International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 36
(09/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1051 – Supplement on critical security controls for information and network security management by telecommunication organizations

ITU-T X-series Recommendations – Supplement 36

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Supplement 36 to ITU-T X-series Recommendations

ITU-T X.1051 – Supplement on critical security controls for information and network security management by telecommunication organizations

Summary

Supplement 36 to ITU-T X-series Recommendations describes the critical security controls (CSCs) to supplement the implementation of Recommendation ITU-T X.1051. CSCs are a prioritized set of actions that collectively form a defence-in-depth set of best practices that mitigate the most common attacks as part of the information and network security management of an organization. These controls are developed by a community of information technology (IT) experts who apply their first-hand experience as cyber defenders to create globally acceptable security best practices and to include multiple sectors such as retail, manufacturing, healthcare, education, government and defence.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 36	2021-09-03	17	11.1002/1000/14809

Keywords

Audit, compliance, information security, information security management, management guideline, network security, risk management, security requirements, ITU-T X.1051 | ISO/IEC 27011.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

Critical security controls (CSCs) are developed and maintained by the Centre of Internet Security (CIS) and published by European Telecommunications Standards Institute (ETSI) as a multipart technical report [b-ETSI TR 103 305]. [b-ETSI TR 103 305-1] contains the controls themselves. [b-ETSI TR 103 305-2] to [b-ETSI TR 103 305-5] contain information relating to the implementations of CSCs in different contexts. CIS is a non-profit standards development organization formed to identify, develop, validate, promote and sustain best practice specifications for cyber defence and to assist communities to enable an environment of trust in cyberspace.

The CSCs provide additional benefits as they are implemented in most cyber defence solutions to detect, prevent, respond and mitigate damage from the most common to the most advanced of cyber-attacks. The control requirements include the assessment and treatment of information security risks tailored to the needs of the organization.

The control requirements set out are generic and intended to be applicable to all organizations, regardless of size, type or nature within the information and telecommunication sector.

Supplement 36 to ITU-T X-series Recommendations

ITU-T X.1051 – Supplement on critical security controls for information and network security management by telecommunication organizations

1 Scope

This Supplement provides cyber security best practices for security management using critical security controls (CSCs) within the scope of [ITU-T X.1051]. The use of the CSC framework and the associated critical security controls supports and complements [ITU-T X.1051].

2 References

[ITU-T X.1051] Recommendation ITU-T X.1051 (2016) | ISO/IEC 27011:2016, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Supplement

This Supplement defines the following term:

3.2.1 critical security controls (CSCs): Prioritized set of actions that should be used as security management best practices to mitigate the most common attacks against systems and networks.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

5G fifth Generation

API Application Programming Interface

CSC Critical Security Control

CSF Cybersecurity Framework

DSP Digital Services Provider

ICT Information and Communication Technology

IDS Intrusion Detection System

IPS Intrusion Prevention System

ISMS Information Security Management System

IT Information Technology

NFV Network Function Virtualization

OTT Over The Top

SDN Software-Defined Networking

SIEM Security Information and Event Management

VM Virtual Machine

5 Conventions

None.

6 Digital transformation of services provider

6.1 Evolution of information and communication technology ecosystem into digital services provider ecosystem

The transformation of the information and communication technology (ICT) world from one in which telecommunication companies or communication service providers had their traditional ecosystem of vendors and system integrators into digital space redefined the business requirements of a digital services provider (DSP).

The DSP ecosystem is one in which services such as over the top (OTT), cloud or application service providers, infrastructure cloud service providers and traditional enterprises are driven by digitalization and digitization of organizations, products and services.

Transformation drivers such as the Internet of things, multi-stakeholder element of fifth generation (5G) and future networks provide a completely new context of regulations, certifications, labelling, business dynamics, etc. For example, Figure 1 illustrates a new virtualized technology of software-defined networking/network function virtualization (SDN/NFV) transformed from traditional network infrastructure based on router, firewall, switch, etc.

