12.2 Models, architectures, interfaces, protocols, and information structures

The work of global controls collaboration presently remains in a formative state.

History

Document history		
V1.1.1	August 2016	Publication
V2.1.1	September 2018	Publication
V3.1.1	November 2022	Publication