CYBERSECURITY AND DATA PROTECTION AUDIT GUIDELINE

INTOSAI
Working Group on IT Audit

INTOSAI
Goal Chairs
Collaboration
PSC – CBC – KSC

Quality Assurance Certificate of the Chair of the INTOSAI Working Group on Information Technology Audit (WGITA)

This is to certify that ***Cybersecurity and Data Protection Audit Guideline*** which is placed at level ***2 (two)*** of Quality Assurance as defined in the paper on "Quality Assurance on Public goods developed outside Due Process" approved by the INTOSAI Governing Board in November 2017 has been developed by following the Quality Assurance processes as detailed below:

I. The project proposal was developed by the team in consultation with INTOSAI WGITA members;

II. The project was discussed during the 30th and 31st annual WGITA meeting held virtually, in 2021 and 2022, respectively;

III. A draft document was circulated to the INTOSAI community on 15 July 2022 and was exposed for 45 days (from 15 July 2022 to 30 August 2022) for review and feedback; Feedback received was duly considered for finalization of the document.

IV. The finalized draft document was hosted on the WGITA website and was circulated to WGITA members in October 2022. Additional feedback received was duly considered for the final product.

The product developed is consistent with relevant INTOSAI Principles and Standards. The structure of the product is in line with the drafting convention of non-IFPP documents.

The product is valid till ***25 October 2023*** and if it is not reviewed and updated by ***25 October 2023***, it will cease to be a public good of INTOSAI developed outside the Due Process.

Girish Chandra Murmu
Chair of INTOSAI Working Group on Information Technology Audit

INTOSAI
Goal Chairs
Collaboration
PSC – CBC – KSC

Quality Assurance Certificate of the Chair of Knowledge Sharing and Knowledge Services Committee (KSC)

Based on the assurance provided by the Chair of the ***INTOSAI Working group on Information Technology Audit (WGITA)*** and the assessment by the Goal Chair, it is certified that ***Cybersecurity and Data Protection Audit Guideline*** which is placed at level ***2 (two)*** of Quality Assurance as defined in the paper on "Quality Assurance on Public goods developed outside Due Process" approved by the INTOSAI Governing Board in November 2017 has been developed by following the Quality Assurance processes as detailed in the Quality Assurance Certificate given by the Working Group Chair.

The product is valid till ***25 October 2023*** and if it is not reviewed and updated by ***25 October 2023,*** it will cease to be a public good of INTOSAI developed outside the Due Process.

Girish Chandra Murmu
Chair of Knowledge Sharing and
Knowledge Services Committee

1 Table of Contents

1 Table of Contents 1
I. Introduction 3
1.1 Background 3
1.2 Structure of this guideline document 3
1.3 Audience 4
1.4 Key concepts and definitions 4
1.5 Key Cybersecurity and Data Protection Standards and Frameworks 5
1.6 Cybersecurity and Data Protection Best Practices and Key Methodology 7
2 Guidance during audit phases 8
2.1 Planning and designing an audit 8
2.1.1 Defining the terms of the engagement 8
2.1.2 Defining the scope 9
2.1.3 Audit Skill Requirements 11
2.2 Conducting 12
2.2.1 General Audit Process 12
2.2.2 Define the security baseline 12
2.2.3 Define the method of scoring against the selected framework 13
2.2.4 Principles for specific audit areas 15
2.2.3 Considerations 18
2.2.4 Penetration Testing 19
2.3 Reporting 19
2.3.1 Principles 20
3 Auditing national cybersecurity and data protection 21
3.1 National Cybersecurity Strategy and Governance 21
3.1.1 Importance of Up-To-Date National Cybersecurity Strategies 21
3.1.2 The Three Dimensions: Governmental, National, and International 22
3.1.3 The Five Mandates of National Cybersecurity 22
3.1.4 The Five Dilemmas of National Cybersecurity 22
3.1.5 Cybersecurity and data protection governance and oversight 23
3.1.6 Regulations by country 24
3.1.7 Cybersecurity strategy and program evaluation 27
3.1.8 National Cybersecurity Maturity Evaluation Models 28

3.2 Cybersecurity evaluation to critical processes and resources 30
3.2.1 Critical Infrastructures 30
3.2.2 General Auditing of Critical National Infrastructure 32
3.2.3 Semi-Specific Auditing of Critical National Infrastructure 40
3.2.4 Specific Auditing of Critical National Infrastructure by Sectors 41
3.2.5 National Resilience / Disaster Recovery 46
3.3 Auditing National Cyber Incident Response 51
3.3.1 The role of government entities in charge of cyber incident response. 51
3.3.2 Entities Responsible for National Cybersecurity 51
3.3.3 CERT/CSIRT functions 52
3.3.4 Computer Emergency Response Team (CERT) and Computer Security Incident Response Team (CSIRT) 53
3.3.5 Guide for cybersecurity CSIRT 54
3.3.6 Assessing the maturity level of a CSIRT 59
4 Considerations of cybersecurity and data protection by sector 62
4.1 Key Cybersecurity Guidance and Criteria for Critical Infrastructure Sectors 64
4.2 Challenges, Risks, and Threats for Critical Infrastructure Sectors 64
4.2.1 Cybersecurity threats to critical infrastructure sectors 65
4.3 Considerations for Auditing Critical Infrastructure Sectors 69
4.3.1 Identifying Key Vulnerabilities, Threats, and Actors 69
4.3.2 Identifying Stakeholder Roles and Regulatory Frameworks 72
4.3.3 Identifying Potential Challenges or Audit Findings 73
4.4 Example Audit Reports on Critical Infrastructure 75
4.4.1 Government-Wide Critical Infrastructure Reviews 75
4.1.1. Sector-Specific Critical Infrastructure Reviews 75
Appendix – Acronyms and abbreviations 77

I. Introduction[1]

1.1 Background

Government agencies use information systems and electronic data to carry out their missions. Protecting these systems and the information that resides on them is essential to prevent unauthorized or unintentional exposure, disclosure, or loss that can lead to serious consequences and result in substantial harm to individuals and the government. Specifically, ineffective protection of information technology (IT) systems and information can potentially result in:

Inappropriate access to and disclosure, modification, or destruction of sensitive information;

- Loss or theft of resources, including money and intellectual property;
- Loss of privacy, emotional distress, or reputational harm;
- Loss of public confidence; or
- High costs to remediate the effects of a breach.

These IT systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks. Compounding the risk, systems and networks used by government agencies and critical infrastructure are also often interconnected with other internal and external systems and networks, including the internet. Government agencies and critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on IT systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and security, prosperity, and well-being. Thus, it is imperative to protect the confidentiality, integrity, and availability of this information and effectively respond to data breaches and security incidents when they occur.

1.2 Structure of this guideline document

The purpose of this guideline document is to integrate and facilitate access to useful information and guidance pertaining to cybersecurity[2] and data protection. This document is not meant to be an exhaustive guide for auditors but could be used as a starting point to assist auditors in identifying criteria for further review.

This document includes four chapters to help auditors plan, execute, and report on audits related to cybersecurity and data protection. These chapters are:

Chapter	Description
1. Introduction	Provides an overview of the rest of the guide, including key definitions, concepts, and best practices.

[1] Please be informed that the reach of this document is to provide auditors / audit public an initial overview of the state that cybersecurity and data protection guard under a global reach hoping to deepen on the subjects referred in a second part of the document.

[2] For consistency purposes, throughout the document the term “cybersecurity” is used instead of “cyber security”.

2. Guidance during audit phases	Provides general guidance on the planning, conducting, and reporting phases of an audit, including the principals for conducting cybersecurity and data protection audits.
3. Auditing national cybersecurity and data protection	Provides highlights on a) the importance of national cybersecurity strategies and attributes of such a strategy, b) national cybersecurity considerations in terms of critical processes such as critical infrastructures, and c) examples of national and regional cybersecurity benchmark studies.
4. Considerations of cybersecurity and data protection by sectors	Provides an overview of critical infrastructure sectors, such as the financial, communications, and energy sectors; key threats to such sectors; considerations for auditing critical infrastructure sectors; and examples of relevant reports for several sectors.

1.3 Audience

This guide is intended for use by auditors responsible for reviewing cybersecurity and data protection. Auditors may use the information presented in this document to help facilitate their planning, evaluating, and reporting of audits. The material presented in this document assumes that the reader has a general knowledge of auditing standards.

1.4 Key concepts and definitions

- **Access controls:** Include both logical and physical controls related to, among other things, protection of system boundaries, identification and authentication, and physical security of facilities.
- **Availability:** Ensuring timely and reliable access to and use of information.
- **Cloud security:** A combination of policies, controls, procedures, and technologies that work together to protect cloud-based infrastructures and systems.
- **Compliance controls:** Controls that enforce information security requirements and deal with privacy laws and cybersecurity standards designed to minimize security threats.
- **Confidentiality:** Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- **Critical infrastructure:** Refers to systems and assets, whether physical or virtual, so vital to a country or organization that their incapacity or destruction would debilitate national security, economic stability, public health or safety, or any combination of these.
- **Cybersecurity:** Protection and restoration of technology such as computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, to ensure its availability, integrity, and confidentiality.
- **Data privacy:** Assurance that the confidentiality of, and access to, certain information about an entity is adequately protected.
- **Data protection:** The practice or process of safeguarding information from corruption and loss.
- **Information security:** The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Integrity:** Guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity.
- **Network security:** A practice of securing networks against unauthorized access, misuse, interference, or interruption of service.
- **Personally identifiable information (PII):** Any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or identification number, and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.
- **Procedural controls:** Controls, including security awareness education, security frameworks, compliance training, and incident response plans and procedures, that prevent, detect, or minimize security risks to any physical assets such as computer systems, data centers, and even filing cabinets.
- **Technical controls:** Security controls for an information system that are implemented and executed through mechanisms in the hardware, software, or firmware components of the system.

1.5 Key Cybersecurity and Data Protection Standards and Frameworks

This section provides a description of relevant best practices across all of the chapters of the guide. This section is not meant to be an exhaustive list of best practices but can help serve as an audit starting point.

Practice (with link)	Description
ISO/IEC 27000:2018 Information technology security techniques	This document, The ISO Information Security Management system (ISMS), includes standards that, among other things, provide direct support, detailed guidance and/or interpretation for the overall process to establish, implement, maintain, and improve an ISMS and address sector-specific guidelines for ISMS.
National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1	This publication describes a voluntary risk management framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risk.
NIST Privacy Framework	This framework is intended to help organizations identify and manage privacy risk so they can build innovative products and services while protecting individuals' privacy.
NIST Special Publication 800-34: Revision 1, Contingency Planning Guide for Federal Information Systems	This document provides instructions, recommendations, and considerations for federal information system contingency planning.
NIST Special Publication (SP) 800-37, Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle	This document describes a risk management framework, that provides a structured and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.

Approach for Security and Privacy	
NIST SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View	This document provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations resulting from the operation and use of federal information systems.
NIST SP 800-53A Rev 5: Assessing Security and Privacy Controls in Federal Information Systems and Organizations	This document provides guidelines for building effective security and privacy assessment plans and procedures for assessing the effectiveness of security controls and privacy.
NIST SP 800-53B: Control Baselines for Information Systems and Organizations	This provides suggested security and privacy control baselines for each system impact level—low-impact, moderate-impact, and high-impact—as well as a privacy baseline.
NIST SP 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations	This document provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets from a set of threats and risks, including hostile attacks, human errors, natural disasters, and privacy risks.
NIST SP 800-55 Rev. 1: Performance Measurement Guide for Information Security	This document provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate nonproductive controls.
NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide	This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.
NIST 800-82 Rev. 2: Guide to Industrial Control Systems (ICS) Security	This document provides guidance on how to secure industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.
NIST SP 800-115: Technical Guide to Information Security Testing and Assessment	This document provides guidance to assist organizations in planning and conducting technical information security tests and examinations, analyzing findings, and developing mitigation strategies. The guide provides practical recommendations for designing, implementing, and maintaining technical information security test and examination processes and procedures. These can be used for several purposes, such as finding vulnerabilities in a system or network and verifying compliance with a policy or other requirements.

NIST SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations	This special publication was developed to assist organizations in the development of a continuous monitoring strategy and the implementation of a continuous monitoring program providing visibility into organizational assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls.
NIST SP 800-161, Rev 1 (Final): Supply Chain Risk Management Practices for Federal Information Systems and Organizations	This document provides guidance to organizations on identifying, assessing, and mitigating cyber supply chain risks.
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27	This regulation requires entities to manage data securely by implementing "appropriate technical and organizational measures." Technical measures mean anything from requiring employees to use two-factor authentication for accounts where personal data is stored to contracting with cloud providers that use end-to-end encryption. Organizational measures are things like training staff, adding a data privacy policy to the employee handbook, or limiting access to personal data only to those employees who need it.

1.6 Cybersecurity and Data Protection Best Practices and Key Methodology

The methodology listed below may be more prescriptive and assist an auditor in completing audits in a repeatable manner. These may include steps to be taken in an audit, explain why the steps are important, and how an auditor should complete each step.

Methodology (with link)	Description
NIST SP 800-53A Rev 5: Assessing Security and Privacy Controls in Federal Information Systems and Organizations	This document provides guidelines for building effective security and privacy assessment plans and procedures for assessing the effectiveness of security controls and privacy.

2 Guidance during audit phases

2.1 Planning and designing an audit

This section will define high-level principles for planning and designing of cybersecurity audits. The principles will provide guidelines on:

- Defining the terms of the engagement; and
- Defining the scope.

2.1.1 Defining the terms of the engagement

The audit should consider the cybersecurity requirements and goals of an organization. This will entail analyzing industry trends to identify emerging cybersecurity risks and engaging with senior management to understand their expectations. Understanding the organization´s cybersecurity requirements and goals will help with identifying risks to the organization and defining the audit objective.

The following are examples of cybersecurity goals[3].

- Emerging risk is reliably identified, appropriately evaluated and adequately treated.
- Cybersecurity policies, standards and procedures are adequate, effective and comply with regulations.
- Cybersecurity transformation processes are defined, deployed and measured.
- Attacks and breaches are identified and treated in a timely and appropriate manner.

The organization's cybersecurity requirements and goals can be identified from the following sources:

- Government regulations and policies;
- Frameworks, policies and procedures;
- Organization charts;
- Terms of reference;
- Minutes of meetings;
- Internal reports;
- External reports; and
- Intranet Site.

The audit objective should provide management with an assessment of the effectiveness of cybersecurity processes, policies, procedures, governance and controls. The assessment should focus on:

- The use of cybersecurity frameworks, standards, guidelines;
- Design of processes, procedures and controls; and
- Implementation of relevant controls.

The following provides examples of audit objectives[4]:

- Provide management with an assessment of their cybersecurity policies and procedures and their operating effectiveness;

[3] Source: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2019/volume-2/auditing-cybersecurity_joa_eng_0319

[4] Source: ISACA, IS Audit/Assurance Program, Cybersecurity: Based on the NIST Cybersecurity Framework

- Confirm the systems in place meet minimum compliance requirements;
- Identify security control concerns that could affect the reliability, accuracy and security of the enterprise data due to weaknesses in security controls; and
- Evaluate the effectiveness of response and recovery programs.

2.1.2 Defining the scope

The audit scope should be based on the audit objectives. The audit objectives should be used to define the areas and aspects of cybersecurity to be covered. The following should be considered when defining the audit scope:

- Organization's systems, IT architecture and information assets;
- Organization's risk management and cybersecurity frameworks;
- Government and regulatory security frameworks; and
- Baseline cybersecurity framework.

2.1.2.1 Risk-based Approach to Cybersecurity

The above factors will assist with understanding the organization's approach to cybersecurity. The following provides a model for implementing cybersecurity using a risk-based approach[5].

2.1.2.2 Risk-based Approach to Cybersecurity

Steps	Description
1. Define the system	Determine the type, value and security objectives for the system based on an assessment of the impact if it were to be compromised.
2. Risk assessment	Assess the vulnerability of key assets and the key controls to mitigate against the risks identified.
3. Select controls	Select controls for the system and tailor them to achieve desired security objectives.
4. Implement controls	Implement controls for the system and its operating environment.
5. Assess controls	Assess controls for the system and its operating environment to determine if they have been implemented correctly and are operating as intended.
6. Authorize the system	Authorize the system to operate based on the acceptance of the security risks associated with its operation.
7. Monitor the system	Monitor the system, and associated cyber threats, security risks and controls, on an ongoing basis.
8. Reporting	Collate audit findings and make recommendations for change or improvement, including recommendations for addressing residual risks or identified weaknesses not mitigated by controls.

Understanding the organization's approach to cybersecurity supports a risk-based approach to the audit. It allows the audit to focus on important areas that are valuable to the organization. The audit can focus on systems and information assets that the organization should protect, and the level of protection the organization should be implementing for

[5] Source: https://www.cyber.gov.au/acsc/view-all-content/advice/using-information-security-manual

stronger security controls. The following considerations can assist with further enhancing the audit scope:

- The prioritization of the defined systems can assist with targeting important systems. Organizations would typically implement security controls for higher priority systems as opposed to those of less importance to the organization;
- The selected controls forms the security baseline for specific systems and, in some cases, for all systems. The security baseline can be used as the basis for compliance audits if a legal and regulatory security baseline does not exist;
- The organization's mechanisms for assessing, authorizing and monitoring security controls can provide an early indication of the cybersecurity maturity of the organization. An organization with overarching framework supporting the assessment, authorization and monitoring of security controls is likely to be more mature than those that do not have such a framework; and
- A risk and threat assessment can provide an understanding of specific risks the organization is aiming to mitigate. The risk and threat assessments should provide information on the intrusion process for particular systems. Adversaries execute a series of steps or stages within the intrusion process to execute a cyber-attack. The high-level stages of targeted cyber intrusions are malicious software delivery and execution, network propagation, and data exfiltration. The audit scope should include an assessment of controls related to the intrusion process. This will help assess the organization's ability to mitigate cybersecurity incidents.

2.1.2.3 Risk Management and Security Frameworks

The following organizations and frameworks provide examples of risk management and cybersecurity practices that could be used to assist with scoping the audit:

- US National Institute of Standards and Technology Cybersecurity Framework (CSF);
- Systems and Organizational Controls (SOC);
- The US Sarbanes-Oxley Act of 2002 (SOX);
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC);
- EU General Data Protection Regulation (GDPR);
- Center for Internet Security (CIS) Controls;
- Committee of Sponsoring Organizations of the Treadway Commission (COSO);
- Australian Government Protective Security Policy Framework (PSPF); and
- Australian CyberSecurity Centre (ACSC) Information Security Manual (ISM).