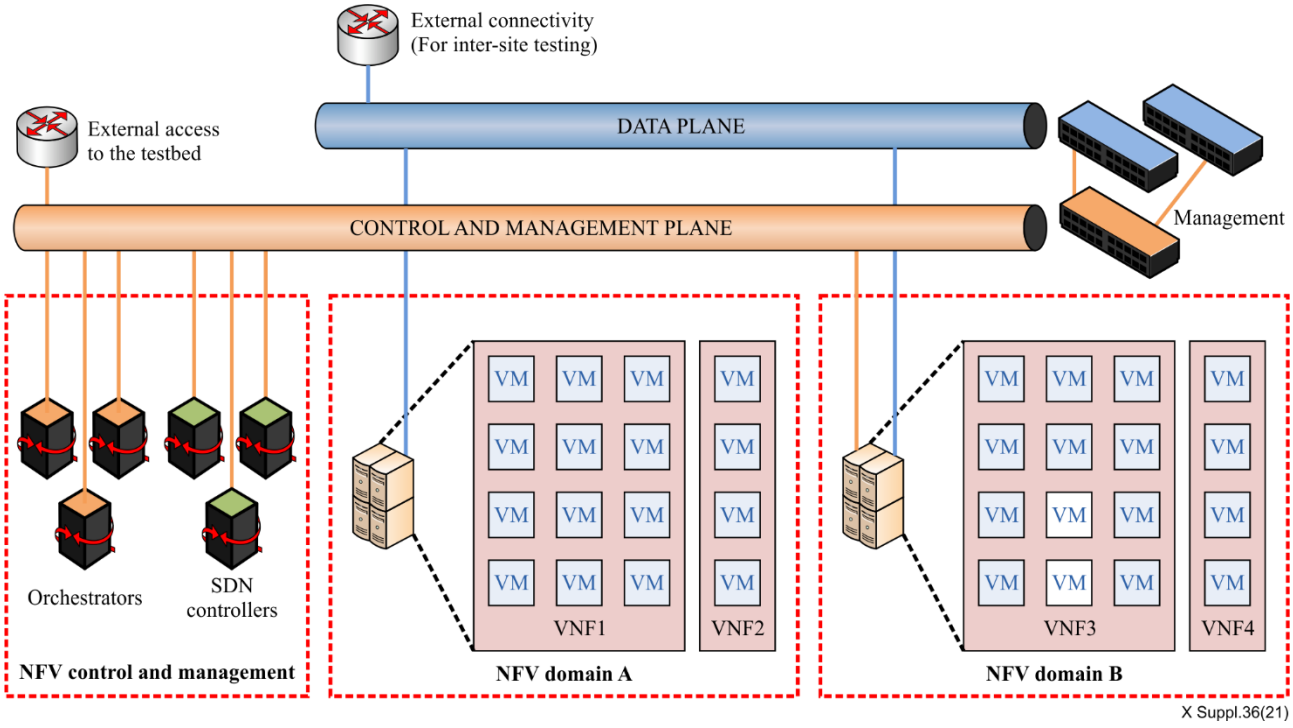

Figure 1 – A new virtualized technology of SDN/NFV transformed from traditional network infrastructure

6.2 Digital ecosystem security risks and cyber threats

SDN is very close to what traditional IT does in terms of virtualization.

a) Benefits of a virtual infrastructure are as follows.

– Scalable – Allows provisioning as many or as few logical servers as required, and users only pay for what they use.
– Flexible – Allows for multiple server and networking configurations as compared to a hardwired physical infrastructure, which requires more capital and effort to change.
– Secure – Allows more security to be layered on top of whatever security is already present in the virtual infrastructure because all traffic to the virtual infrastructure goes through the actual physical infrastructure.
– Load balancing – Allows software-based servers to share workloads easily and distribute them properly so that no single logical server is taxed more than the others.
– Backup and recovery – Promotes easier backups because everything can be saved somewhere, allowing for quick recovery in other hosts if a few hosts are down. This is almost impossible with physical servers, which have to be revived before services can resume.

b) The risks in a virtualized platform are:

– virtual machine (VM) sprawl;
– sensitive data within a VM;
– security of offline and dormant VMs;
– security of pre-configured (golden image) VM or active VMs;
– lack of visibility and control over virtual networks;
– resource exhaustion;
– hypervisor security;
– unauthorized access to hypervisor;
– account or service hijacking through the self-service portal;
– workloads of different trust levels located on the same server;
– risk due to application programming interfaces (APIs).

c) Security issues in a virtualized environment are as follows.