2.1.2.4 Audit Program Development

The following aspects should be considered when developing the audit program:

- A security baseline should be identified to allow for the assessment of a minimum level of protection against in-scope systems and information assets.
- A scoring methodology should be defined to allow for a systematic approach to assessing the performance of cybersecurity controls. The scoring methodology will

be dependent on the audit objective and scope of the audit. The scoring methodology should consider the following components:

- Weighted scores based on the priority or importance of the security control, such as mandatory versus desired controls;
- Level of security control implementation, such as operation versus documented; and
- Strength of audit evidence to support the score, such as inquiry would result in a lower score and reperformance would result in a higher score.

The following provides resources that could assist with defining the security baseline:

- NIST CSF[6];
- Australian Government's Protective Security Policy Framework[7];
- Australian Government's Information Security Manual[8]; and
- UK Security Policy Framework[9].

2.1.3 Audit Skill Requirements

The audit scope and program will determine the security knowledge and expertise required to execute the audit program. The following factors should be considered when determining the audit team members:

- Specialized areas and technologies being audited, such as blockchain, artificial intelligence, encryption, and cloud-computing;
- Tools and technology used to support cybersecurity management within the organization; and
- Tools and technology used by the organization to manage its IT environment.

The following provides a list of areas that audit team members should have skills, expertise and knowledge that would assist with performing an assessment of cybersecurity:

- Cyber and security management governance frameworks, specifically across recognized standards, such as NIST, ISO, PSPF and the ISM;
- Cyber and security legal and regulatory environments, specifically understanding the government's security criteria (requirements, policies, standards and procedures);
- Cyber and information security risk management, specifically performing risk assessments;
- System design and development lifecycles, including agile approaches;
- Security operations management, specifically the management of vulnerabilities and incidents; and
- Common hacking toolkits such as nmap, Metasploit and Kali.

Security expertise may be required to be included in the audit team depending on the areas being reviewed and the type of approach to testing. The following provides a list of security certifications that may assist with addressing the resource requirements.

---

[6] Source: https://www.nist.gov/cyberframework
[7] Source: https://www.protectivesecurity.gov.au/
[8] Source: https://www.cyber.gov.au/acsc/view-all-content/ism
[9]Source: https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework

Certification	Description
Certified Information Systems Security Professional (CISSP)	Experience and skills for designing, implementing, and monitoring a cybersecurity program.
Certified Information Systems Auditor (CISA)	Experience and skills for assessing, designing and implementing security controls.
Certified Information Security Manager (CISM)	Experience and skills for managing information security, including in governance, program development, incident and risk management.
CompTIA Security+	Experience and skills for assessing and monitoring security management across an organization.
CompTIA Cybersecurity Analyst (CySA+)	An IT certification that applies behavioral analytics to networks and devices to prevent, detect and combat cybersecurity threats through continuous security monitoring.
Certified Ethical Hacker (CEH)	Demonstrates knowledge of assessing security of computer systems by looking for weaknesses and vulnerabilities in target systems, using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system.
Certified in Risk and Information Systems Control (CRISC)	A qualification that verifies your knowledge and expertise in risk management.
GIAC Security Essentials Certification (GSEC)	Experience and skills in security operations, such as cyber offense and defense, network security, and incident response.

2.2 Conducting

This section will define principles for conducting the following types of audits:

- Cybersecurity capability/maturity;
- Cyber resilience maturity;
- Data privacy;
- Data protection; and
- Technical configuration.

2.2.1 General Audit Process

Cybersecurity audits can cover several areas within an organization. The execution of cybersecurity audits can be modelled after the audit process listed in section 2.1.2.3.

The principles associated with each audit process is described in the following subsections.

2.2.2 Define the security baseline

The security baseline will provide the basis for assessing the entities performance. The security baseline should be based on the following:

- Security frameworks and standards used by the organization to develop and manage its security management and controls; and
- Security legal and regulatory requirements that govern the organization's business environment.

If the organization has not defined this security baseline, then the security baseline should be selected using the following considerations:

- Security frameworks and standards used in the organization's industry and jurisdiction;
- Security frameworks and standards used in a similar industry and jurisdiction; or
- Internationally recognized frameworks and standards.

The use of international frameworks and standards is suggested as these are likely to have been developed by a wider community of professional associations and experts. A list of example security frameworks and standards has been provided in Planning and designing an audit section.

2.2.3 Define the method of scoring against the selected framework

If the security frameworks and standards do not provide a scoring methodology, the audit team may want to define a scoring methodology based on the selected security frameworks and standards. The following principles may assist with defining a scoring methodology:

- Prioritization of requirement: each framework and standard requirement should be given a priority. This can be determined by the importance of the requirement, where mandatory (must) requirements have a greater score associated and desirable (should) requirements have a lesser score;
- Level of implementation: scores can be allocated to the level of implementation for a requirement or control. Example implementation levels could be based on: documented or designed; implemented or exists; and operational. Operational levels has a higher score than documented controls; and
- Impact on identified risks: scores can be allocated based on the impact a requirement may have on mitigating the risks. This may be necessary as the type of control may have less impact on mitigating the identified cybersecurity risk/threat (i.e., documentation and plans may be unlikely to stop an actual malware attack as opposed to implementing a security configuration within the required system).

The scoring methodology should include the definition of the audit evidence required to support the assessment and score. The audit evidence should support the type of scoring attributes used. The following provides examples of audit evidence and potential score categorization.

Audit Evidence Type	Example	Score
Inquiry	Interviews	Low
Observation	Walkthroughs	Low/Moderate
Inspection	Review security configurations	Moderate/High
Reperformance	Executing a system test	High

The audit team may choose to apply several factors and methods that contribute to an overall score. For example, the following calculation could be applied.

Requirement Score = (Level of Implementation) X (Prioritization) X (Impact on identified risks)

A range of scores should be defined to allow for reporting of performance, specifically against the baseline security requirements. This can provide an indication of the gap against required security control implementation, capability or maturity.

2.2.3.1 Define the audit procedures to support the collection of audit evidence

The audit procedures will be dependent on the areas being reviewed. The following principles should be considered when designing audit procedures:

- Audit procedures should be based on the framework and standards. This will ensure that the audit evidence will support the assessment against the applicable requirements;
- Audit procedures should be developed with the support from policy and operational specialists. This will ensure that the methods used for assessing against frameworks are likely to align to expectations of policy and operational specialists;
- Audit procedures should be aligned to the scoring methodology. If a score is based on the specific configuration of a security control, then audit procedures need to be developed to inspect security configurations against the required standard (e.g., password configurations); and
- Audit procedures should consider the use of security tools, especially those within the organization. The use of security tools could increase the effectiveness and efficiency of audit procedures. For example, the use of a vulnerability scanning tool may reduce the need to source security data from systems through scripts and programs. Vulnerability scanning and Security Information and Even Management (SIEM) tools are useful tools to incorporate into audit procedures. If the security tools are in-house developed or highly customized, then procedures may need to be performed to assess the integrity of the security tool and the reports being generated.

The following provides sources of audit programs that may assist with designing audit procedures:

- NIST, Technical Guide to Information Security Testing and Assessment, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- ACSC, Cloud Assessment and Authorization – Frequently Asked Questions, https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-assessment-and-authorisation-frequently-asked-questions
- ISACA, Auditing Cybersecurity, https://www.isaca.org/resources/isaca-journal/issues/2016/volume-1/auditing-cybersecurity
- ACSC, Information Security Manual, https://www.cyber.gov.au/acsc/view-all-content/ism

- ISACA, IS Audit Basics: Audit Program, https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/is-audit-basics-audit-programs

2.2.3.2 Perform audit procedures

The audit procedures should be performed as planned and managed as per the relevant auditing standards and quality management processes within the audit team's organization. The following principle should be considered when performing audit procedures:

- Requirements that deviate from the security requirements should be supported by a risk assessment. Organizations may choose to deviate from a security requirement based on their specific circumstances. This deviation should at least be supported by a robust assessment of associated risks and this should be managed through the organization's security governance processes.

2.2.3.3 Assess the audit evidence and apply a score to the areas audited

The audit evidence should be assessed using the planned scoring methodology. The scores may need to be adjusted depending on the type of audit being performed. For example, if the audit is assessing compliance, then the scores could be quite strict as a deviation is seen as non-compliance or an exception. However, a performance audit focused on assessing the management of cyber risks may include the evidence of risk assessments as a factor into the performance score. It is best to determine this when defining the scoring methodology.

2.2.3.4 Assess the risks and impact associated with exceptions

An assessment of the risks associated with exceptions would be applicable to any audit engagement. This assessment should reflect back to the audit objective and the information gathered during the planning stage of the audit. Further, the auditor is required to report its findings to those charged with governing the organization. This assessment can provide:

- Insights into what risks could impact an organization to achieving business objectives;
- Information to support decision making on security initiatives and projects; and
- Support for adjusting the financial statement audit program to ensure appropriate assurance is obtained.

2.2.4 Principles for specific audit areas

2.2.4.1 Cybersecurity capability/maturity

An audit of cybersecurity capability/maturity should include a review across the following areas:

- Cybersecurity strategy;
- Cybersecurity risk management;
- Program management and governance;

- Regulatory and legal requirements;
- Threat and vulnerability management;
- Security incident management;
- Security Monitoring;
- Workforce management;
- Third-party management; and
- Data protection.

The following provides references to guidance to assist with auditing cybersecurity capability/maturity:

- NIST, Cybersecurity Framework, https://www.nist.gov/cyberframework
- Office of Cybersecurity, Energy Security, and Emergency Response, Cybersecurity Capability Maturity Model (C2M2), https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
- Office of the Under Secretary of Defense, Cybersecurity Maturity Model Certification (CMMC), https://www.acq.osd.mil/cmmc/
- ACSC, Essential Eight Maturity Model, https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

2.2.4.2 Cyber resilience maturity

An audit of cyber resilience maturity should include a review across the following areas:

- Business impact analysis;
- Business continuity planning;
- Disaster recovery planning;
- Security incident management;
- Threat and vulnerability management;
- Security monitoring;
- Third-party management; and
- Workforce management.

The following provides references to guidance to assist with auditing cyber resilience maturity:

- MITRE, Cyber Resiliency Engineering Framework, https://www.mitre.org/sites/default/files/pdf/11_4436.pdf
- MITRE, Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring, https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

2.2.4.3 Data Protection

An audit of data protection should include a review across the following areas:

- Data governance;
- Regulatory and legal requirements;

- Data classification;
- Data security;
- Data quality management;
- Information records management; and
- Data loss prevention.

The following provides references to guidance to assist with auditing data protection:

- NIST, Security and Privacy Controls for Information Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
- Information Commissioner's Office (ICO), Auditing data protection: a guide to ICO data protection audits, https://ico.org.uk/media/1533/auditing_data_protection.pdf
- Information Commissioner's Office (ICO), Data Protection Impact Assessments, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
- ISACA, Best Practices for Privacy Audits, https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2020/volume-6/best-practices-for-privacy-audits

2.2.4.4 Technical Configuration

An audit of technical configurations should include a review across the following areas:

- Hardening standards;
- Configuration management;
- Security build and testing;
- Development lifecycles;
- Patch management; and
- Vulnerability management.

The following provides references to guidance to assist with auditing the above areas:

- ACSC, Guidelines for System Hardening, https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-system-hardening
- ACSC, Hardening Linux Workstations and Servers, https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-linux-workstations-and-servers
- ACSC, Hardening Microsoft Windows 10 version Workstations, https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-10-version-21h1-workstations
- ACSC, Web Hardening Guidance, https://www.cyber.gov.au/acsc/government/web-hardening-guidance
- ACSC, Securing PowerShell in the Enterprise, https://www.cyber.gov.au/acsc/view-all-content/publications/securing-powershell-enterprise

2.2.3 Considerations

This section will outline the considerations of IT risk and complexity, multi-organization audits and the advantages and disadvantages od penetration testing.

2.2.3.1 IT Risk and Complexity

Cybersecurity is important for any organization and the cybersecurity audit should consider the organization's cybersecurity risks. A good indicator of cybersecurity risks is an organization's attack surface. The attack surface is the amount of ICT equipment and software used by an organization. The greater the attack surface, the greater the opportunities for adversaries in finding vulnerabilities to exploit. An organization with a large attack surface or high cybersecurity risk rating should have a greater level of protection measures or should have a more sophisticated cybersecurity implementation. The following table provides examples of small, medium and large organizations:

	Attack Surface/Cybersecurity Risk Rating		
	Small/Low	**Medium/Moderate**	**Large/High**
Organization's Environment	- <10 ICT equipment and software - IT management is managed by business teams - All systems are Commercial-Off-The-Shelf (COTS) implementations - No internet-facing systems	<250 ICT equipment and software	>250 ICT equipment and software

The following table outlines a model that could be used to determine the extent of audit testing required and has suggested areas of focus:

	Attack Surface/Cybersecurity Risk Rating		
	Small/Low	**Medium/Moderate**	**Large/High**
Extent of Testing	- Inquiry and inspection procedures. - Assess high-level security documentation, such as policies, procedures and work instructions. - Assess for: automation of updates, backup and recovery, multi-factor authentication, and cybersecurity training. - Assess assurance mechanisms, management reporting and self-assessment/reporting. - Conduct interviews of Executive Boards and Chief Security Officers.	Inquiry, Inspection and Observation.	Inquiry, Inspection, Observation and Reperformance.

The following is a list of sources of information that will assist with determining the attack surface and/or cybersecurity risk rating:

- Hardware and software asset registers;
- Architecture and Network diagrams;
- Organizational Structure Diagrams; and
- Access Control Listings, specifically privileged users with access to administrative functions on networks, databases and applications.

2.2.3.2 Multi-organization Audits

The auditor may need to adjust their approach when auditing multiple organizations. The guidance provided is focused on performing an audit of an organization or can be scaled to include a small number of organizations. The auditor may want to consider the use of surveys, questionnaires, or self-reporting to support gathering of audit evidence. The following should be considered when taking this approach.

Survey and questionnaire design should focus on obtaining sufficient and appropriate evidence to support the assessment against the scoring methodology and audit criteria. The design should provide details on evidence requirements, especially for supporting the responses provided by organizations. For example, an organization who states that they have met regulatory requirements for implementing patch management standards needs to provide evidence supporting its response. The auditor should provide examples of evidence to assist the accuracy of survey responses.

2.2.4 Penetration Testing

Penetration testing is an approach that can provide information on the performance of security controls. The following are some advantages and disadvantages of using penetration testing to support audit activities.

2.2.4.1 Advantages

- Penetration tests can provide direct evidence of controls operating effectively. It may provide greater evidence of the impact of control weaknesses as opposed to highlighting the potential for an incident occurring; and
- Penetration tests can be more efficient as some tests can be automated.

2.2.4.2 Disadvantages

- Limiting the scope of penetration testing reduces the attack surface and reduces the likelihood of identifying gaps in cybersecurity strategies. Conversely, allowing greater scope may not directly test the performance of a control, however, it would provide insights into broader problems within the security architecture;
- Poorly designed penetration tests and processes may result in creating security vulnerabilities or be used by adversaries to disguise malicious activities. It is important for audit teams to ensure that vulnerabilities identified and/or created during and after penetration testing are appropriately managed and rectified. The audit team needs to restore the organization’s systems back to its original state; and
- Auditors need to have the necessary skills and expertise to perform penetration testing, such as use of tools and restoration of systems.

2.3 Reporting

The audit team will review the audit evidence in order to reach a conclusion or issue an opinion. The audit team should evaluate whether the audit evidence obtained is sufficient and appropriate so as to reduce the audit risk to an acceptably low level. The evaluation should consider evidence to determine if it supports or contradicts the conclusions, audit

report or audit opinion. The following are principles to consider when reporting cybersecurity audit results.

2.3.1 Principles

For audit reports that will be published to the public, the following should be considered:

- Information included in the report should be reviewed to determine whether it increases the cybersecurity risks to the organization and/or nation. This assessment is important as information provided, which typically is not available in the public forum, can assist adversaries in accelerating a cyber-attack. The auditor should engage the policy and operational cybersecurity specialists to discuss the associated risks. The following are strategies for reducing the risks associated;
    - Information that is not publicly available should not be included in the report.
    - Names of systems, tools, staff and teams should be removed if possible.
    - Security information such as security monitoring processes, security configurations, and vulnerabilities should not be included in the report, and more importantly, connected to systems or organizations;
- The materiality of the information can be used to exclude information from the report. If security related information, such as vulnerabilities, can be excluded without affecting the conclusions then that information should be removed. The auditor will need to balance accountability and transparency against security risks; and
- The auditor can aim to aggregate and generalize security information to reduce the risks of security controls being attributed to specific systems.

3 Auditing national cybersecurity and data protection

To develop national cybersecurity and data protection audits, this document provides relevant information and reference on the following themes:

- National Cybersecurity Strategy and Governance;
- Cybersecurity evaluation to critical processes and resources; and
- National Agencies / government entities Cybersecurity Assessment.

This is in order to provide the reader with a general overview on the different ways Cybersecurity and Data Protection has been approached globally speaking.

3.1 National Cybersecurity Strategy and Governance

3.1.1 Importance of Up-To-Date National Cybersecurity Strategies

A national cybersecurity strategy (NCSS) is often the key cornerstone of organizational measures at national cybersecurity level. According to the ITU Guide to developing a national cybersecurity strategy, a national cybersecurity strategy is a comprehensive framework or strategy which must be developed, implemented, and executed in a multi-stakeholder approach, that tackles coordinated action for prevention, preparation, response, and incident recovery on the part of government authorities, the private sector and civil society.

More and more countries are developing NCSS to manage cybersecurity in a more structured way. Such strategies can confer several benefits, including countries convening relevant stakeholders, clarifying national priorities, and planning cybersecurity capacity development.

Any overall strategy that seeks to address National Cybersecurity (NCS) will most likely need to orientate itself according to various parameters: what is the purpose of the strategy? who is the intended audience? These are standard questions for any national security strategy and are independent of the cybersecurity domain. But what is inherent to the cybersecurity topic are more specific questions: firstly, where is the strategy directed at, what is its actual purpose, who are the stakeholders? Secondly, how is the cybersecurity domain segmented, and how are the different interpretations of NCS understood? And thirdly, how does this all relate to the wider well-being of the nation?

For these last three questions the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) suggests three conceptual tools to help focus strategic deliberations: respectively, they are termed the ‘three dimensions’, the ‘five mandates’, and the ‘five dilemmas’ of national cybersecurity. Together they provide for a comprehensive view of the topic. Not all NCSS will want to provide equal weight to the different aspects of national cybersecurity described in their Manual. Therefore, these tools are intended to provide an overview of what aspects can be considered, rather than a checklist of what should be taken into account. (of what should be done.)

3.1.2 The Three Dimensions: Governmental, National, and International

Any approach to a NCS strategy needs to consider the 'three dimensions' of activity: the governmental, the national (or societal) and the international.

3.1.3 The Five Mandates of National Cybersecurity

Within the general context of discussing national cybersecurity, it is important to keep in mind that this is not one single subject area. Rather, it is possible to split the issue of NCS into five distinct perspectives or 'mandates', each of which could be addressed by different government departments. This split is not an ideal state, but it is a reality due to the complexity and depth of cybersecurity as a whole: Military Cyber, Counter Cyber Crime, Intelligence and Counterintelligence, Critical Infrastructure Protection, National Crisis Management and Cyber Diplomacy and Internet Governance.

3.1.4 The Five Dilemmas of National Cybersecurity

National cybersecurity is a tool to reach a desired state of affairs (desired situation, not an end). Most nations define a strategic goal of a safe and secure environment within which they can achieve full economic potential and protect citizens from various cyber and non-cyber related risks, both domestic and foreign. To achieve this, NCS must deal with its own, overarching set of 'national cybersecurity dilemmas'. In international relations theory, the traditional 'security dilemma' states that both a country's security strength and its weakness can create unfavorable reactions in their adversaries. The NCS Dilemmas are, however, different: both a strong and a weak NCS posture can have economic and social costs:

1. Stimulate the Economy vs. Improve National Security.
2. Infrastructure Modernization vs. Critical Infrastructure Protection.
3. Private Sector vs. Public Sector.
4. Data Protection vs. Information Sharing.
5. Freedom of Expression vs. Political Stability.

For more information:

Document	Link
National Cybersecurity Framework Manual	https://www.ccdcoe.org/uploads/2018/10/NCSFM_0.pdf
An evaluation framework for Cybersecurity Strategies	https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
A National Cybersecurity Strategy	https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213

3.1.5 Cybersecurity and data protection governance and oversight

Organization	Country	Document	Link
United States Government Accountability Office (GAO)	United States	Cybersecurity Clarity of Leadership Urgently Needed to Fully Implement the National Strategy	https://www.gao.gov/assets/gao-20-629.pdf

The GAO reviewed the contents of the National Cyber Strategy and its associated Implementation Plan dated June 2019. They obtained the content of the Implementation Plan through observation at the request of the NSC not to submit a copy of the plan. From the observation, they transcribed, among other things, the title of each activity and the leadership and support of the federal agencies. They also transcribed sections of each element containing data related to the desirable features of a national strategy developed from our previous GAO work, such as new resources and authorities, targets and deadlines, and designation of levels. They did not transcribe all the information contained in the Plan of Implementation.

They then evaluated the National Cyber Strategy and the transcribed elements of the Implementation Plan to determine whether they collectively possessed the desirable characteristics of a national strategy developed from their prior work by identifying possible indicative statements in the documents.

Guideline

Characteristic	Definition	Required Information	Analysis
Purpose, scope, and methodology	Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed.	Applicable policies, strategies, and laws to confirm the key federal entities with roles and responsibilities in supporting the nation's cybersecurity.	• "This plan was created to…" • "Purpose" statement • Executive summary
Problem definition and risk assessment	Addresses the national problems and threats the strategy is directed towards and entails a risk assessment that includes an analysis of threats, and vulnerabilities of, critical assets and operations.	A risk assessment that includes an analysis of threats, and vulnerabilities of critical assets and operations.	• Risk assessment, including an analysis of threats and vulnerabilities • Issue areas
Goals, subordinate objectives, activities, and performance measures	Addresses what the strategy is trying to achieve, steps to achieve those results, as well as the priorities, milestones, and performance measures to gauge results.	Priorities, milestones, and performance measures to gauge results.	• Milestones for achieving goals • Performance measures for tracking progress • Reporting requirements • Life cycle/time frames • Standards
Resources, investments, and risk management	Addresses what the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted	Cost analysis. Specific risks assessment.	• Analysis of the cost of planned activities • Estimates of how activities will be funded in the future

Characteristic	Definition	Required Information	Analysis
	based on balancing risk reductions with costs.		• Source and type of resources needed to carry out the goals and objectives • Assessment of the specific risks and resources needed to mitigate them
Organizational roles, responsibilities, and coordination	Addresses who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.	Relevant federal officials' interviews to confirm the key federal entities. Cybersecurity-related roles and responsibilities for each federal entity.	• Delegation of responsibilities • Oversight responsibilities • Clarity for individual agencies' response options to specific incidents • Coordination groups • "XX is responsible for…"/ "XX shall..." • "XX will do ___ by doing…"
Integration and implementation	Addresses how a national strategy relates to the goals, objectives, and activities of other strategies, and to subordinate levels of government and their plans to implement the strategy.	Applicable policies, strategies, and laws.	• How strategy is linked to or superseded by other documents and strategies • Describes progress made since previous strategies or plans • Why activities in this plan are prioritized differently than in other plans • Crosswalk(s)

3.1.6 Regulations by country

Regional

Country	Legislation, Best Practices and Certifications in Cybersecurity		
European Union	Cybersecurity regulatory framework in the European Union	**Directive NIS** The main standard approved by the EU on cybersecurity is Directive 2016/1148 of security of networks and information systems (NIS Directive).	https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG
		Cybersecurity law (EU Cybersecurity Act) This Cybersecurity law was approved by the EU in March 2019. It aims to renew and strengthen the EU Cybersecurity Agency (ENISA) and establish a cybersecurity certification framework throughout the EU for products, services, and processes.	https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881
		GDPR The EU General Data Protection Regulation (GDPR) is a regulatory framework for data protection and privacy that came into force on May 25, 2018.	https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU.

Country	Legislation, Best Practices and Certifications in Cybersecurity		
		Digital Operational Resilience Act (DORA) DORA, as an EU regulation, it aims to establish a comprehensive and cross-sector digital operational resilience framework with rules for all regulated financial institutions. It is an important step in creating a harmonized regulatory framework for the operational resilience of financial services in EU law. For the first time, it will bring together the rules that address the risk of ICT in finance in a single piece of legislation. The rules are intended to cover a wide range of financial services entities and the requirements are applied proportionately based on the size and business profile of the business.	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

Country

Country	Legislation, Best Practices and Certifications in Cybersecurity		
United Estates	Federal Laws	**Cybersecurity Information Exchange Act (CISA)** Its goal is to improve cybersecurity in the United States through the enhanced sharing of cybersecurity threat information and for other purposes. The law allows the exchange of internet traffic information between the US government and technology and manufacturing companies. The bill was introduced in the United States Senate on July 10, 2014 and was approved October 27, 2015.	https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance
		Cybersecurity Enhancement Act of 2014 This law was signed into law on December 18, 2014. It provides an ongoing, voluntary public-private partnership to improve cybersecurity and strengthen cybersecurity research and development, workforce development, and education and public awareness and the preparation.	https://www.govinfo.gov/content/pkg/COMPS-12455/pdf/COMPS-12455.pdf
		Federal Exchange Data Breach Notification Act of 2015 This law requires a health insurance exchange to notify everyone whose personal information is known to have been obtained or accessed because of a breach of the security of any system. Notification must be made as soon as possible but no later than 60 days after discovery of the violation.	https://www.congress.gov/bill/114th-congress/house-bill/555
		National Cybersecurity Breakthrough Protection Act of 2015 This act amends the Homeland Security Act of 2002 to allow the Department of Homeland Security Communications Integration Center (NCCIC) to include tribal governments, information sharing, and analysis centers, and private entities among its non-federal representatives.	https://www.congress.gov/bill/114th-congress/house-bill/1731
Spain	Code of Cybersecurity Law in Spain		https://www.boe.es/biblioteca_juridica/codigos/codigo.php?modo=2&id=173_Codigo_de_Derecho_de_la_Ciberseguridad

Russia	Cybersecurity Regulations	**Federal Law N ° 187-FZ on the security of critical information infrastructure of the Russian Federation** The law, approved in July 2017, establishes the basic principles for ensuring the security of critical information infrastructure, the related powers of Russian state bodies, as well as the rights, obligations and responsibilities of people who own facilities with information infrastructure. critical information, communication providers and information systems that provide interaction. The law requires the implementation of protection measures, assigning the category of protection (according to the statutes) and then registering with the Federal Service for Technical and Export Control, which will oversee supervision in this field.	https://cis-legislation.com/document.fwx?rgn=98928
		Federal Law Nº 152-FZ about personal data The Personal Data Law, passed in July 2006, covers almost all aspects of data protection. Unlike European legislation, the Personal Data Law does not distinguish between data controllers and data processors. Therefore, any person or entity that works with personal data is considered an operator of personal data and is governed by the regulation of the Personal Data Law.	https://eng.pd.rkn.gov.ru/
		Federal Law No. 149-FZ on Information, Information Technologies, and Information Protection (the Information Law) This law has been substantially strengthened with some additional amendments and affects the Russian internet and telecommunications industries. Mobile operators will need to store the recordings of all phone calls and the content of all text messages for a period of six months, which carries huge costs.	https://eais.rkn.gov.ru/docs.eng/ 149.pdf
Portugal	Legislations and Regulations	**Resolution of the Council of Ministers (RCM) No 36/2015, of June 12** Resolution of the Council of Ministers (RCM) No 36/2015, of June 12 The National Cyberspace Security Strategy is committed to deepening networks and information security, as a way to ensure the protection and defense of critical infrastructures and vital information services, and promote the free, safe and efficient use of cyberspace by all citizens, companies and public and private entities	https://files.dre.pt/1s/2015/06/11300/0373803742.pdf
		Order No. 1195/2018, of February 2 The Superior Council for Cyberspace Security (CSSC) is the Prime Minister's specific consultation body for matters relating to cyberspace security.	https://files.dre.pt/2s/2018/02/024000000/03949039 50.pdfh
		Law No.46/2018, of August 13, Establishes the legal framework for cyberspace security, transposing Directive (EU) 2016/1148, of the European Parliament and of the Council, of 6 July 2016, on Ensuring a common level of security for networks and information systems across the European Union. The Cyberspace Security Legal Regime applies to Public Administration entities, critical infrastructure operators, essential service operators, digital service providers, as well as any other entities that use	https://www.cncs.gov.pt/docs/regime-jurdico-da-segurana-do-ciberespao.pdf

		information networks and systems, namely, within the scope of voluntary incident reporting.	
		Resolution of the Council of Ministers (RCM) No 92/2019, of June 5 National Cyberspace Security Strategy (ENSC) 2019-2023 is based on three strategic objectives: maximizing resilience, promoting innovation and generating and securing resources. The implications and needs associated with each of the strategic objectives make it possible to define a general and specific orientation, translated into six intervention axes, which form concrete lines of action aimed at reinforcing the national strategic potential in cyberspace	https://files.dre.pt/1s/2019/06/10800/0288802895.pdf
		Decree-Law No. 65/2021, of July 30 The Cyberspace Security Legal Regime applies to Public Administration entities, critical infrastructure operators, essential service operators, digital service providers, as well as any other entities that use information networks and systems, namely, within the scope of voluntary incident reporting.	https://www.cncs.gov.pt/docs/decreto-lei-65-2021.pdf
		Decree-Law Nº. 20/2022, of January 20 Approves procedures for the identification, designation, protection and resilience of national and European critical infrastructures.	https://files.dre.pt/1s/2022/01/02000/0000200014.pdf
		Regulation No 183/2022, of 21 February; Configures technical instructions for communication between entities and the National Cybersecurity Center.	https://files.dre.pt/2s/2022/02/036000000/0003400039.pdfh

Local

Country	**Legislation, Best Practices and Certifications in Cybersecurity**		
United States	Governmental Laws.	**New York Cybersecurity Laws** This regulation is designed to promote the protection of customer information, as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that robustly addresses its risks.	https://www.dfs.ny.gov/industry_guidance/cybersecurity
		California Consumer Privacy Act The California Consumer Privacy Act, or CCPA, is a state-level law that requires, among other things, that companies notify users of the intent to monetize their data and provide them with a direct means to opt out of such monetization	https://oag.ca.gov/privacy/ccpa

3.1.7 Cybersecurity strategy and program evaluation

Organizational measures examine the governance and coordination mechanisms within countries that address cybersecurity. Organizational measures include ensuring that cybersecurity is sustained at the highest level of the executive and assigning relevant roles and responsibilities to various national entities and making them accountable for the national cybersecurity posture.

The lack of adequate organizational measures can contribute to a lack of clear responsibilities and accountability in the national cybersecurity governance, and it can prevent effective intragovernmental and inter-sector coordination.

3.1.8 National Cybersecurity Maturity Evaluation Models

Overview of analyzed maturity models								
Model Name	**Institution Source**	**Purpose**	**Target**	**Nb of Levels**	**Nb of attributes**	**Assessment Method**	**Results Representation**	**Link**
Cybersecurity Capacity Maturity Model for Nations (CMM)	Global Cybersecurity Capacity Centre University of Oxford	Increase the scale and effectiveness of cybersecurity capacity-building internationally	Countries	5	5 main dimensions	Collaboration with local organization to fine-tune the model before applying it to the national context	Five-section radar	2016 Cybersecurity Report https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean 2020 Cybersecurity Report: https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean
The Global Cybersecurity Index (GCI)	International Telecommunication Union (ITU)	To review the cybersecurity commitment and situation and help countries identify areas for improvement in the field of cybersecurity	Countries	N/A	5 pillars	Self-assessment	Ranking table	Global Cybersecurity Index (GCI) 2018: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf Global Cybersecurity Index (GCI) 2020: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
National Capabilities Assessment Framework (NCAF)	The European Union Agency for Cybersecurity (ENISA)	The framework aims at providing Member States with a self-assessment of their level of maturity by assessing their NCSS objectives, that will help them enhance and build cybersecurity capabilities both at strategic and at operational level.	EU Member States	5	4 clusters	Self-assessment	Ranking table	National Capabilities Assessment Framework: https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

Comparison of Attributes/ Dimensions			
	Cybersecurity Capacity Maturity Model for Nations (CMM)	**The Global Cybersecurity Index (GCI)**	**National Capabilities Assessment Framework (NCAF)**
Levels	Five dimensions divided into several factors themselves including multiple aspects and indicators (Figure 4)	Five pillars including several indicators	The National Capabilities Assessment Framework covers 17 strategic objectives and is structured around four main clusters.
Attributes/ Dimensions	i. Devising cybersecurity policy and strategy; ii. Encouraging responsible cybersecurity culture within society. iii. Developing cybersecurity knowledge; iv. Creating effective legal and regulatory frameworks; and v. Controlling risks through standards, organizations, and technologies.	i. Legal; ii. Technical; iii. Organizational; iv. Capacity-building; v. Cooperation.	i. Cybersecurity governance and standards • Develop a national cyber contingency plan • Establish baseline security measures • Secure digital identity and build trust in digital public services ii. Capacity-building and awareness • Organize cybersecurity exercises • Establish an incident response capability • Raise user awareness • Strengthen training and educational programs • Foster R&D • Provide incentives for the private sector to invest in security measures • Improve the cybersecurity of the supply chain ii. Legal and regulatory • Protect critical information infrastructure, OES, and DSP • Address cyber crime • Establish incident reporting mechanisms • Reinforce privacy and data protection v.Cooperation • Establish a public-private partnership • Institutionalize cooperation between public agencies • Engage in international cooperation

3.2 Cybersecurity evaluation to critical processes and resources

The present introduces the different Techniques to assess and perform risk analysis for critical infrastructure and National Resiliency / Disaster Recovery considering some study cases and audits reports from SAI audits of critical processes and resources.

3.2.1 Critical Infrastructures

One important activity in the development of a National Cybersecurity Strategy (NCSS) is to identify and classify Critical National Infrastructure (CNI) and Critical Information Infrastructure.

Nevertheless, nowadays there is no standard methodology to help nations address this foundational identification task, for that reason we present some examples and guidelines that are used in auditing of critical national infrastructure.

It should be noted that this chapter only provides a brief introduction and points out the importance of having a classification of the critical infrastructures of the countries, which was identified through the study of the audit reports of the different SAIs, however, for greater detail of the execution of audits by sectors to critical infrastructures go to chapter 4 “Cybersecurity and Data Protection by Sectors”.

Critical National Infrastructures (CNI) describes broadly physical and virtual infrastructure that supports virtual nation functions as well as national goals and aspirations, so the incapacity or destruction of such systems and assets would have a debilitating impact on the nation’s **security**, **economic stability, public health or safety, or any combination of these factors**.

Equally, Critical Information Infrastructures (CII) is an important component of Critical National Infrastructure, especially to the extent different national functions rely on information and communications technology (ICT) for their operation.

3.2.1.1 Common Factors to Consider while Preparing for Conducting CNI/CII Assessments

As it has been shown among different countries, identifying CNI/CII is fundamentally a matter of classifying the risk exposure that information and communications technologies introduce to assets and functions that are important to national goals, objectives, and aspirations. The key to determinate risk is designing an effective formal, inclusive, and rigorous governance structure and process to enumerate, define, and validate important cyber risk exposures, in particular developing a consensus on the potential harms of critical infrastructure disruptions to securE the economy and citizens.

Most conventional approaches for dealing with cyber risks are focused on cyber-threats, attack types and vectors rather than on impact (e.g., economic, national security, societal) caused by cyber means. Nowadays, attempts to identify and measure the harm caused by inadequate cybersecurity of critical infrastructures have used various means to express the

severity of the attack. However, a threat-based approach too often encompasses a linear, cause-and-effect analysis of cyber threats. Therefore, a more holistic approach to assessing the effect of cyber threats and attacks requires the inclusion of the concept of cyber harm, which describes the negative impact upon an entity, whether individual, organizational, or national.