– Securing virtual environments should be no different to physical ones
  • Protection for virtual environments requires as much care as that for physical ones. Lots of IT people still think that virtual environments are safer than physical ones. However, this is a mistake. A determined attacker will always find a way in.
– Understand the specific risks to virtual environments
  • Virtual environments have their own, very different vulnerabilities to physical ones, e.g., they may have a larger attack surface. This is because components within a virtual infrastructure are often interconnected. Any unauthorized or malicious action has the potential to affect all VMs sharing the same host, magnifying its effect. Moreover, there is the risk that VMs may be misconfigured or copied and misused. Both can seriously impact critical business activity.
– Do not leave your virtual environment in a blind spot
  • System administrators need to have insight into the entire IT infrastructure, virtual as well as physical. Both should have regular IT audits that look proactively for any suspicious activity. IT departments need ready answers to questions such as the following.
    ▪ Who created each VM?
    ▪ Who reconfigured or disabled a particular VM?
    ▪ Who changed resource pool parameters?

7 Managing cyber security risks in a digital ecosystem

Managing cyber security risks in a digital ecosystem require security management that should collectively form a defence in depth and a set of best practices that mitigate the most common attacks against systems and networks such as CSCs.

For example, SDN is used to manage load on telecommunication services by adding or removing VMs, the activity on provisioning should be carefully secured and audited. In a traditional software deployment, an application or service update requires that a component be changed in production, while the complete service or application remains operational. Immutable infrastructure instead relies on instancing, where components are assembled on computing resources to form the service or application. Once the service or application is iterated, its components are set – thus, the service or application is immutable. When a change is made to one or more components of a service or application, a new iteration is assembled, tested, validated and made available for use. The old iteration is then discontinued to free computing resources within the environment for other tasks.

All unauthorized changes need to be spotted and investigated immediately – even an innocent mistake can lead to a security incident. Two ways of managing the security risk and compliance are:

– traditional: each box could be an asset;

– SDN/NFV: each workload could be an asset and service managed as a business asset (application asset grouping multiple assets together).

8 Critical security control framework

The CSC framework is presented in Figure 2. The 20 controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create a globally accepted security best practice.

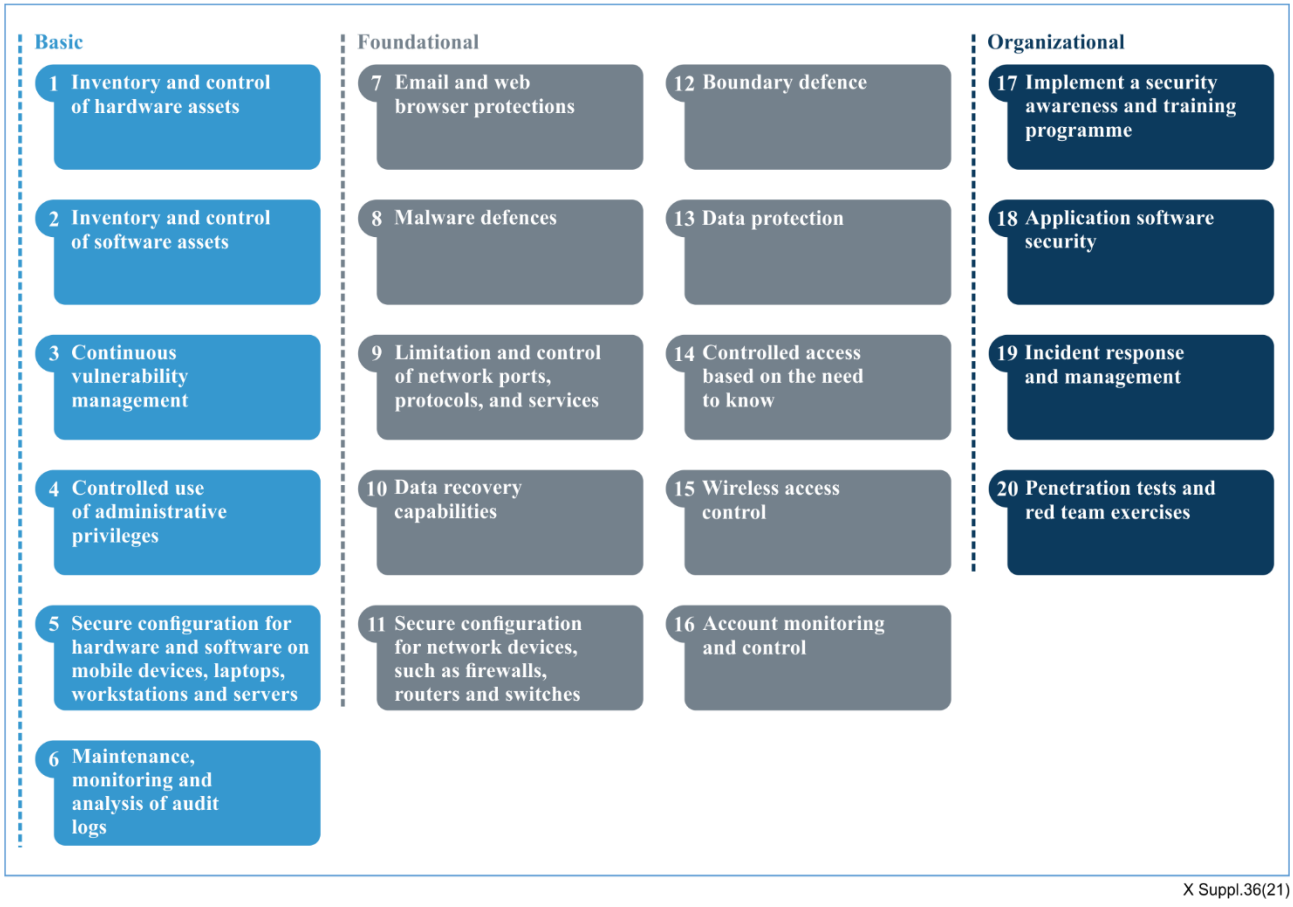

Figure 2 – Critical security control framework

9 Critical security control framework and [ITU-T X.1051]

To supplement [ITU-T X.1051] with the established global cyber defence framework of CSCs requires their integration into telecommunication environment information security management. [ITU-T X.1051] provides additional and specific requirements for the telecommunication organization world.

Currently, most telecommunication organizations manually check against network hardening best practices and regulations to ensure that devices are configured to the correct standard, that traffic is not permitted in restricted areas and that hardware and software is frequently patched to close vulnerability gaps. For telecommunication organizations it is a tedious and mostly ineffective process to manage. The hardening process can take days to understand based on the impact of a single vulnerability. As a result, many organizations fail to keep their networks access hardened because enforcing mandatory standards becomes problematic.

Most network teams are just beginning to implement workflow automation into their security processes. As a result, manual processes become a challenge in verifying network hardening policies and troubleshooting cyberattacks. This is equally challenging when it comes to reactive workflows where the objective is to mitigate active cyber threats. Typically, most organizations leverage intrusion detection system (IDS), intrusion prevention system (IPS) or security information and event management (SIEM) tools to alert administrators when someone is trying to maliciously compromise the network.

Manual processes of cyber threat management need to be eliminated, so organizations have the capability to instantly access the information they need to conduct mitigation and troubleshooting processes. Every day that an organization relies on manual processes is another day that their network is at risk. As the importance and reliance on technology grows and creates even higher degrees of complexity, security issues will also grow tremendously. Telecommunication organizations should be ready to close security vulnerabilities by enabling full visibility into the network.

10 Critical security control mapping with [ITU-T X.1051]

10.1 Key principles

CSCs are based on the following seven key principles to guide the design and development of the CSC framework:

1) improvement in the consistency and simplification of the wording of each sub-control;
2) implementation of "one task" per sub-control;
3) increase in focus on authentication, encryption, and application whitelisting;
4) accounting for improvements in security technology and emerging security problems;
5) better alignment with other frameworks (such as the NIST cybersecurity framework (CSF));
6) support for the development of related products (e.g., measurements or metrics and implementation guides);
7) identification of CSC types (basic, foundational, and organizational).

10.2 Types of critical security control

10.2.1 Basic controls

The basic controls are as follows:

1) inventory and control of hardware assets;
2) inventory and control of software assets;
3) continuous vulnerability management;

4) controlled use of administrative privileges;
5) secure configuration for hardware and software on mobile devices, laptops, workstations and servers;
6) maintenance, monitoring and analysis of audit logs.

10.2.2 Foundational controls

The basic controls are as follows:
1) email and web browser protections;
2) malware defences;
3) limitation and control of network ports, protocols and services;
4) data recovery capabilities;
5) secure configuration for network devices, such as firewalls, routers and switches;
6) boundary defence;
7) data protection;
8) controlled access based on the need to know;
9) wireless access control;
10) account monitoring and control.

10.2.3 Organizational controls

The organizational controls are as follows:
1) implemention of a security awareness and training programme;
2) application software security;
3) incident response and management;
4) penetration tests and red team exercises.