Thus, based on the analysis of the different SAI's audit reports the most important principles for effectively formalizing and assessing a CNI/CII includes:

- To identify if there is a mandate or policy from national leadership.
- Technical and policy competence and clear and transparent policy development processes.
- Leveraging existing laws and organizations and public-private relationships to facilitate critical infrastructure identification.
- Developing consensus on CNI/CII identification criteria and policies that are created by active participation of all partners in whatever mechanisms nations use.
- Considerations of the degree of national harm created by elements of risk – threat, vulnerability, likelihood, and predictability as well as the potential cascading consequences of prolonged disruptions.
- Use of international frameworks or standards to assess CNI/CII.
- Assess risks using the method of benchmark, in order to identify certain risk assessment policy and methodological approaches that other countries have used successfully, this is focused on nations that have similar national goals and circumstances.

3.2.1.2 CNI / CII Policy Guidance

Based on the foregoing, national strategies may integrate or update existing CNI/CII policy guidance, legal frameworks, or national programs that address critical infrastructure. When developing policies and strategies to identify CNI / CII, policymakers may consider the following perspective.

- Transactional Perspective:
  The policymakers should understand related international policies, norms, and best practices. They also should explore the CNI/CII identification approaches of other nations to better situate and contextualize the effects of relevant practices, additionally, they should understand the implications of CNI/CII across sectors and borders considering dependences and interdependencies.

- Societal Perspective:
  A key part is to address the potential societal harms associated with the disruption of essential functions supported by critical infrastructure (e.g., healthcare, financial services, food supply). Thinking in terms of how critical service disruptions could impact citizen may uncover perspectives on risks associated with services that have not traditionally been prioritized.

Categories for CNI/CII strategies:
This document contains a compilation of the audits carried out by different Supreme Audit Institutions (SAI's), among which they were classified into three main types as General Auditing of Critical National Infrastructure, Semi-Specific Auditing of Critical National Infrastructure and Specific Auditing of Critical National Infrastructure by Sectors, which are defined as follows:

- General CNI/CII audit with generic procedures, except for Canada, which has a specialized guideline for critical infrastructures.
- Semi-Specific CNI/CII audit with general guidelines.
- Specific CNI/CII audit with specialized guidelines for critical infrastructures.

In any case, it is important to mention that this chapter only makes a brief explanation of the categories identified, as well as the case studies based on the audit reports of different SAIs, however, the details of the execution and the elements that must be consider executing an audit of critical infrastructures for each sector is described in chapter 4, so for further details go to that chapter

3.2.2 General Auditing of Critical National Infrastructure

As it's mentioned, nations may apply different frames of references as they work to identify CNI/CII. Many of them, initially oriented CNI/CII efforts around discrete sectors such as the financial service, energy, or transportation sectors, to identify and address critical ICT assets. This approach has been modified over time to focus more on identifying critical national functions which is intended to facilitate cross-sector views of risk vs. within single sectors and helps account for the possibilities of cascading effects when critical assets are disrupted.
And that is why, many countries perform a general audit of Critical National Infrastructure, focused on the impact of cybersecurity attacks in the society.

Therefore, we present the use cases based on different SAIs reports, that perform a general audit of critical infrastructure, to encourage cybersecurity audits to create an applicable and locally adoptable guides that helps countries to develop and implement processes for CNI/CII identification, as follows:

3.2.2.1 Canada
The goal of the *National Strategy for Critical Infrastructure* is to build a safer, more secure and more resilient Canada. To this end, the National Strategy advances more coherent and complementary actions among federal, provincial, and territorial initiatives and among the ten critical infrastructures sectors listed below:

- Energy and utilities
- Information and communication technology
- Finance
- Health
- Food
- Water
- Transportation

- Safety
- Government
- Manufacturing

The National Strategy supports the principle that critical infrastructure roles and activities should be carried out in a responsible manner at all levels of society in Canada. Responsibilities for critical infrastructure in Canada are shared by federal, provincial, and territorial governments, local authorities and critical infrastructure owners and operators – who bear the primary responsibility for protecting their assets and services.

The National Strategy is based on the recognition that enhancing the resiliency of critical infrastructure can be achieved through the appropriate combination of security measures to address intentional and accidental incidents, business continuity practices to deal with disruptions and ensure the continuation of essential services, and emergency management planning to ensure adequate response procedures are in place to deal with unforeseen disruptions and natural disasters.

Objective

The purpose of the *National Strategy for Critical Infrastructure* (the Strategy) is to strengthen the resiliency of critical infrastructure in Canada. The Strategy works toward this goal by setting the direction for enhancing the resiliency of critical infrastructure against current and emerging hazards.

Scope and Methodology

To be effective, the National Strategy must be implemented in partnership among all levels of government and critical infrastructure sectors. Critical infrastructure owners and operators have the expertise and information that governments need to develop comprehensive emergency management plans. In turn, governments will share relevant information in a timely manner, respecting existing federal, provincial, and territorial legislation and policies, to help owners and operators assess risk and identify best practices. This partnership approach recognizes that more resilient critical infrastructure helps foster an environment that stimulates economic growth, attracts, and retains business, and creates employment opportunities. Governments bring value to the partnership through activities such as:

- providing owners and operators with timely, accurate, and useful information on risks and threats;
- ensuring industry is engaged as early as possible in the development of risk management activities and emergency management plans; and
- working with industry to develop and prioritize key activities for each sector.

The *National Strategy for Critical Infrastructure* represents the first milestone in the road ahead. It identifies a clear set of goals and objectives and outlines the guiding principles that will underpin our efforts to strengthen the resiliency of critical infrastructure. The National Strategy establishes a framework for cooperation in which governments and owners and operators can work together to prevent, mitigate, prepare for, respond to, and recover from disruptions of critical infrastructure and thereby safeguard the foundations of our country and way of life.

Frameworks and Guides

- An Emergency Management Framework for Canada

  https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-frmwrk/mrgnc-mngmnt-frmwrk-eng.pdf
- National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure

  https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/index-en.aspx
- National Cybersecurity Strategy

  https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

Conclusions

Federal, provincial, and territorial governments will work together to monitor the implementation of the Strategy and support the assessment of programs and activities targeted at enhancing the resiliency of critical infrastructure in Canada. It is expected that the collaborative approach established in the Strategy will remain evergreen and strengthen coherency of action among all levels of government and critical infrastructure sectors.

The Strategy is to be read in conjunction with the Action Plan for Critical Infrastructure, which will be reviewed three years after launch and every five years thereafter.

3.2.2.2 Turkey

With the 2016-2019 National e-Government Strategy and Action Plan, the Turkish Court of Accounts (TCA) bears responsibility for “Ensuring the Efficiency of Audit for e-Government Projects in Public Sector”. In this context, the TCA has created an audit model for e-Government projects, prepared a draft audit guideline concordant with the model and carried out a pilot audit on GocNet e-Government Project, which is executed by Ministry of Interior, Directorate General of Migration Management.

Objective

The objective of the audit is based on the following:

- Examination and evaluation of IT controls, which are set to ensure confidentiality, integrity, availability, reliability, efficiency, effectiveness, and compliance to legislation of the project itself and the IT environment in which it is executed;
- Contributing to the Institution by identifying the problems that may prevent the successful completion of the project and by providing recommendations for taking the necessary precautions; and
- Providing information about the project to its stakeholders through reporting.

Scope and Methodology

In the audit, the methodology determined in the *e-Government Projects Audit Guideline (Draft)* was followed. The Guide has been prepared based on COBIT (Control Objectives

for Information and Related Technologies), ITAF (Information Technology Assurance Framework), PMBOK (Project Management Body of Knowledge).

In this context, the following risk-based audit approach was followed:

1. Identifying the risks related to the Project itself and the IT environment where it is executed;
2. Determination of the controls that can minimize these risks;
3. Examination of whether these controls are established by the Institution, and if so, whether they are functioning effectively;
4. Evaluation of the control weaknesses identified; and
5. Reporting of material control weaknesses to the stakeholders.

Besides the project and the application, itself, the corporate IT environment, and infrastructure (servers, network, databases) and the web (and mobile) structures where the application was put into service have been subject to audit and specific audit tests.

The audit team has determined the modules to be tested according to the following criteria:

- Materiality (The impact of the application on the activities of the Institution and financial statements, etc.);
- Criticality (Integrity, confidentiality, and availability of corporate information, etc.),
- Complexity (Number of users, transaction volume, etc.);
- Technological Infrastructure (Operating system, software development environment, database, etc.);
- Control Environment (Support personnel, documentation, errors, etc.) ; and
- Audit Resources (Time and human resources constraints, etc.).

Frameworks and Guides

GocNet e-Government Project Information Systems Audit
https://www.sayistay.gov.tr/reports/download/3529-gocnet-e-government-project-information-
Control Objectives for Information and Related Technologies (COBIT)
https://www.isaca.org/resources/cobit

Project Management Body of Knowledge (PMBOK)
https://www.pmi.org/pmbok-guide-standards/foundational/pmbok?sc_camp=D750AAC10C2F4378CE6D51F8D987F49D

Conclusions

As a result of the audit, detected control weaknesses have been negotiated with the audited Institution and explained in the Report in such way to include the relevant control area, the associated audit criteria, the level of risk, the relevant legislation and/or standards, the possible effects, actions taken by the auditee and the recommendations thereof.
A follow-up audit will be planned and conducted separately.

3.2.2.3 Korea

Due to the rapid development of Information Communication Technology (ICT), the dependency on information communication in both the private and public sectors have been increasing.

However, instances of cyber terror, such as the paralysis of Nonghyup computer networks (April 2011) and EBS personal information leakage of nearly 4 million users (May 2012) continuously occur, proving that the security of the nation and society are at risk. Based on the foregoing it is necessary to conduct audits in ICT systems including critical infrastructures.

Objective

The Board of Audit and Inspection of Korea (BAI) inspected the overall conditions of cyber safety management of the Ministry of Security and Public Administration (MOSPA) and 35 other organizations, to relieve the societal anxiety and concern derived from cases of information leakage and cyber terror.

Scope and Methodology

The methodology determined by the group was into two steps.

- Personal Information Protection and Management

One of the significant roles of the MOSPA is to supervise and guide the local autonomous entities that implement tasks, which also includes the task of the resident registration search. Regulations state that personal information can only be used within the range of what is necessary**.**

- Establishment of Infrastructure for Information Protection

The MOSPA had developed the Disaster Recovery System (DRS) measure against system breakdowns resulting from natural disaster or acts of cyber terror.

Nevertheless, the MOSPA has not been checking on its regular operations, nor been performing simulation training, as prescribed by regulation, Military Manpower Administration's (MMA) DRS in 2010.

Frameworks and Guides

Audit on Information Security and Cybersecurity Management in Public Organizations
https://bai.go.kr/bai_eng/board/base/list?brdId=BAE_0004
IT Application and Improvement focusing on the Government Information Systems
https://bai.go.kr/bai_eng/board/base/list?brdId=BAE_0006

Conclusions

The BAI recommended the MOSPA to regularly monitor the implementation of tasks of the local autonomous entities regarding resident registration and personal information. According to the BAI, the government officials responsible for perusing resident registration

information for personal use are ordered to receive disciplinary action. Additionally, the malfunctions detected in the MMA's DRS should be analyzed and compensated for.

Finally, the BAI has notified six organizations, including the Korean Local Information Research and Development Institute (KLID), to regularly monitor PCs and to meticulously secure the management of equipment and labor provided to service companies.

3.2.2.4 Australia

In June 2014, ANAO Audit Report No. 50 2013–14, Cyber Attacks: 1. Securing Agencies ICT Systems was tabled in Parliament. The report examined seven Australian Government entities implementation of the mandatory strategies in the Australian Government Information Security Manual (Top Four mitigation strategies). The Top Four mitigation strategies are: application whitelisting, patching applications, patching operating systems and minimizing administrative privileges.

The audit found that none of the seven entities were compliant with the Top Four mitigation strategies and none were expected to achieve compliance by the Australian Government's target date of 30 June 2014.

In this context, the seven entities were: Australian Bureau of Statistics, Australian Customs and Border Protection Service, Australian Financial Security Authority, Australian Taxation Office, Department of Foreign Affairs and Trade, Department of Human Services, and IP Australia.

Objective

The objective for this audit was to assess whether the Australian Taxation Office, the Department of Human Services, and the Department of Immigration and Border Protection are compliant with the Top Four mitigation strategies in the Australian Government Information Security Manual.

To form a conclusion against the audit objective, the ANAO adopted the following high-level assessment criteria:

- Do the entities comply with the Top Four mitigation strategies? and
- Are entities cyber resilient?

Scope and Methodology

This audit is a follow-up audit of the ANAO Performance Audit Report No. 50 2013–14 that was table in June 2014.

The audit objective was to assess whether three of the seven entities assessed in the first audit had achieved compliance with the Top Four mitigation strategies. The three entities were:

- Australian Taxation Office;
- Department of Human Services; and

- Department of Immigration and Border Protection.

These three major Australian Government entities are significant users of technology:

- The Department of Human Services relies on its ICT systems to process $172 billion in payments annually;
- Through its electronic lodgment systems, the Australian Taxation Office collects over $440 billion tax revenue per year; and
- The Department of Immigration and Border Protection electronically processes around seven million visas annually and inspects and examines over two million air and sea cargo imports and exports.

All three entities collect, store, and use data, including national security data and personally identifiable information that can be used to identify, contact, or locate an individual such as date of birth, bank account details, driver's license number, tax file number and biometric data.

The ANAO reviewed records and interviewed relevant personnel from each entity and conducted assessment and tests of controls that underpin the compliance of the Top Four mitigation strategies for each entity.

Frameworks and Guides

- Protective Security Policy Framework

  https://www.protectivesecurity.gov.au/policies
- AGD's PSPF, Security planning and risk management policy,

  https://www.protectivesecurity.gov.au/governance/security-planning-risk-management/
- ISO 31000:2018, Risk management – Guidelines

  https://www.iso.org/standard/65694.html

Conclusions

Recommendation 1.

The ANAO recommends that entities periodically assess their cybersecurity activities to provide assurance that: they are accurately aligned with the outcomes of the Top Four mitigation strategies and entities' own ICT security objectives; and that they can report on them accurately. This applies regardless of whether cybersecurity activities are insourced or outsourced.

- Department of Human Services' response: Agreed.
- Australian Taxation Office's response: Agreed.
- Department of Immigration and Border Protection's response: Agreed.

Recommendation 2.

The ANAO recommends that entities improve their governance arrangements, by:

1. Asserting cybersecurity as a priority within the context of their entity-wide strategic objective;
2. Ensuring appropriate executive oversight of cybersecurity;
3. Implementing a collective approach to cybersecurity risk management; and
4. Conducting regular reviews and assessments of their governance arrangements to ensure its effectiveness.

3.2.2.5 Brazil

Objective

The Brazilian Federal Court of Audits reviewed the level of awareness and knowledge through the application of surveys and audits, recommending that the user has a technical profile and ideally, be the manager or be assigned to a unit responsible for managing the organization's information technology (IT) security. As part of the guideline developed, it was clarified that the criteria used to support the preparation of this questionnaire were freely adapted from the professional judgment of the TCU team of auditors on version 8 of the framework developed by the Center for Internet Security (CIS). The questionnaire addresses four of the eighteen critical cyber controls listed in this version as followed:

- Inventory and Control of Enterprise Assets;
- Inventory and Control of Software Assets;
- Continues Vulnerability Management; and
- Security Awareness and Skills Training.

Scope and Methodology

The audit was conducted by the Federal Audit Court, specifically, by the Information Technology Infrastructure Secretariat (SETIC), which takes care of IT infrastructure, customer service and process and project management. The study involved document analysis, interviews, and researcher observations.

The documental analysis covered the court's regulations and publications, as well as the report of an organizational climate survey conducted in 2012. Organizational climate refers to people's perception of the work environment. The report provided an overview of the organizational culture of the IT area of this court but did not identify facilitators and obstacles to IT governance.

Frameworks and Guides

- CIS Critical Security Controls, version 8.
- ABNT NBR ISO/IEC 20000-22008,
- ABNT NBR ISO/IEC 27002:2013
- Information Technology Infrastructure Library (ITIL) v3

- GSI/PR 3/2021, Chapter 11 (Mapping of information assets)
- Standard 8/IN01/DSIC/GSIPR (Guidelines for managing incidents in computer networks - TIR management - in the bodies and entities of the Federal Public Administration (APF)
- Risk Management Manual of the Federal Court of Auditors (TCU, 2018)

Conclusions

The Brazilian Federal Court of Audits expects for the researched agencies to use the assessment results to boost their risks management strengthening process. Among the benefits that organizations may acquire, the following stand out: greater possibility of achieving their goals; improvement of operational effectiveness and efficacy; governance improvement; greater confidence of the organization´s stakeholders; optimization on loss and incident management prevention; better information for planning and decision-making process; complying with the applicable legal and regulatory requirements.

3.2.3 Semi-Specific Auditing of Critical National Infrastructure

We identified that United Kingdom conducts its critical infrastructure audits specifically, with general guidelines to examine CNI and CII identification and mitigation programs, as shown below:

3.2.3.1 United Kingdom

The future of the UK's security and prosperity rests on digital foundations. The challenge of our generation is to build a flourishing digital society that is both resilient to cyber threats and equipped with the knowledge and capabilities required to maximize opportunities and manage risks.

We are critically dependent on the internet. However, it is inherently insecure and there will always be attempts to exploit weaknesses to launch cyber-attacks. This threat cannot be eliminated completely, but the risk can be greatly reduced to a level that allows society to continue to prosper, and benefit from the huge opportunities that digital technology brings.

Our strategy refers to the protection of information systems (hardware, software, and associated infrastructure), the data on them, and the services they provide, from unauthorized access, harm, or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.

Objective

The strategy is intended to shape the Government's policy, while also offering a coherent and compelling vision to share with the public and private sector, civil society, academia, and the wider population

Scope and Methodology

The audit considered the effectiveness of centre of government in defining government's strategic approach to protecting information across critical infrastructure in central

government departments (the departments) (Part One); the centre's performance in protecting information, including managing specific projects (Part Two); and departments' performance in protecting their information (Part Three).

The center consists of various teams within the Cabinet Office as well as other organizations such as CESG and the National Cybersecurity Centre. The central government departments consist of the 17 largest departments of state, although we have included other bodies where the evidence allows, as many of these issues are not unique to central government.7

Frameworks and Guides

National Cybersecurity Strategy 2022
https://www.gov.uk/government/publications/national-cyber-strategy-2022
Cyber Assessment Framework (CAF)
https://www.ncsc.gov.uk/collection/caf

Conclusions

Protecting information while re-designing public services and introducing new technology to support them is a complex challenge for government. To achieve this, the centre of government requires departments to risk manage their information, but few departments have the skills and expertise to achieve this by themselves. How successful government is in dealing with this challenge will therefore continue to depend on effective support from the Cabinet Office and other bodies at the center of government.