10.3 CSC mapping with [ITU-T X.1051]

CSC mapping with [ITU-T X.1051] as presented in Table 1 summarizes the relationship between [ITU-T X.1051] and CSCs. The CSC mapping supplements ITU-T X.1051 security controls [ITU-T X.1051] that focus on three security domains:
– organization (related organizational or basic controls);
– infrastructure (related foundational controls);
– people (related organizational/basic controls).

Table 1 – Critical security control mapping with [ITU-T X.1051]

No	Critical security controls (CSC)	ITU-T X.1051 | ISO/IEC 27011 (ISO/IEC 27002:2013)	Types of CSCs	ITU-T X.1051 domains
1	Inventory of authorized and authorized devices	8.1.1 9.1.2 13.1.1	basic	infrastructure
2	Inventory of authorized and unauthorized software	12.5.1 12.6.2	basic	infrastructure

Table 1 – Critical security control mapping with [ITU-T X.1051]

No	Critical security controls (CSC)	ITU-T X.1051 | ISO/IEC 27011 (ISO/IEC 27002:2013)	Types of CSCs	ITU-T X.1051 domains
3	Secure configurations for hardware and software	14.2.4 14.2.8 18.2.3	basic	infrastructure
4	Continuous vulnerability assessment and remediation	12.6.1 14.2.8	basic	environment
5	Controlled use of administrative privileges	9.1.1 9.2.2-9.2.6 9.3.1 9.4.1-9.4.4	basic	people
6	Maintenance, monitoring, and analysis of audit logs	12.4.1-12.4.4 12.7.1	basic	infrastructure
7	Email and web browser protections	14.2.4 14.2.8 18.2.3	foundational	infrastructure
8	Malware defences	8.3.1 12.2.1 13.2.3	foundational	infrastructure
9	Limitation and control of network port	9.1.2 13.1.1 13.1.2 14.1.2	foundational	infrastructure
10	Data recovery capability	10.1.1 12.3.1	foundational	organization
11	Secure configuration for network devices	9.1.2 13.1.1 13.1.3	foundational	infrastructure
12	Boundary defence	9.1.2 12.4.1 12.7.1 13.1.1 13.1.3 13.2.3	foundational	infrastructure
13	Data protection	8.3.1 10.1.1-10.1.2 13.2.3 18.1.5	foundational	organization

Table 1 – Critical security control mapping with [ITU-T X.1051]

No	Critical security controls (CSC)	ITU-T X.1051 | ISO/IEC 27011 (ISO/IEC 27002:2013)	Types of CSCs	ITU-T X.1051 domains
14	Controlled access based on the need to know	8.3.1 9.1.1 10.1.1	foundational	infrastructure
15	Wireless access control	10.1.1 12.4.1 12.7.1	foundational	infrastructure
16	Account monitoring and control	9.1.1 9.2.1-9.2.6 9.3.1 9.4.1-9.4.3 11.2.8	foundational	infrastructure
17	Security skills assessment and appropriate training to fill gaps	7.2.2	organizational	people
18	Application software security	9.4.5 12.1.4 14.2.1 14.2.6-14.2.8	organizational	infrastructure
19	Incident response and management	6.1.3 7.2.1 16.1.2 16.1.4-16.1.7	organizational	organization
20	Penetration tests and red team exercises	14.2.8 18.2.1 18.2.3	organizational	infrastructure

11 Critical security control implementation approach

CSCs are designed to be agnostic to any security management framework. The CSCs should be linked to any security management framework by selecting the CSCs and establishing the mapping with other framework. The compliance mapping should not only support CSC requirements, but also other regulatory requirements such the Payment Card Industry Data Security Standard [b-PCI-DSS], the Health Insurance Portability and Accountability Act [b-HIPAA] or the ISO/IEC information security management system (ISMS) [b-ISO/IEC 27002].

12 Critical security control implementation model

The overall flow of the CSC implementation model is provided in Figure 3.