The Cabinet Office is taking action to improve its support for departments but needs to set out how this will be delivered in practice. To reach a point where it is clearly and effectively coordinating activity across government, the Cabinet Office must further streamline the roles and responsibilities of the organizations involved, deliver its own centrally managed projects cost-effectively and clearly communicate how its various policy, principles and guidance documents can be of most use to departments.

3.2.4 Specific Auditing of Critical National Infrastructure by Sectors

On the other hand, we identified that USA conducts its critical infrastructure audits across specific sectors, and it has developed individual guidelines for each sector, aiming to understand and examine CNI and CII identification and mitigation programs in every sector.

Please note that this section only points out the importance of having a classification of critical infrastructures and addresses in a general way the analysis that an audit of critical infrastructures entails without going into the detail of an evaluation by sectors that must be carried out in the Execution of audits of critical infrastructures by sector.

3.2.4.1 United States of America

Our nation's critical infrastructure refers to systems and assets, whether physical or virtual are so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on the nation's security, economic stability, public health or safety, or any combination of these factors. Critical infrastructure includes, among other

things, banking and financing institutions, telecommunications networks, and energy production and transmission facilities, most of which are owned and operated by the private sector.

Threats to the systems supporting critical infrastructures are evolving and growing. These cyber-based assets are susceptible to unintentional and intentional threats. Unintentional, or non-adversarial threat sources include equipment failures, software coding errors, or the accidental actions of employees. They also include natural disasters and the failure of other critical infrastructures since the sectors are often interdependent.

The framework is to provide a flexible and risk-based approach for entities within the nation's sixteen critical infrastructure sectors to protect their vital assets from cyber-based threats.

It should be noted that for the identification of the 16 critical factors indicated by the United States of America, an evaluation must be carried out that contemplates the risks and the possible impact in case of these risks materializing, in the life and governance of the country, hence the importance of having a classification of the country's sectors, industries and critical infrastructures.

Likewise, the detail of the 16 sectors defined by the United States of America, as well as the considerations that must be taken into account in the execution of critical infrastructure audits by sector, is presented in chapter 4 “Considerations of cybersecurity and data protection by sector”.

Objective

The objectives of our review are to determine the extent to which the National Institute of Standards and Technology (NIST) facilitated the development of voluntary standards and procedures to reduce cyber risks to critical infrastructure, and federal agencies promote the standards and procedures to reduce cyber risks to critical infrastructure.

Scope and Methodology

To determine how NIST facilitated the development of voluntary standards and procedures for critical infrastructure, we reviewed and analyzed the actions taken by NIST to develop its Framework for Improving Critical Infrastructure Cybersecurity. In addition, we analyzed Executive Order 13636, issued in February 2013, and the Cybersecurity Enhancement Act of 2014, enacted in December 2014, to identify key NIST responsibilities for developing a cybersecurity framework. We analyzed documents and performed interviews with NIST officials to assess its collaborative efforts with industry stakeholders in soliciting input in the development of the framework, including workshops it hosted and the website it set up to disseminate updates on the framework. Specifically, we reviewed documentation and videos of the six workshops hosted by NIST intended to obtain industry, academic, and government representative feedback in the development of the framework, in addition to NIST’s two requests for information to the public for input on cybersecurity standards and

methodologies. We also analyzed the resulting framework to assess whether NIST had fulfilled its responsibilities under law.[10]

Additionally, to address this objective, we conducted a web-based survey of individuals who provided written comments with contact information in response to a NIST request for information notice or registered for at least one of the workshops hosted by NIST to develop the framework. There were 2,082 individuals in the population that we targeted, and to make the survey as inclusive as possible we sent the survey request to all of them. The questionnaire included questions about the effectiveness of NIST's collaborative efforts in fulfilling requirements to develop the framework using an open and public comment process. To minimize errors arising from differences in how questions might be interpreted and to reduce variability in responses that should be qualitatively the same, we conducted pretests with critical infrastructure representatives over the telephone. Based on feedback from these pretests, we revised the questionnaire to improve the clarity of the questions. An independent survey specialist within GAO also reviewed a draft of the questionnaire prior to its administration.

After completing the pretests, we administered the survey to the NIST workshop attendees and request for information respondents on August 10, 2015, notifying them that our online questionnaire would be activated within a couple of days. On August 18, 2015, we sent a second e-mail message to these individuals, informing them that the questionnaire was available online and providing them with unique passwords and usernames. We collected responses through August 24, 2015. We were able to obtain 252 completed questionnaires, a 12 percent response rate, in the time available for survey fieldwork. Because we do not know if the answers that nonrespondents would have given would materially differ from those that did respond, our results can only represent the views of those who did respond. Their views are not generalizable to the registrant and respondent population. To address our second objective, we reviewed and analyzed actions and documentation related to promoting the framework by the nine sector specific agencies (SSAs) responsible for the 16 critical infrastructure sectors established in Presidential Policy Directive-21, including the Department of Homeland Security (DHS), and NIST. For DHS, we analyzed agency documentation and the website of its Critical Infrastructure Cyber Community (C3) Voluntary Program to identify the framework promotional guidance and tools provided to the critical infrastructure sectors. Also, we analyzed the metrics and information being used by the DHS C3 Voluntary Program to determine if DHS could measure the effectiveness of its activities and programs to promote the adoption of the framework. We also interviewed DHS officials on their activities related to the promotion of the framework, including their current and future promotional efforts. To analyze the promotional efforts by the nine SSAs, we analyzed relevant documentation and interviewed agency officials representing each of the SSAs. We specifically asked each of the SSAs whether promoting the framework was a priority in their draft 2015 sector-specific plans and whether they had decided to develop framework implementation guidance in accordance with Executive Order 13636. See table 5 for the sectors and SSAs included in our review.

[10]https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
https://www.govinfo.gov/content/pkg/COMPS-12455/pdf/COMPS-12455.pdf

https://www.cisa.gov/ccubedvp

Frameworks and Guides

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1
National Institute of Standards and Technology, April 16, 2018
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
https://www.nist.gov/cyberframework

Conclusions

Most sectors have taken action to facilitate adoption of the NIST cybersecurity framework within their respective sectors. By developing implementation guidance and aligning existing sector information resources with framework principles, most SSAs and SCCs have established a set of tools that entities could leverage to adopt the framework. However, none of the SSAs have assessed the extent to which their entities have adopted the framework. Without an accurate assessment of framework adoption within each sector, federal entities, SSAs, and SCCs lack a comprehensive understanding of the current adoption level within critical infrastructure sectors. As such, SSAs are unable to tailor their guidance to effectively encourage use of the framework to sector stakeholders.

Recommendations

We are making nine recommendations to sector-specific agencies in our review for them to develop methods to determine the level and type of framework adoption across their respective sectors. Specifically:

- The Secretary of Agriculture, in cooperation with the Secretary of Health and Human Services, should take steps to consult with respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector;
- The Secretary of Defense should take steps to consult with respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector;
- The Secretary of Energy should take steps to consult with respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector; and
- The Administrator of the Environmental Protection Agency should take steps to consult with respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector.

Guidelines by sector

Chemical

https://www.cisa.gov/uscert/sites/default/files/c3vp/framework_guidance/chemical-framework-implementation-guide-2015-508.pdf

Commercial Facilities Sector
https://www.cisa.gov/uscert/sites/default/files/c3vp/framework_guidance/commercial-facilities-framework-implementation-guide-2015-508.pdf

Communications Sector
https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf

Critical Manufacturing Sector
https://www.cisa.gov/uscert/sites/default/files/c3vp/framework_guidance/critical-manufacturing-framework-implementation-guide-2015-508.pdf

Dams Sector
https://www.cisa.gov/uscert/sites/default/files/c3vp/framework_guidance/dams-framework-implementation-guide-2015-508.pdf

Defense Industrial Sector
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

Emergency Services Sector
https://www.cisa.gov/uscert/sites/default/files/c3vp/framework_guidance/ess-framework-implementation-guide-2015-508.pdf

Energy Sector
https://www.energy.gov/sites/default/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf

Financial Services Sector
https://www.csbs.org/sites/default/files/2020-10/R-SAT_0.pdf
https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf
https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf

Healthcare and Public Health Sector
https://www.fda.gov/media/86174/download
https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

Nuclear Reactors, Materials, and Waste Sector
https://www.cisa.gov/uscert/sites/default/files/c3vp/framework_guidance/nuclear-framework-implementation-guide-2015-508.pdf

Transportation Systems Sector
https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf

https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf
https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Maritime_BLT_CSF.pdf?ver=2017-07-19-070544-223

Water and Wastewater Systems Sector
https://www.awwa.org/Portals/0/AWWA/ETS/Resources/AWWACybersecurityGuidance2019.pdf?ver=2019-09-09-111949-960
https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319-013

3.2.5 National Resilience / Disaster Recovery

Organizational resilience is important to assure users and managers that the expected level of service will be provided. Outages are also often unavoidable driving factors in organizations; therefore, preparation is key to be able to continue operations while protecting people, assets, and the organization's reputation; employing process resiliency tactics helps organizations to address these issues and limit the impacts.

It is worth to mention that the importance of having a resilience strategy and a disaster recovery plan lies in the fact that in the event of a contingency, the operational continuity of the critical systems and infrastructures of each country must be protected and ensured.

Likewise, these audits plans were classified into two main types:

- General disaster recovery audit with generic procedures; and
- Disaster recovery audit with specialized guidelines by functions.

3.2.5.1 General Disaster Recovery

3.2.5.1.1 Australia

Objective

Information and communications technology (ICT) systems are critical for the operations of government agencies. Agencies depend on them to:

- Deliver public services—including essential services—to the community.
- Efficiently and effectively manage operations.
- Fulfill their statutory obligations.

To make sure their systems remain available and continue to operate reliably, agencies must be able to recover and restore them in the event of a disruption—such as an event that interrupts access to premises, to the data that systems rely on, or to the systems themselves. Further, agencies need to
be able to recover and restore their systems within a time frame that reflects the business-critical nature of each system.

ICT disaster recovery is the process for recovering systems following a major disruption. ICT disaster recovery planning forms part of an agency’s wider business continuity strategy.

Managing disaster recovery risk presents special challenges. The likelihood of a major disaster or significant disruption is generally low, often remote—but the consequences of a system failure that cannot be restored could be significant or even catastrophic.

Without effective disaster recovery capability, agencies risk:

- Extended disruption or inability to deliver public services that depend on systems;
- Inability to recover systems and restore lost data;
- Subsequent financial loss to themselves and the Victorian economy; and
- Reputational damage, including loss of community confidence in the effective delivery of government services.

Agencies can reduce the likelihood of disruption events; however, this approach can require significant investment compared to the direct costs of responding to a disruption when it occurs. It can therefore be challenging for agencies to determine the balance between focusing on preventative actions and planning to manage the consequences of possible disruptions.

Scope and Methodology

In this audit, we examined disaster recovery at Victoria Police and four departments that provide essential government services—the Department of Economic Development, Jobs, Transport and Resources (DEDJTR), the Department of Environment, Land, Water and Planning (DELWP), the Department of Health and Human Services (DHHS) and the Department of Justice and Regulation (DJR).

We assessed whether their ICT disaster recovery processes are likely to be effective in the event of a disruption.

Frameworks and Guides

- Protective Security Policy Framework
  https://www.protectivesecurity.gov.au/policies
- AS/NZS ISO 31000:2009 Risk management – Principles and guidelines
  https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en
- ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity
  https://www.iso.org/standard/44374.html
- ICT Disaster Recovery Planning
  https://www.audit.vic.gov.au/sites/default/files/2017-12/20171129-ICT-Disaster-Recovery.pdf

Conclusions

At present, none of the agencies we audited have sufficient assurance that they can recover and restore all their critical systems to meet business requirements in the event of a disruption.

They do not have sufficient and necessary processes to identify, plan and recover their systems following a disruption. Compounding this is the relatively high number of obsolete ICT systems all agencies are still using to deliver some of their critical business functions.

This both increases the likelihood of disruptions though hardware and software failure or external attack and makes recovery more difficult and costly. These circumstances place critical business functions and the continued delivery of public services at an unacceptably high risk should a disruption occurs.

Agencies are beginning to fully understand the importance of comprehensively identifying and prioritizing their business functions, maintaining the ICT systems that support these functions, and establishing recovery arrangements to maintain continuity of service.

They need to significantly improve and develop well-resourced and established processes that fully account for and can efficiently recover the critical business functions of agencies following a disruption.

Recommendations

We recommend to the Departments of Economic Development, Jobs, Transport and Resources, Environment, Land, Water and Planning, Health and Human Services, Justice and Regulation and Victoria Police to:

1. Appoint a team of suitably qualified and experienced professionals to form a collaborative disaster recovery working group to:

- Provide advice and technical support;
- Share lessons learnt based on disaster recovery tests and exercises;
- Coordinate disaster recovery requirements for resources shared between agencies.
- Identify, develop, implement, and manage initiatives that may impact multiple agencies; and
- Coordinate funding requests to ensure critical investments and requirements are prioritized.

2. Perform a gap analysis on their disaster recovery requirements and resource capabilities to determine the extent of the capability investment that will be required.

3. Develop disaster recovery plans for the systems that support critical business functions and test these plans according to the disaster recovery test program.

4. Provide advice and training to staff on:

- Newly developed frameworks, policies, standards and procedures to increase awareness and adoption as needed; and
- Specific disaster recovery systems.

5. Establish system obsolescence management processes to:

- Identify and manage systems at risk of becoming obsolete, those that will soon have insufficient support or those that will be difficult to manage when they become obsolete;
- Enable strategic planning, life-cycle optimization, and the development of long-term business cases for system life-cycle support; and
- Provide executive with information to allow risk-based investment decisions to be made.

Finally, it was not identified that there is an agency that oversees coordination and activation of the national disaster recovery plan.

3.2.5.2 Disaster Recovery by Functions

3.2.5.2.1 United States of America

We identified that USA conducts its Disaster Recovery Plans audits across specific sectors, and it has developed individual guidelines for each sector.

The Department of Homeland Security's (DHS) Federal Emergency Management Agency (FEMA) is responsible for implementing the National Disaster Recovery Framework (NDRF) and working in partnership with states as they play a lead role in the recovery process. As shown in the figure below, FEMA coordinates federal recovery stakeholders using six Recovery Support Functions—structures through which federal coordinating agencies provide assistance to state and local communities, before and after a disaster. FEMA's regional offices facilitate pre-disaster recovery planning at the state and local level, promote state adoption of NDRF principles into state pre-disaster recovery plans, and coordinate collaboration between federal, state, local, and tribal governments. Under the NDRF, states have primary responsibility for managing recovery in their communities, including developing pre-disaster recovery plans based on the principles and structures in the NDRF.

The National Disaster Recovery Framework (NDRF) enables effective recovery support to disaster-impacted states, tribes, territorial and local jurisdictions. It provides a flexible structure that enables disaster recovery managers to operate in a unified and collaborative manner. The NDRF focuses on how best to restore, redevelop, and revitalize the health, social, economic, natural, and environmental fabric of the community and build a more resilient nation.

The NDRF is a first step toward achieving a shared understanding and a common, integrated perspective in order to achieve unity of effort and to build a more resilient nation.

The National Disaster Recovery Framework's Recovery Support Functions and Corresponding Federal Coordinating Agencies

Recovery Support Function	Federal Coordinating Agency
Community Planning and Capacity Building	Department of Homeland Security/Federal Emergency Management Agency
Economic	Department of Commerce/Economic Development Administration
Health and Social Services	Department of Health and Human Services
Housing	Department of Housing and Urban Development
Infrastructure Systems	Department of Defense/Army Corps of Engineers
Natural and Cultural Resources	Department of the Interior

Source: GAO analysis of Federal Emergency Management Agency (FEMA) information. | GAO-16-476

It is important to point out that the importance of considering, within the scope of the audits of disaster recovery plans, the operational continuity of critical infrastructures, lies in the fact that natural events (storms, floods, fires, etc.), as well as cyber-attacks could stop the substantive operations of the essential sectors of each country

3.2.5.3 Factors to Consider for Disaster Recovery by Functions audits.

In order to conduct a disaster recovery audit by functions, the US government analyses the following:

- Risk should be identified and managed in a coordinated way within the critical infrastructure community to enable effective resource allocation;
- Critical infrastructure partnerships can greatly improve understanding of evolving risk to both cyber and physical systems and assets and can offer data and perspectives from various stakeholders;
- Understanding and addressing risks from cross-sector dependencies and interdependencies is essential to enhancing overall critical infrastructure security and resilience;
- Gaining knowledge of and reducing infrastructure risk requires information sharing across all levels of the critical infrastructure community;
- A partnership approach, involving public and private stakeholders, recognizes the unique perspectives and comparative advantages of the diverse critical infrastructure community. For example, Emergency Support Function 14 of the National Response Framework supports the coordination of cross-sector operations, including stabilization of key supply chains and Community Lifelines, among infrastructure owners and operators, businesses, and their government partners;

- Regional, state, and local partnerships are crucial to developing shared perspectives on gaps and improvement actions;
- Critical infrastructure transcends national boundaries, requiring bilateral, regional, and international collaboration; capacity building; mutual assistance; and other cooperative agreements. For example, the “Canada-U.S. Action Plan for Critical Infrastructure” sets the foundation for cross-border critical infrastructure security and resilience efforts between the two countries; and
- Security and resilience should be considered during the design of infrastructure elements.

In this context, chapter 4 addresses in greater depth the elements and methodologies to be considered to carry out an audit of cybersecurity and data protection by sectors, so for more details please consult chapter 4 “Cybersecurity and Data Protection by Sectors”.

3.3 Auditing National Cyber Incident Response

3.3.1 The role of government entities in charge of cyber incident response.

This section identifies the role of government entities in charge of cyber incident response (CSIRT), specifying CSIRT evaluation schemes, identifying the elements of review to understand the nature, scope, and operation of a cybersecurity incident handling service, as well as explaining the SIM3 model for the evaluation of the maturity level of a CSIRT which reviews the competence achieved, either in the execution of specific functions or in a set of functions or services.

3.3.2 Entities Responsible for National Cybersecurity.

There are government cybersecurity agencies specialized in the investigations of the different computer crimes or frauds committed in cyberspace, their fundamental task is to combat computer crimes and frauds that are carried out through the internet, all this through legal processes established in the laws of each country; The computerized or cybernetic police forces receive complaints through social networks or telephone calls, which are essential to begin investigations in relation to crimes.