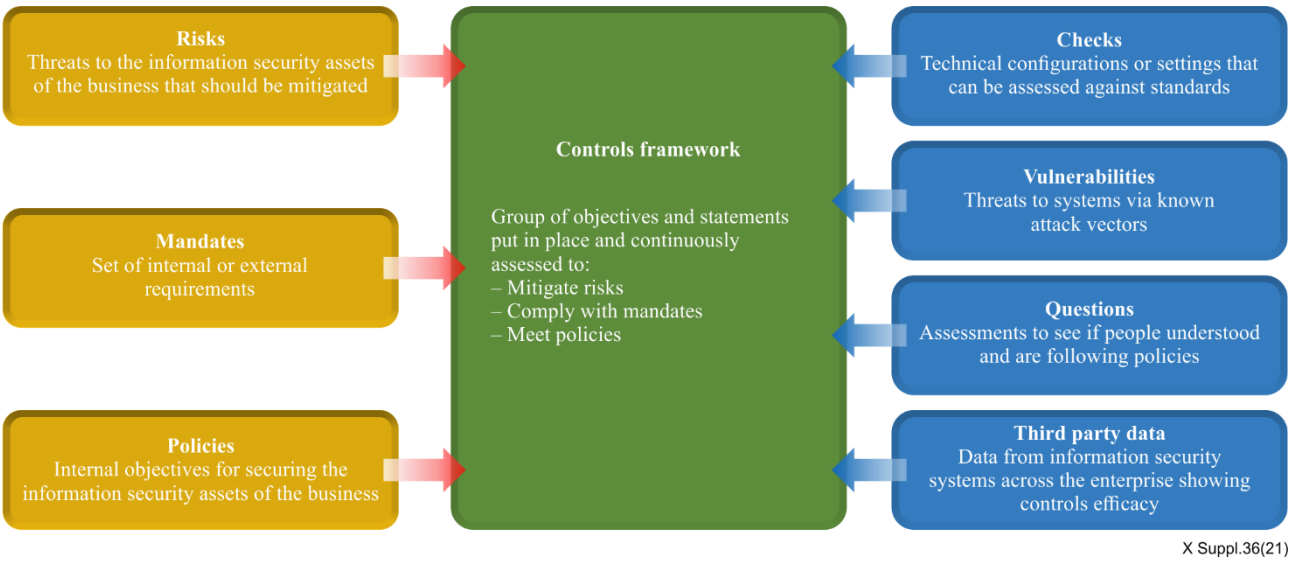

Figure 3 – Critical security control implementation model

The control framework is where the security objectives are continuously assessed to mitigate risks. The control framework provides a set of security requirements to comply with mandates and to meet policies that are associated with CSC objectives and statements. For each statement, a control with an associated test is established based on underlying technology or requirements.

Automation is a critical requirement in the process of collecting the technical evidence directly from the assets (operating system, application, network, etc.) and to run periodical assessments for procedural controls. For each iteration, the information is automatically stored and ready to be used to measure compliance status and risk posture, and to propose remediation steps.

The four types of assessment to ensure compliance are: checks; vulnerabilities; questions; and third party data.

12.1 Policy management and mapping

As shown in Figure 4, based on the control statement, organization policies should be linked to assess their security effectiveness.