These police organizations dedicated to the computer world pursue and prevent bank fraud, identity theft, cyberbullying or online bullying, child pornography, identity theft through different social networks and hacks that result in loss or kidnapping of information. Their functions are diverse. Among them, they are in charge of fighting virtual terrorism, carrying out cyber patrolling to avoid computer crimes or fraud against computer systems and/or banking institutions, carrying out the necessary investigations to pursue cases involving computer crimes, cyberbullying and child prostitution through the use of the internet as a means of contact, and are also in charge of analyzing and identifying the different types of computer crimes and scams carried out through the internet.

The cybernetic police operate throughout cyberspace carrying out antihacker cyber patrols, with the help of specialized equipment (computers) and personnel for its execution. Units specializing in cybercrime seek to protect all citizens who use the network, monitoring through the so-called CSIRT/CERT, protecting citizens social network accounts, responding

to calls for complaints or scams, or any other computer crime. These teams (CSIRT/CERT) are of vital importance since they are the ones in charge of coordinating the different organizations that oversee identifying and responding to cyber incidents.

It is important to underline that each country has a different political structure, culture, geography, legal framework, and resources, and thus, the guidelines are not intended to be imposed, but rather must be adapted to the local conditions of each country.

3.3.3 CERT/CSIRT functions

- **CERT** - Computer Emergency Response Teams. It is a trademark registered by Carnegie Mellon University in the USA and for a response team to be called in this way, it must meet certain requirements and evaluations by this university; and
- **CSIRT** - Computer Security Incident Response Teams, is a concept that may be more commonly used by incident response teams. Associations such as FIRST, TF-CSIRT or CSIRT validate, based on their skills and references, who should be considered as such.

The services provided by CSIRTs can be divided into three areas:

- Preventive/Proactive: in charge of alert monitoring, security audits, vulnerability scanning, malicious artifact scanning, technology monitoring, artifact analysis, and forensic analysis;
- Reactive: they manage an incident, from analysis, to response actions, support, and coordination, which implies post-mortem analysis, on-site assistance, response to vulnerabilities, response to malicious artifacts, etc.; and
- Added value, help manage the organization's security by conducting risk assessments, participating in business continuity plans, disaster recovery, as well as participating in awareness programs.

All CSIRTs work differently depending on the entities they provide protection to. However, in general terms, most of these groups have an attack team, which is responsible for studying the behavior of cybercriminals and the main attack vectors, and a defense team, whose objective is to analyze the traffic of the networks to be alert under the presence of a computer eventuality. Additionally, these teams have great challenges such as sharing information, adding synergies with other CSIRTs to be able to share information in forums (such as APCERT or FIRST) and being able to offer an effective and rapid response to any threat to the most critical information or the interruption of services and/or business.

National CSIRTs respond to state/national level incidents and typically monitor and address incidents on government networks and serve as information security coordinators for the private sector or other sectors and institutions. The role and target community of a national CSIRT varies depending on their roles and the existence of other response centers; in this sense, it is very common that there are several CSIRTs with specific functions (for example, a critical infrastructure CSIRT) as part of the community served by a national CSIRT.

3.3.4 Computer Emergency Response Team (CERT) and Computer Security Incident Response Team (CSIRT)

Distinctions are made between CERT and CSIRT: A CERT is conceived as a study center and a place where methods and procedures are established to improve incident response teams; a CSIRT team are those responsible for responding to incidents[11] and it should be clarified that there are only two CERTs defined as such in the world: one is the CERT/CC (CERT Coordination Center), which is part of the Software Engineering Institute of Carnegie Mellon University, in Pennsylvania, United States, and the other is US-CERT, the response team of the US Department of Homeland Security. In all other countries around the world, cybersecurity teams are called Computer Security Incident Response Teams (CSIRTs), which upon obtaining certification offered by Carnegie Mellon University can include in its name is the acronym CERT[12].

These teams can be public or private, the main types of CSIRT are listed below[13]:

- National CSIRTs: In addition to serving a defined community, a country's CSIRT typically assumes the role of national incident response coordinator and is the contact for national and international incidents;
- Government CSIRTs: Government CSIRTs serve State institutions to ensure that the government's IT infrastructure and the services offered to citizens have adequate levels of security;
- Military Sector CSIRT: These CSIRTs provide services to the military institutions of a country. Their activities are generally limited to the defense or offensive cyber capabilities of a nation; and
- Critical Infrastructure CSIRT: In some cases, there are CSIRTs determined specifically for the protection of information assets and critical infrastructure of the nation, regardless of whether it is operated by the public or private sector, or its sector.

The TF-CSIRT site is the main European CERT's forum in which the most outstanding CERT's in the world collaborate, innovate and share information, you can see lists of

[11] SIC- Spanish magazine specializing in information security and the security of technological information and communication systems used in organisations. SIC number 142- November 2020- CSIRTs: At the foot of the Canyon: https://www.first.org/newsroom/releases/FIRST-Press-Release-20201118.pdf; ENISA- Document HOW TO CREATE A CSIRT STEP BY STEP WP2006/5.1: https://www.enisa.europa.eu/publications/csirt-setting-up-guide/@@download/fullReport; ENISA- How to setup up CSIRT and SOC/ good practice guide: https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc/at_download/fullReport .

[12] CERT & CSIRT : https://www.eleconomista.com.mx/tecnologia/Que-es-un-Equipo-de-Respuesta-ante-Emergencias-Informaticas-CERT-20180122-0009.html .

[13] General Secretariat of the Organization of American States (OAS), 20006 United States of America- April 2016- Good practices to establish a national CSIRT: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Best%20Practices%20CSIRT.pdf; ENISA- Document HOW TO CREATE A CSIRT STEP BY STEP WP2006/5.1 : https://www.enisa.europa.eu/publications/csirt-setting-up-guide/@@download/fullReport; ENISA- How to setup up CSIRT and SOC/ good practice guide: https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc/at_download/fullReport .

accredited teams (194), certified (31) and lists (185) of the European Union at the date of this document (January 2022), both from the public and private sectors.

3.3.5 Guide for cybersecurity CSIRT

3.3.5.1 Assessment guide for cybersecurity CSIRT

The first analysis that must be carried out consists of knowing if cybersecurity agencies and their operating entities (CSIRT/CERT) have been established at the national level, by answering the following questions:
Operating entities:

1. Is there a competent national authority for information security and cybersecurity (NIS)?
2. Is there an incident reporting platform to collect cybersecurity incident data?
3. Are national cybersecurity exercises carried out?
4. Is there a National Incident Management Structure (NIMS) to respond to cybersecurity incidents?
5. Is there a National Computer Emergency Response Team (CERT)? o Computer Security Incident Response Team (CSIRT)?
6. In what year was the Computer Emergency Response Team (CERT) established?

In a study made by the European Union (EU)[14], it is shown a board with the complete description of the estate of the actual cybersecurity frames and its capacities for each member. The report considers five main areas of cybersecurity politics of each state of EU:

- Legal foundations of cybersecurity;
- Operating Entities;
- Public-private partnerships; and
- Education.

Incident response capabilities must be established in the Operating Entities, managing the most critical and significant events that threaten the confidentiality, integrity, or availability of significant information networks nationally and systems. Computer Emergency Response Teams (CERT) and Computer Security Incident Response Teams (CSIRT) can play a crucial role in improving cyber resiliency

Once verified the existence of those cybersecurity entities can be taken into consideration the following two evaluations:

- A pillar-based evaluation in which the bases, mission, vision, and objectives are reviewed, up to its operation, analyzing it as ad hoc with its purpose to achieve the benefits expected by the organization; also reviews compliance with legal and institutional frameworks and that their practices adhere to existing and approved standards; and

[14] BSA The Software Alliance- Document EU Cybersecurity Panel. A path to a secure European cyberspace: www.bsa.org/EUcybersecurity .

- On the other hand, there is the assessment of the maturity level of a CSIRT, which focuses on comparing the current level of the organization with respect to how its functions are governed, documented, performed, and measured and allows understanding the improvement actions to be addressed.

3.3.5.2 Pillar-based assessment for cybersecurity agencies

The objective of the pillar-based evaluation guide for a CSIRT is to analyze its creation and implementation, including the different criteria that were considered to define its constitution, mission, vision, scope, budget, types of services, organizational model, availability, legal and institutional frameworks, applicable regulations and their organizational structure; it also contains an analysis of human resources requirements, both in terms of skills and conduct, and of continuing training, which are considered necessary. On the other hand, the review considers the physical infrastructure, which includes physical installations, hardware, software, network, and technical tools that allow its operation; and finally, the policies, procedures, standards are analyzed[15].

The Pillars refer to 5 paragraphs where criteria are integrated that must be evaluated, these ranging from its constitution to its operation[16]:

- Bases: The root (business plan, constitution, legal restrictions, etc.);
- Organization: Attributions (mandate and related organizational structures);
- Human: Human resources (team personnel, structure, experience, code of conduct and training options);
- Tools: Physical and logical infrastructure for the work (everything required to carry out the tasks of the agency); and
- Processes: Policies, procedures, processes, standards (for agency operation, incidents, media, etc.).

Table 1: Evaluation by mainstay

¿What is evaluated?	Description	Required Information	Elements to be evaluated	Reference guides and good practices
	To carry out the evaluation of the BASES pillar, we must consider the mission, objectives, vision, values, priorities, stakeholders, legal	1. Identification document of the interested parties. 2. Stakeholder management plan. 3. Constitution document of the national CSIRT. a. Mission and vision.	Agency definition 1. Scopes of action of the CSIRTs. 2. Concerned parties 3. Mission, Objective, and vision	Organization of American States (OAS) Good practices to establish a national CSIRT. https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Best%20Practices%20CSIRT.pdf National Cryptologic Center (CCN) CCN-CERT

[15] SIC- Spanish magazine specializing in information security and the security of technological information and communication systems used in organisations. SIC number 142- November 2020- CSIRTs: At the foot of the Canyon: https://www.first.org/newsroom/releases/FIRST-Press-Release-20201118.pdf; CCN- Guide to creating a CERT/CSIRT- CCN-STIC-810: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/520-ccn-stic-810-guia-de-creacion-de-cert-s/file.html; Cybersecurity Agency of Catalonia - Tools and software packages: https://csirt-kit.org/: General Secretariat of the Organization of American States (OAS), 20006 United States of America- April 2016- Good practices to establish a national CSIRT: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Best%20Practices%20CSIRT.pdf .

[16] ThaiCERT (Thailand Computer Emergency Response Team a member of ETDA)- Translation into Spanish CSIRT CEDIA- Document Establishing a CSIRT: https://csirt.cedia.edu.ec/wp-content/uploads/2020/08/Estableciendo.un_.CSIRT_.v1.3-es_EC.pdf .

Pillar: Foundations The foundations of the CSIRT	alignment, its target community, its institutional and legal framework and finally the range and nature of services it offers. This review should identify why the CSIRT exists, what it does, to whom it performs services, what values motivate it, the route that the organization will take in the long term, which is the constitution of the CSIRT (as an independent (private) as a unit within a public or private organization, and finally the legal framework governing it at country level imposing restrictions to protect the CSIRT and its operations.	b. Institutional framework. c. Legal framework. 4. Minutes of planning and implementation meetings. 5. Lists of participants in the different activities. 6. Emails exchanged with experts. 7. Definition of target community. 8. List of services with their description.	4. Alignment with the legal framework. Constitution of the agency 5. Institutional framework. 6. Legal framework. Review of applicable laws and regulations, at least the following: a. Cybersecurity b. Security of the information c. Personal data protection. d. Critical infrastructures. e. Telecommunications service providers (data retention, user protection) f. International cooperation. 7. Business plan (budget, implementation plan). Reach 8. Target community (government, private sector, or both). 9. Services (reactive services, proactive services, and value-added services).	CCN-STIC-810 CERT/CSIRT creation guide. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/520-ccn-stic-810-guia-de-creacion-de-cert-s/file.html Thailand Computer Emergency Response Team a member of ETDA Establishing a CSIRT https://csirt.cedia.edu.ec/wp-content/uploads/2020/08/Estableciendo.un_.CSIRT_.v1.3-es_EC.pdf Carnegie Mellon University (CMU) Handbook for Computer Security Incident Response Teams (CSIRTs) https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf European Union Agency for Cybersecurity (ENISA) How to create a CSIRT step by step WP2006/5.1 https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc/ European Union Agency for Cybersecurity (ENISA) How to setup up CSIRT and SOC/ good practice guide https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc/at_download/fullReport LACNIC/ AMPARO Project Computer security incident management manual. https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf
Pillar: Organization CSIRT's Organization	To carry out the evaluation of the ORGANIZATION pillar, the organizational model (mandate) must be considered, which indicates the position and attributions of the CSIRT within the target organization or community, as well as its relationship with other internal and external organizational structures.	1. CSIRT organizational model 2. Participation reports in cybersecurity forums.	Organizational model 1. Structure definition. 2. Information exchange. a. Registration to forums and information communities on cybersecurity.	Carnegie Mellon University (CMU) Organizational Models for Computer Security Incident Response Teams (CSIRT) https://pdfs.semanticscholar.org/1994/5cacfd441dd0863b34ead3ca598a5f4d35de.pdf?_ga=2.43035820.888637854.1645152937-1222354997.1645152937 Organization of American States (OAS) Good practices to establish a national CSIRT. https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Best%20Practices%20CSIRT.pdf LACNIC/ AMPARO Project Basic IT security incident management manual.

				https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf
Pillar: Human CSIRT human resources	The evaluation of the HUMAN pillar refers to who carries out the services required by the target community, for this it is necessary to evaluate the organizational structure of the CSIRT, including functions and responsibilities of each member. Likewise, the evaluation must consider the knowledge, experience, and necessary skills of said resources and the training options that are required to potentiate their functions in the CSIRT, and finally, the review must include the conduct guidelines established for the CSIRT.	1. Organizational structure. 2. Hired human resources. 3. Applicable code of conduct. 4. Cybersecurity training calendar.	Organization and HR 1. Organizational structures (number of areas and resources). 2. Roles and responsibilities. Selection of human resources: Training requirements: 3. Certifications and technical training (in basic areas: general cybersecurity, incident response, cybersecurity and malware and forensic analysis, etc.). 4. Personal skills (resistance to stress, analytical skills, flexibility, creativity, etc.). Conduct guidelines 5. Code of conduct	Book: Organizational Structure By Mario Javier Brume Gonzalez https://www.itsa.edu.co/docs/ESTRUCTURA-ORGANIZACIONAL.pdf Organization of American States (OAS) Good practices to establish a national CSIRT. https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Best%20Practices%20CSIRT.pdf Official College of Psychologists Technical guide and good practices in recruitment and selection of personnel (R&S). https://issuu.com/colegiooficialpsicologosmadrid/docs/guia_tecnica_buenas_practicas Trusted Introducer CSIRT Code of Practice https://www.trusted-introducer.org/CCoPv21.pdf LACNIC/ AMPARO Project Basic IT security incident management manual. https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf
Pillar: Tools CSIRT Tools and Facilities	The evaluation of the TOOLS pillar includes everything that is required to carry out the tasks of the agency, from the basic general services that correspond to the equipment of the physical space and services, the physical access methods, and the IT equipment, to the tools or specialized software packages for the operation.	1. Location of physical facilities, rental contracts, etc. 2. Technological infrastructure and the respective support contracts. 3. Network diagrams. 4. Hardware relation. 5. Software Relationship. 6. Storage platform. 7. Backup schedule 8. Classification of information.	Facilities and IT infrastructure 1. Physical facilities 2. Basic network design 3. IT infrastructure and tools, at least the following: a. Institutional web server b. Institutional mail server. c. Intranet server. d. File server. e. Server backups. f. DNS server. g. Event monitoring, collection, and correlation server. h. Recording and monitoring of incidents. IT infrastructure design and network architecture 4. Confidential information protection 5. Information storage.	Book: The Control Center Design Book By: Armando Gonzalez Lefler https://books.google.com.mx/books?id=mnXgDwAAQBAJ&pg=PA52&dq=normas+y+est%C3%A1ndares+generales+para+data+center&hl=es&sa=X&ved=2ahUKEwjf4Za52fD1AhXGCTQIHcabBkgQ6AF6BAgHEAI#v=onepage&q=normas%20y%20est%C3%A1ndares%20generales%20para%20data%20center&f=false, páginas 52-59. Organization of American States (OAS) Good practices to establish a national CSIRT. https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Best%20Practices%20CSIRT.pdf International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) ISO 27001 ISO 22301 https://www.iso.org/ Cybersecurity Agency of Catalonia Toolkit to provide the first steps to new incident management equipment. Tools such as: open-source threat intelligence platforms, incident management information, operational intelligence,

				incident response platforms, forensic network analysis, records management, etc. https://csirt-kit.org/
Pillar: Process The processes governing the CSIRT	The evaluation of the PROCESSES pillar must include the analysis of the organization's policies and procedures because they are essential to govern its operation and the activities of the response center, and these should ensure the confidentiality, availability and integrity of the information and resources, as well as the quality of its services.	1. Operations manual with policies and procedures. 2. Formalized security policies and procedures. 3. Documentation of implemented standards. 4. Technical memories of implementation of configurations. 5. Formalized operating procedures. 6. Formalized security guidelines. 7. Description of specific incidents. 8. Definition of information exchange formats. 9. General cybersecurity guides. 10. Statistical reports.	Politics and procedures 1. Definition of policies and procedures. 2. Formalization and application of operational policies and procedures of at least the following policies: a) Information classification. b) Data protection. c) Withholding information. d) Iinformation destruction. e) Disclosure of information. f) Access to information. g) Appropriate use of agency systems. h) Definition of security incidents and event policy. i) Incident management. j) Cooperation. k) Use of internet. l) Incident reporting. m) Agency communication. n) Training and coaching. o) Security of personal equipment. p) Network security. q) Use of email. r) Use of mobile devices. s) Telecommunications equipment security. t) Backups. u) Segregation of duties. v) Change control and passwords. 3. Standards and good practices implemented for the operation of the CSIRT: a. Incident management procedures. b. Incident prevention and management procedures. c. Incident detection procedure. d. Specific incident process. e. Procedures for integrating forensic techniques in incident response. f. Incident response procedures. g. Guidelines for the collection and archiving of evidence.	Politics: Organization Forum of Incident Response and Security Teams (FIRST) https://www.first.org/ Standards: Nacional Institute of Standards and Technology (NIST) of USA. SP 800-61 SP 800-83 SP 800-86 https://www.nist.gov/ IETF/RFCS (INTERNET ENGINEERING TASK FORCE) RFC 2350 RFC 3227 RFC 3067 RFC 4765 https://www.ietf.org/standards/rfcs/ International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) ISO 27035 ISO/IEC 29147 ISO 27001 ISO 27032 https://www.iso.org/ ENISA Standards and tools for exchange and processing of actionable information https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information

			h. Intrusion detection message exchange formats. i. Procedures for disclosure of information.	

Source: Created by ASF.

3.3.6 Assessing the maturity level of a CSIRT

The objective of the maturity level evaluation is to analyze how well a CISRT team governs, documents, performs, and measures its function. This analysis compares the level where the CISRT is currently, which allows organizations to visualize the information and consider it as a baseline to detect existing gaps, carry out in-depth reviews, issue opinions and take actions focused on continuous improvements.

3.3.6.1 SIM3 Model

Maturity is a level of competency achieved either in the execution of specific functions or in a set of functions or services. The maturity of an organization will be determined by the scope, the quality of established policies and documentation and the ability to execute an established process, the level of advancement in knowledge, skills and competence measured against a defined reference model.

The Security Incident Management Maturity Model (SIM3) issued by the Open CSIRT Foundation and used since 2009[17], is based on three basic elements for its evaluation:

1) Maturity parameters, 44 parameters: 10 in organization, 7 in human, 10 in tools and 17 in processes.
2) Quadrants of maturity: Organization, Human, Tools and Processes.
3) Maturity Levels:

> 0 = unavailable / undefined / unaware;
> 1 = implicit (known/considered but not written, “between the ears”);
> 2 = explicit, internal (written but not formalized in any way);
> 3 = explicit, formalized with the authorization of the head of the CSIRT (sealed or published);and
> 4 = explicit, audited by the authority of the levels of government above the head of the CSIRT (subject to control/audit/enforcement process).

Maturity models such as SIM3 can be used by new CSIRTs as well as well-established CSIRTs around the world. Using this maturity model, they can ensure that they have a

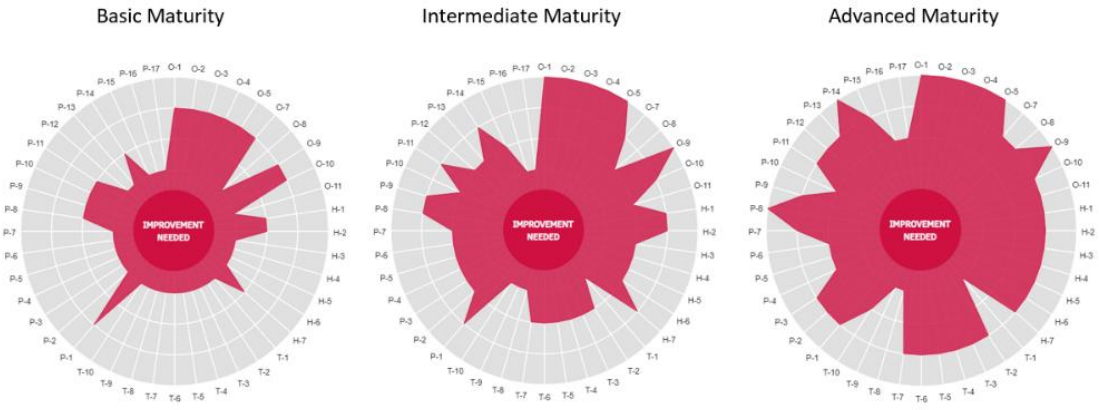
[17] SIM 3 Model:
chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fthegfce.org%2Fwp-content%2Fuploads%2F2020%2F05%2FMaturityFrameworkfornationalCSIRTsv1.0_GFCE.pdf&clen=523923&chunk=true

clearly defined framework for achieving their goals. Considering that SIM3 is designed incorporating extensive experience from incident response professionals, organizations should consider it as a baseline and focus on continuous improvements.

This model is used as a support in the certification frame of Trusted Introducer (which belongs to the European Union, Austria, Brazil, China, Czech Republic, France, Germany, Hong Kong, India, Israel, Italy, Japan, Luxemburg, Netherlands, Spain, United Kingdom, United States, etc.,) and its being adopted by several organizations members of FIRST (to which belongs 99 countries such as United States, Canada, Mexico, Colombia, Brazil, Peru, Argentina The Russian Federation, China, Switzerland, Norway, Germany, Spain, Saudi Arabia, South Africa, and Australia, etc.,) and the Nippon CSIRT Association -NCA in Japan with (440 members)[18].

There is a self-assessment survey offered by ENISA (European Union Cybersecurity Agency), based on the SIM3 maturity model, that can be done online which evaluates the 44 parameters divided into four categories: organization, processes, tools, and human resources of an incident response team. These will determine a basic, intermediate, or advanced level of maturity[19].

Figure 1.



[18] ThaiCERT (Thailand Computer Emergency Response Team a member of ETDA)- Translation into Spanish CSIRT CEDIA- Document Establishing a CSIRT: https://csirt.cedia.edu.ec/wp-content/uploads/2020/08/Estableciendo.un_.CSIRT_.v1.3-es_EC.pdf; FIRST- Map of forum members: https://www.first.org/members/map; Members of NCA- Japan: https://www.nca.gr.jp/member/index.html .

[19] ENISA- Self-assessment SIM3 model: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-survey .

Parameters to cover according to maturity levels

Through the following link the assessment can be done: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-survey

Parameters of the SIM3 model[20]

Parameter	Number of questions	ID	What is checked?
Organization	10	O-1, O-2, O-3, O-4, O-5, O-7, O-8, O-9, O-10 y O-11.	Mandate, distribution, authority, responsibility, service description, service level description, incident classification, participation in existing CSIRT frameworks, organizational framework, and security policy.
Human	7	H-1, H-2, H-3, H-4, H-5, H-6 y H-7.	Code of Conduct/Practice/Ethics, Personal Resilience, Skill/Skill Set Description, Internal Training/Training, Technical Training (External), Communication Training (External), and External Networks.
Tools	10	T-1, T-2, T-3, T-4, T-5, T-6, T-7 T-8, T-9 y T-10	IT resource list, source list, consolidated email system, incident tracking system, rugged phone, resilient email, resilient internet access, incident prevention toolkit, Incident detection toolkit and incident resolution toolkit.
Process	17	P-1, P-2, P-3, P-4, P-5, P-6, P-7 P-8, P-9, P-10 P-11, P-12, P-13, P-14, P-15 P-16 y P-17.	Scaling to governance level, scaling to press function, scaling to legal function, incident prevention process, incident detection process, incident resolution process, specific incident processes, audit/feedback process, emergency accessibility process, internet presence best practices, question about the secure information management process, information sources process, disclosure process, reporting process, statistics process, collection process and peer-to-peer process.

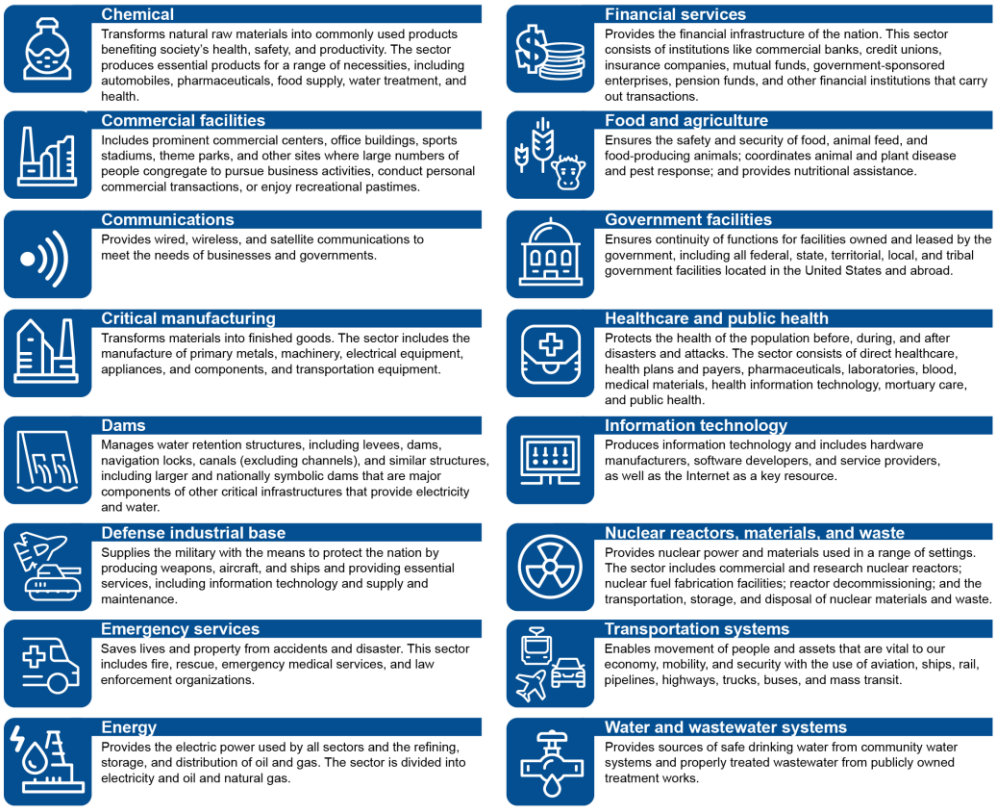
[20] Source provided by SAI Mexico.

4 Considerations of cybersecurity and data protection by sector

Critical infrastructure sectors contain vital systems, which if incapacitated, could debilitate or destabilize a nation's security, economy, public health or safety. Critical infrastructure can include, among others, banking and financial institutions, telecommunications networks, and energy production and transmission facilities.

Figure 1 describes examples of critical infrastructure sectors that may be in place. Although these sectors were defined for the United States, other nations' critical infrastructure sectors may be similar or vary depending on the assets nations consider essential for the functions of their society and economy.

Figure 1. Examples of critical infrastructure sectors.



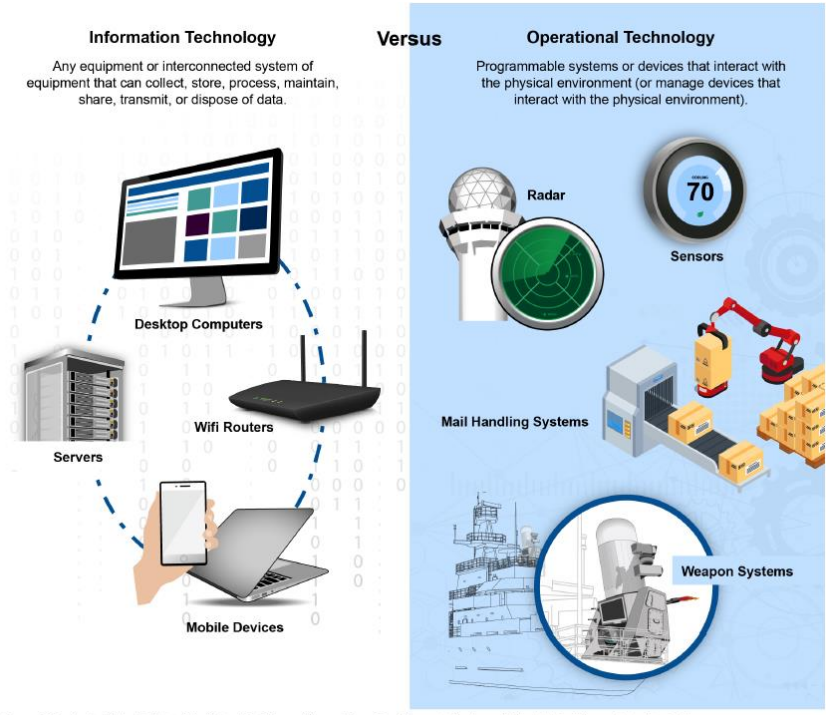
Source: GAO analysis of Presidential Policy Directive-21 and DHS's National Infrastructure Protection Plan 2013; images: motorama/stock.adobe.com.

However, increasing cyber threats to these critical infrastructure sectors represent a significant security challenge. Specifically, malicious actors have intruded and extracted information from, and disrupted the networks of, government agencies and major critical infrastructure companies throughout the world. Recent incidents illustrate the pressing need to strengthen critical infrastructure cybersecurity. For example, attacks targeted health care and essential services in the United States and United Kingdom during the Coronavirus Disease 2019 (COVID-19) pandemic, and the United States, United Kingdom, and Australia

noted an increase in ransomware incidents against critical infrastructure organizations starting in 2021.[21]

Organizations within a country's critical infrastructure may use both information technology (IT) and operational technology (OT) systems in doing their jobs. IT systems include any equipment or interconnected system of equipment that can collect, store, process, maintain, share, transmit, or dispose of data. OT systems, on the other hand, are programmable systems or devices that interact with the physical environment, such as industrial control systems, transportation systems, and physical access control systems. Initially, OT systems were isolated, ran proprietary control protocols, and used specialized hardware and software. However, as OT systems are adopting IT solutions to promote connectivity and remote access capabilities, they have started to resemble IT systems. It is important for agencies to protect operational technology from being compromised and accessed without authorization to avoid the disruption of critical devices or functions. Figure 1 depicts common types of IT and operational technology, and how they differ.

Figure 2. Common Types of Information Technology and Operational Technology



Source: GAO analysis of National Institute of Standards and Technology guidance and Coast Guard documentation; images: Vikivector/stock.adobe.com, kurtcan/stock.adobe.com, robu_s/stock.adobe.com, royyimzy/stock.adobe.com, Yevhenii/stock.adobe.com. | GAO-22-105092

[21] In May 2020, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency released a joint alert with the United Kingdom's National Cyber Security Centre regarding advanced persistent threat groups exploiting COVID-19 to target health care and essential services. The alert warned that advanced persistent threat groups were frequently targeting organizations in order to collect bulk personal information, intellectual property, and intelligence that aligns with national priorities. See GAO, *HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration*, GAO-21-403 (Washington, D.C.: June 28, 2021). In February 2022, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency released a joint alert with cybersecurity authorities in Australia and the United Kingdom related to incidents of ransomware against critical infrastructure sectors. These ransomware groups were diversifying their approaches to extort money and were targeting organizations of all sizes.

4.1 Key Cybersecurity Guidance and Criteria for Critical Infrastructure Sectors

Many countries have specific laws or guidance to protect such critical infrastructure sectors. In many cases, the guidance and criteria used to audit critical infrastructure sectors is broad and may cover many (or all) critical infrastructure sectors. Cybersecurity guidance and legislation related to the critical infrastructure sectors may include relevant laws in each country (refer to chapter 3), each country's internal auditing standards, and international guidance documents relevant to the audit.

For example, to better protect against cyber threats, the National Institute of Standards and Technology (NIST) facilitated the development of a voluntary framework of cybersecurity standards and procedures for sectors to use. Specifically, in February 2014, NIST published the *Framework for Improving Critical Infrastructure Cybersecurity*, which has been translated into seven languages and has been adopted by many governments around the world.[22] NIST has also provided crosswalks—known as online informative references—between elements in NIST documents and those found in other guidance such as ISO standards, COBIT 2019, and others.[23] Much of the guidance specific to critical infrastructure is discussed in chapter 3 of this guide.

4.2 Challenges, Risks, and Threats for Critical Infrastructure Sectors

According to the U.S. Department of Homeland Security, the threats that critical infrastructure sectors face can vary from natural disasters, human-made accidents, or malicious actions. Examples of these threats can include the following:

- **Geophysical, climatological, meteorological events, and other natural disasters**: drought, earthquakes, extreme heat, extreme precipitation, floods, geomagnetic storms, hurricanes, tropical cyclones, volcanic eruptions, wildfires

- **Technological and industrial accidents, malfunctions, and other unscheduled disruptions**: aging infrastructure, chemical spills, equipment malfunction, hazardous substance releases, industrial fires, large scale power outages, structural failures

- **Criminal and terrorist incidents, foreign interference operations, and other malicious actions**:
    - Cybersecurity incidents such as denial of service attacks, malware, phishing active shooter incidents,
    - Supply chain attacks, vandalism, theft
    - Foreign influence to spread misinformation or undermine democratic processes, untrusted foreign investment that give foreign powers undue influence over a nation's critical infrastructure, property damage

[22]National Institute of Standards and Technology*, Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014). Version 1.1 of the framework was issued Apr. 16, 2018.
[23]See National Institute of Standards and Technology, *National Online Informative References Program*, at https://csrc.nist.gov/projects/olir.

4.2.1 Cybersecurity threats to critical infrastructure sectors

As noted above, cybersecurity and other technology-based incidents are key threats to critical infrastructure sectors. Ineffective protection of cyber assets from threats can increase the likelihood of security incidents and cyberattacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security, economic well-being, and public health and safety. Cyber threats to critical infrastructure can be classified as unintentional or intentional:

- *Unintentional* or non-adversarial threat sources may include failures in equipment or software due to aging, resource depletion, and errors made by end users. They also include the effects of natural disasters and failures of critical technological infrastructure on which the organization depends but that are outside of the control of the organization.

- *Intentional* or adversarial threats may include corrupt employees, criminal groups, terrorists, and nations that seek to leverage the organization's dependence on cyber resources (e.g., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies). These threat adversaries vary in terms of their capabilities, their willingness to act, and their motives, which can include seeking monetary gain or seeking an economic, political, or military advantage. Because systems and networks used by critical infrastructure sectors are often interconnected with other systems and the internet, they can be vulnerable to disruptions in service due to cyberattacks. Critical infrastructures in general are becoming more reliant on technology, which may leave them more vulnerable to attack. Attackers may use various tactics, such as gaining an initial foothold on target systems, running malicious code, and moving through various systems—to exploit vulnerabilities and position themselves to achieve their ultimate goals. The table below includes examples of common intentional cyberattack tactics for both IT and OT systems.

Table 1: Common Methods of Intentional Cyber Exploits

Exploit	Description
Watering hole	A method by which threat actors exploit the vulnerabilities of carefully selected websites frequented by users of the targeted system. Malware is then injected to the targeted system via the compromised websites.
Phishing and spear phishing	A digital form of social engineering that uses authentic-looking emails, websites, or instant messages to get users to download malware, open malicious attachments, or open links that direct them to a website that requests information or executes malicious code.
Credentials based	An exploit that takes advantage of a system's insufficient user authentication and/or any elements of cybersecurity supporting it, to include not limiting the number of failed login attempts, the use of hard-coded credentials, and the use of a broken or risky cryptographic algorithm.
Trusted third parties	An exploit that takes advantage of the security vulnerabilities of trusted third parties to gain access to an otherwise secure system.