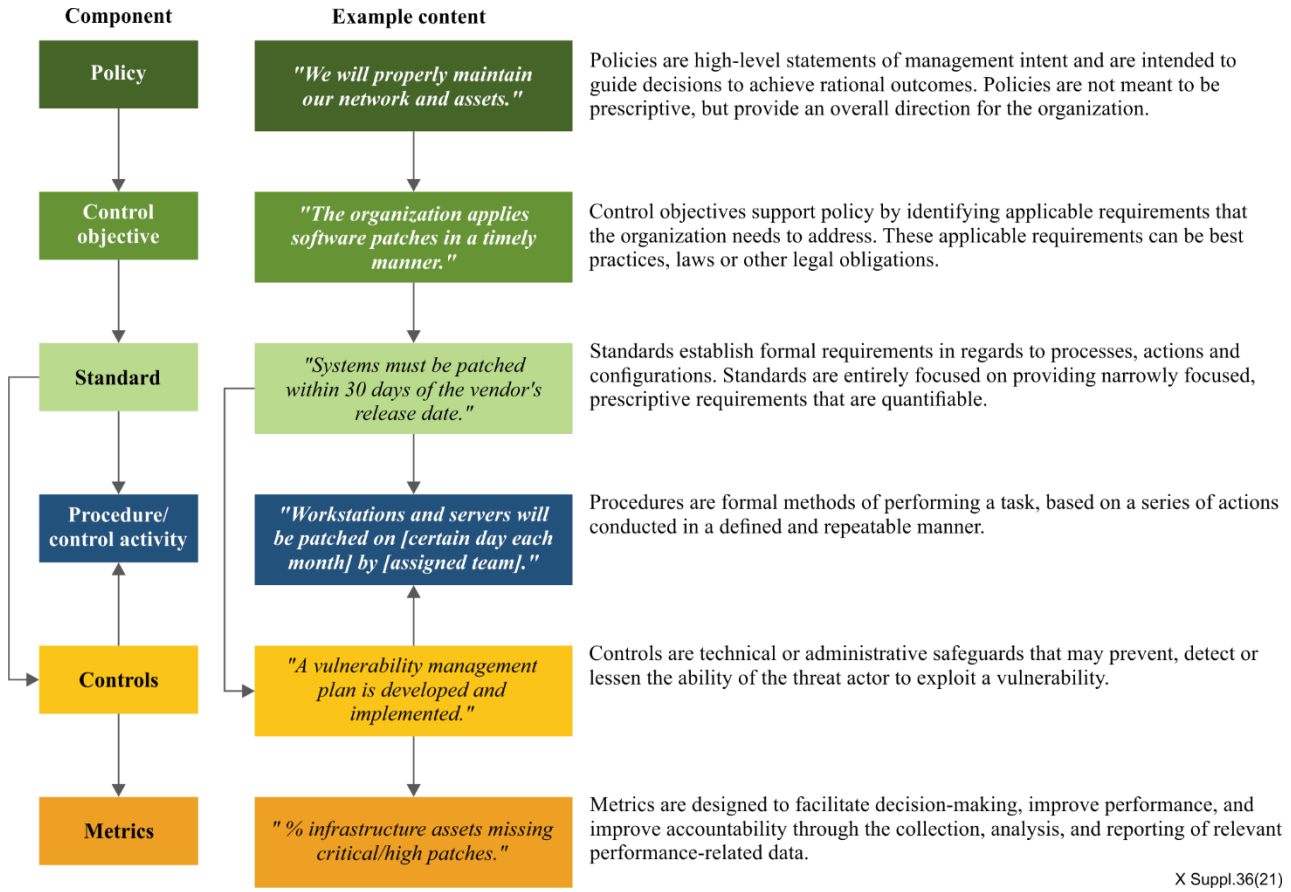

Figure 4 – Policy management and its mapping

The example in Figure 4 maps both mandate and policy to a control statement; the organization can then review the effectiveness of each CSC and procedure, based on the metrics used.

12.2 Risk monitoring and mapping

The coverage of the control statement may be extended to map the organization risk objectives and policies [b-ETSI TR 103 305]. The risk objectives of the organization can then be correlated with its security policies for effective security risk monitoring. Table 2 lists an example of the control mapping as part of security risk management ([b-HIPAA 45 CFR § 164.312], [b-HIPAA 45 CFR § 164.308], [b-NERC Standard CIP–007–4a], [b-NIST SP 800-53], Requirement 3.1 of [b-PCI DSS], ISMS of [b-ISO/IEC 27002]).

Table 2 – Risk monitoring and its mapping

Control statement	**Definition**	**CIS benchmarks**	
User account management	**User account activations, terminations, and modifications are properly managed.**	Platform	Control
Critical security control	CSC 16.2	W10	2.3.1.5
[b-HIPAA 45 CFR § 164.312]	164.312(d)	Debian 8	
[b-NERC Standard CIP–007–4a]	R5.3.2	W2016	2.3.1.5

Table 2 – Risk monitoring and its mapping

Control statement	Definition	CIS benchmarks	
[b-NIST SP800-53]	AC-2 (1), AC-2 (6), AC-2 (10), AC-2 (11)		
[b-PCI DSS]	12.5.4		
[b-ISO/IEC 27002]	9.2.1		
Privileged account activity logging	**Privileged account activity is logged.**	Platform	Control
Critical security control	CSC 5.1, CSC 5.4, CSC 5.5	W10	17.8.1
[b-HIPAA 45 CFR § 164.312]	164.312(b)	Debian 8	8.1.12, 8.1.15, 8.1.16
[b-NERC Standard CIP–007–4a]	R5.3.2, R6.3	W2016	17.8.1
[b-NIST SP800-53]	AC-2(7), AC-6(9), AU-2, AU-2(3), SI-4(20)		
[b-PCI DSS]	10.2.2		
[b-ISO/IEC 27002]	12.4.1, 12.4.3		
IT security incident response procedure	**Procedures for responding to IT security incidents are clearly defined.**	Platform	Control
Critical security control	CSC 19.1	Corporate	Questionnaire
[b-HIPAA 45 CFR § 164.308]	164.308(a)(1)(i), 164.308(a)(6)(i), 164.309(a)(6)(ii), 164.316(b)(1)		
[b-NERC Standard CIP–007–4a]	R1.2		
[b-NIST SP800-53]	IR-1, IR-4		
[b-PCI DSS]	12.10		
[b-ISO/IEC 27002]	12.1.1, 12.6.1, 16.1.1, 16.1.2, 16.1.5, 16.1.7, 6.1.3		
IT vulnerability scans	**IT vulnerability scans are performed periodically.**	Platform	Control
Critical security control	CSC 4.3, CSC 9.3	VM application	Vulnerability found
[b-HIPAA45 CFR § 164.308]	164.308(a)(1)(ii)(A)		Vulnerability risk
[b-NERC Standard CIP–007–4a]	R5.3.2		Vulnerability remediation steps
[b-NIST SP800-53]	IA-5-1		Vulnerability date
Requirement 3.2 of [b-PCI DSS]	8.2.3		
[b-ISO/IEC 27002]	9.4.2, 9.4.3		

Table 2 – Risk monitoring and its mapping

Control statement	Definition	CIS benchmarks	
Data loss prevention controls	**The organizational data is protected from information leakage due to accidental or malicious activity.**	Platform	Control
Critical security control	CSC 13.3, CSC 13.4, CSC 13.6, CSC 13.7, CSC 13.8	DLP application	# Network incident
[b-HIPAA]	None		User behaviour analytics
[b-NERC Standard CIP–007–4a]	None		Tag asset based on data category
[b-NIST SP800-53]	None		
[b-PCI DSS]	None		
[b-ISO/IEC 27002]	8.3.1		

12.3 Need for evidence collection

Evidence should be collected automatically with the CSC implementation model, where the organization can associate each asset result collection with control statements. The result of checks, questions, vulnerability exposures or third party data provides evidence for all control statements used within the scope of the CSCs. Thus, the organization has the capability to manage its cyber threats and security risks more effectively with the following real time end-to-end infrastructure information:

– visibility;
– compliance level;
– IT risk elements;
– control deviation;
– remediation workflow.

Bibliography

[b-ETSI TR 103 305] ETSI Technical Report 103 305 all parts (2018), CYBER; *Critical security controls for effective cyber defence*.

[b-ETSI TR 103 305-1] ETSI Technical Report 103 305-1 V3.1.1 (2018), *CYBER; Critical security controls for effective cyber defence; Part 1: The critical security controls.*

[b-ETSI TR 103 305-2] ETSI Technical Report 103 305-2 V2.1.1 (2018), *CYBER; Critical security controls for effective cyber defence; Part 2: Measurement and auditing*.

[b-ETSI TR 103 305-3] ETSI Technical Report 103 305-3 V2.1.1 (2018), *CYBER; Critical security controls for effective cyber defence; Part 3: Service sector implementations*.

[b-ETSI TR 103 305-4] ETSI Technical Report 103 305-4 V2.1.1 (2018), *CYBER; Critical security controls for effective cyber defence; Part 4: Facilitation mechanisms*.

[b-ETSI TR 103 305-5] ETSI Technical Report 103 305-5 V1.1.1 (2018), *CYBER; Critical security controls for effective cyber defence; Part 5: Privacy enhancement.*

[b-ISO/IEC 27002] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*

[b-HIPAA] Public Law 104-191 (1996-08-21), *Health insurance portability and accountability act*. Washington, DC: US Government. Available [viewed 2021-10-16] at: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

[b-HIPAA 45 CFR § 164.308] HIPAA 45 CFR § 164.308, *Administrative safeguards*. 45 CFR Subtitle A (10–1–07 Edition). Available [viewed 2021-10-16] at: https://www.govinfo.gov/content/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec164-308.pdf

[b-HIPAA 45 CFR § 164.312] HIPAA 45 CFR § 164.312, *Technical safeguards*. 45 CFR Subtitle A (10–1–10 Edition). Washington, DC: US Government. Available [viewed 2021-10-16] at: https://www.govinfo.gov/content/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec164-312.pdf

[b-NERC Standard CIP–007–4a] North American Electric Reliability Corporation Standard CIP–007–4a, *Cyber security – Systems security management*. Available [viewed 2021-10-16] at: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-4a.pdf

[b-NIST SP 800-53] National Institute of Standards and Technology Special Publication 800-53 Revision 5 (2020-12-10) *Security and privacy controls for information systems and organizations.*

[b-PCI DSS] Payment Card IndustryData Security Standard v3.2.1 (2018), *Requirements and security assessment procedures*. Available [viewed 2021-10-16] at: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1634378000206

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021