Classic buffer overflow	An exploit that involves the intentional transmission of more data than a program's input buffer can hold, leading to the deletion of critical data and subsequent execution of malicious code.
Cryptographic weakness	An exploit that takes advantage of a network employing insufficient encryption when either storing or transmitting data, enabling adversaries to read and/or modify the data stream.
Structured Query Language (SQL) injection	An exploit that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database, resulting in data loss or corruption, denial of service, or complete host takeover.
Operating system command injection	An exploit that takes advantage of a system's inability to properly neutralize special elements used in operating system commands, allowing the adversaries to execute unexpected commands on the system by either modifying already evoked commands or evoking their own.
Cross-site scripting	An exploit that uses third-party web resources to run lines of programming code (referred to as scripts) within the victim's web browser or scriptable application. This occurs when a user, using a browser, visits a malicious website or clicks a malicious link. The most dangerous consequences can occur when this method is used to exploit additional vulnerabilities that may permit an adversary to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, or remotely access and control the victim's machine.
Cross-site request forgery	An exploit that takes advantage of an application that cannot, or does not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request, tricking the victim into executing a falsified request that results in the system or data being compromised.
Path traversal	An exploit that seeks to gain access to files outside of a restricted directory by modifying the directory pathname in an application that does not properly neutralize special elements (e.g. '…', '/', '…/', etc.) within the pathname.
Integer overflow	An exploit where malicious code is inserted that leads to unexpected integer overflow, or wraparound, which can be used by adversaries to control looping or make security decisions in order to cause program crashes, memory corruption, or the execution of arbitrary code via buffer overflow.
Uncontrolled format string	Adversaries manipulate externally-controlled format strings in print-style functions to gain access to information and/or execute unauthorized code or commands.
Open redirect	An exploit where the victim is tricked into selecting a URL (website location) that has been modified to direct them to an external, malicious site which may contain malware that can compromises the victim's machine.
Heap-based buffer overflow	Similar to classic buffer overflow, but the buffer that is overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a memory allocation routine, such as "malloc ()".

Unrestricted upload of files	An exploit that takes advantage of insufficient upload restrictions, enabling adversaries to upload malware (e.g., .php) in place of the intended file type (e.g., .jpg).
Inclusion of functionality from untrusted sphere	An exploit that uses trusted, third-party executable functionality (e.g., web widget or library) as a means of executing malicious code in software whose protection mechanisms are unable to determine whether functionality is from a trusted source, modified in transit, or being spoofed.
Certificate and certificate authority compromise	Exploits facilitated via the issuance of fraudulent digital certificates (e.g., transport layer security and Secure Socket Layer). Adversaries use these certificates to establish secure connections with the target organization or individual by mimicking a trusted third party.
Hybrid of others	An exploit combines elements of two or more of the aforementioned techniques.

Source: GAO, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, GAO-16-152 (Washington, D.C.: Dec. 17, 2015).

Examples of Recent Cybersecurity Attacks on Critical Infrastructure Sectors

The consequences of cyberattacks and incidents have already been felt by several critical infrastructure sectors:

Energy sector

In the 2015 cyberattacks on the Ukrainian power grid, attackers issued unauthorized commands to open the breakers at substations that three regional electricity utilities managed, causing a loss of power to about 225,000 customers. It appears the attackers used phishing emails to entice users to download malware onto their computers.

Transportation sector

In May 2021, the U.S.-based Colonial Pipeline Company announced that it was the victim of a ransomware attack that led to temporary disruption in the delivery of gasoline and other petroleum products across much of the southeast U.S.

Prior to the disruption, the U.S. GAO issued several findings and recommendations aimed at addressing significant weaknesses in pipeline security program management within the energy sector. For example, the GAO found that the government agency in charge of pipeline security efforts had no process for determining when to update guidelines for pipeline operators and needed to update its method for assessing risks.

The audit team made 10 recommendations related to these findings, including establishing better processes for updating guidelines and assessing risks. As of May 2022, two of the 10 recommendations remain open. Specifically, the U.S. GAO had recommended that the government agency in charge of U.S. pipeline security incorporate additional risk data into

its analysis of the relative risk of critical pipeline system, and coordinate an external peer review of this risk analysis. If these steps were completed, there would be a better understanding of the relative risk among pipeline systems using the most comprehensive and accurate threat, vulnerability, and consequence information.

Communications sector

In February 2022, Viasat, Inc. began experiencing outages with its European satellite internet service near the start of the Russian invasion of Ukraine, according to press reporting. According to Viasat, the disruption was triggered by an attacker running destructive commands against Viasat network devices. In its forensic analysis of the incident, Sentinel Labs noted that the malware used in this attack shares some similarities with malware used in attacks attributed to the Russian government. As a result of the attack, a German wind turbine manufacturer explained that remote operation of more than 5,000 turbines had been affected. In March 2022, CISA and the FBI warned critical infrastructure and other organizations of possible threats to U.S. and international satellite communication networks.

Water and wastewater sector

In February 2021, the United States Department of Homeland Security issued an alert explaining that cyber threat actors obtained unauthorized access to a U.S. water treatment facility's industrial controls systems and attempted to increase the amount of a caustic chemical that is used as part of the water treatment process.[1] According to the Department of Homeland Security, threat actors likely accessed systems by exploiting cybersecurity weakness, including poor password security and an outdated operating system.

The alert recommended several recommendations to assist organizations in the water sector, including:

- cyber hygiene measures, including updating to the latest version of the operating systems and using strong passwords;
- physical security measures, such as installing systems hat physically prevent dangerous conditions from occurring in the event of a cyberattack; and
- recommendations on the use and implementation of the specific software the hacker used to gain access to the systems.

Healthcare and public health sector

In October 2020, during the COVID-19 pandemic, cybercriminals targeted several organizations in the healthcare and public health sector. The cybercriminals disseminated the malicious software using phishing campaigns that contain either links to malicious websites that host the malware or attachments with the malware. In response to these attacks, the U.S. Department of Homeland Security made several recommendations to organizations in the sector, including maintaining business continuity plans, performing cyber hygiene practices such as patch management, and ensuring that staff are trained.

Threats to multiple sectors

- In June 2017, the "NotPetya" malware was discovered. After NotPetya infected a machine on which that software was installed, it was capable of automatically spreading through a network and infecting other machines. NotPetya spread worldwide, damaged computers used in critical infrastructure, and is estimated to have caused about $10 billion in damages globally. For example, it had infected organizations in several sectors in the U.S., including finance, transportation, energy, commercial facilities, and healthcare. The "NotPetya" malware exploited existing vulnerabilities in computer software or networks to encrypt files and allowed attackers to gain privileged rights and encrypt essential files, thus making the infected Windows computers unusable.

- In December 2020, the U.S. Department of Homeland Security issued an emergency directive and alert explaining that an advanced persistent threat actor had compromised the supply chain of a network management software suite and inserted a "backdoor"—a malicious program that can potentially give an intruder remote access to an infected computer—into a genuine version of that software product. The malicious actor then used this backdoor, among other techniques, to initiate a cyberattack campaign against U.S. government agencies, critical infrastructure entities, and private sector organizations.

4.3 Considerations for Auditing Critical Infrastructure Sectors

When auditing critical infrastructure sectors, it is important to identify key vulnerabilities for that sector, identify stakeholder and regulatory roles for the sector, and identify potential audit findings, as described in more detail below.

4.3.1 Identifying Key Vulnerabilities, Threats, and Actors

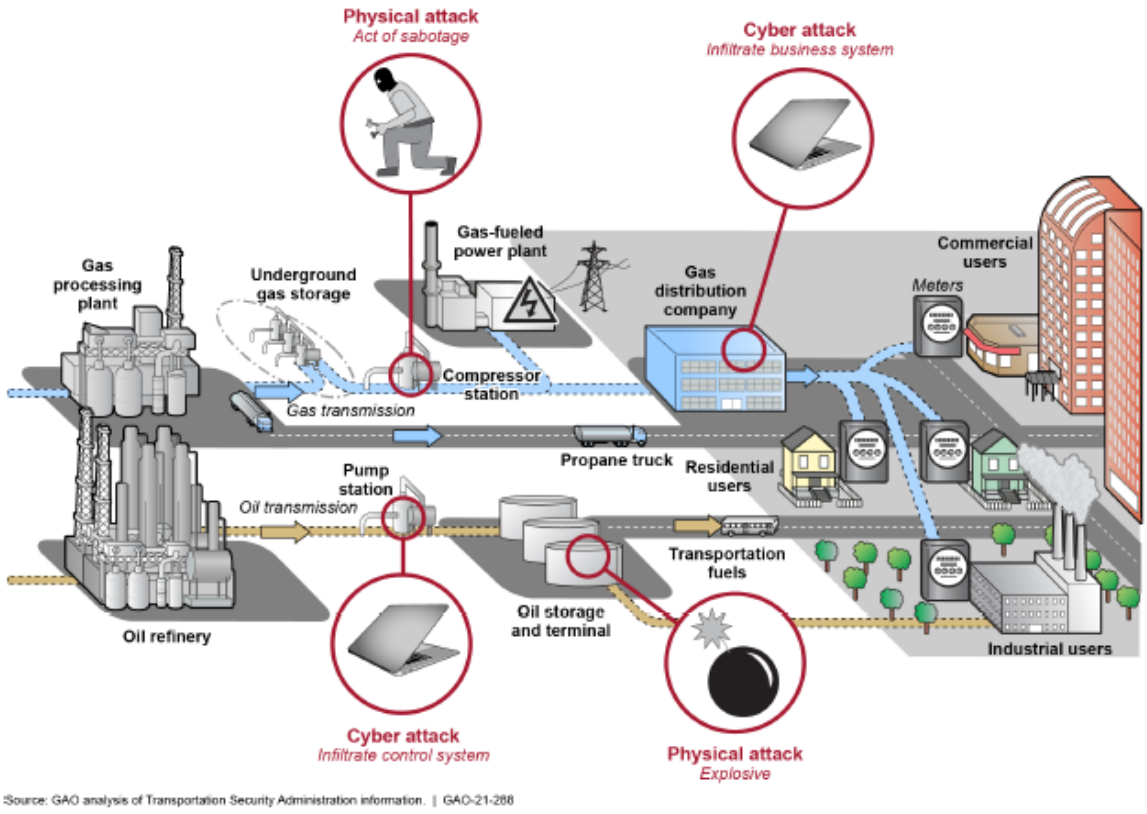
It is important that auditors have a sufficient understanding of the technologies used by a critical infrastructure sector, or key stakeholders or companies within that sector, to identify potential areas of vulnerability. It is also important that audit teams analyze the threats and hazards described above to determine how likely they are to occur and what their potential impacts on the critical infrastructure sector might be.

Each sector uses unique systems and technology to accomplish its goals, but the potential vulnerabilities across the sectors may be similar. However, the consequences and impacts of cybersecurity attacks may be different depending on the technologies used by that sector. Examples of these are described in more detail below.

Energy sector. Figure 2 depicts key potential vulnerabilities for a provider in the energy critical infrastructure sector. The sophisticated computer systems that pipeline operations rely on are vulnerable to various cyber threats, including malicious actors infiltrating business or control systems. For example, an attacker could infiltrate a pipeline's operational systems via the internet or other

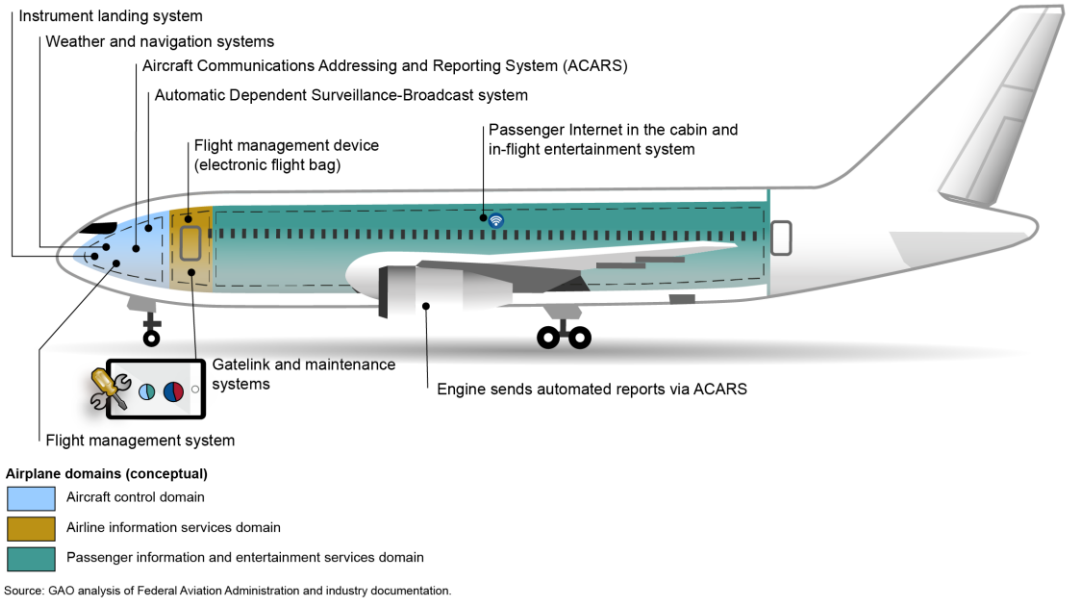
communication pathways to potentially disrupt its service and cause spills, releases, explosions, or fires.

Figure 3. U.S. Natural Gas and Oil Pipeline Systems' Basic Components and Examples of Vulnerabilities



Transportation sector. Modern airplanes are equipped with networks and systems that share data with the pilots, passengers, maintenance crews, other aircraft, and air-traffic controllers (as depicted in fig. 3). These networks and systems share data in ways that were not previously feasible, which creates risk in this sector for entities that have not analyzed the implications of and increasing connectivity in an environment of evolving cyber threats. Vulnerabilities could occur due to (1) not applying modifications (patches) to commercial software, (2) insecure supply chains, (3) malicious software uploads, (4) outdated systems on legacy airplanes, and (5) flight data spoofing.

Figure 4. Key Systems Connections to Commercial Airplanes



Source: GAO analysis of Federal Aviation Administration and industry documentation.

Financial services sector. The composition of the financial services sector extends beyond the categories of financial services to include a network of essential specialized service organizations and service providers that support the sector in its efforts to provide a trusted services environment. For example, the financial services sector has become more dependent on outsourcing certain activities—such as systems and applications, hardware and software, and technically skilled personnel—to third-party providers that are now an indispensable part of the sector's infrastructure. Further, mobile payment applications allow consumers to use their smartphones or other mobile devices to make purchases and transfer money instead of relying on the physical use of cash, checks, or credit and debit cards. Due in part to the introduction of these new technologies, the financial services sector has even stronger need for information technology capabilities and support from supply chain partners and third-party service providers. A successful widespread cyberattack could erode public confidence in financial institutions, deny businesses and individuals access to their funds, result in the loss of funds, or affect the integrity of financial information.

Regardless of which sector is being audited, the team must understand the systems and technology used in that sector, and the potential threats and vulnerabilities. This may be accomplished by reviewing any documentation developed by organizations within the sector, completing physical reviews of companies or locations, and interviewing organizations within the sector. To identify vulnerabilities, an auditor may review prior reports on cyber-based threats facing the sector as well as the threats identified by cybersecurity organizations.[24] Auditors should also interview subject matter experts to confirm their understanding of threats and vulnerabilities.

[24]The U.S. Department of Homeland Security has developed several resources that may assist auditors in evaluating IT and OT. For example, the Cybersecurity Evaluation Tool is a stand-alone desktop application that guides asset owners and operators through a systematic process of evaluating IT and OT systems, and includes a ransomware readiness assessment. See https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr.

4.3.2 Identifying Stakeholder Roles and Regulatory Frameworks

The effort to strengthen critical infrastructure security depends on the extent to which public and private sector critical infrastructure owners and operators to make risk-informed decisions collaboratively. It also depends on their ability to share information regularly to ensure that risk is managed properly. In certain countries such as the United States, the private sector owns the majority of the nation's critical infrastructure instead of the government. Thus, it is vital that the public and private sectors work together to protect these assets and systems.

Each country may oversee critical infrastructure sectors differently. In some cases, there may be a body in charge of regulating all activity for that sector. In other cases, there may be a government body that collaborates with critical infrastructure owners and operators and provides government support as needed but does not have a direct oversight role. Additionally, a particular country may not have regulators or regulatory bodies overseeing or providing support for a sector. Before beginning an audit, it is important that auditors understand the roles and responsibilities for protecting the sector that they are evaluating.

For example, in the United States, efforts to protect various critical infrastructure sectors are carried out through the joint efforts of multiple components of a public-private partnership model, including government agencies. These federal government agencies, referred to as "sector risk management agencies," prioritize and coordinate security and resilience efforts and carry out incident management responsibilities for their assigned critical infrastructure sectors. For example:

These critical infrastructure sectors may be regulated in different ways. For example, the electricity subsector of the energy sector is highly regulated in the United States. The U.S. Department of Energy is responsible for, among other things, collaborating with critical infrastructure owners and operators, identifying vulnerabilities, and helping to mitigate incidents. The U.S. Department of Homeland Security assists those efforts by coordinating the overall federal effort to promote the security and resilience of the nation's critical infrastructure. In addition to those agencies, U.S. federal and state authorities play key roles in regulating the reliability of the grid, which can be impaired by cybersecurity attacks. For example, the Federal Energy Regulatory Commission is the federal regulator of interstate transmission of electricity with responsibility to review and approve standards to provide for the reliable operation of the bulk power system. The commission also oversees the North American Electricity Reliability Corporation, which is responsible for conducting reliability assessments and enforcing mandatory standards to ensure the reliability of the bulk power system.

These agencies and organizations provide cybersecurity support to operators in this critical infrastructure sector. For example, the Departments of Energy and Homeland Security offer services aimed at helping grid owners and operators assess cybersecurity risks and perform forensic analysis. They have also developed policies, strategies, and plans to define their roles and responsibilities for responding to and recovering from grid cybersecurity incidents. The Federal Energy Regulatory Commission has also performed regulatory activities aimed

at addressing grid cybersecurity risks, such as approving mandatory cybersecurity standards, and enforcing regulatory requirements through imposition of civil penalties.

Other sectors may not be as regulated:

- In the **transportation sector**, the U.S. Federal Aviation Administration is co-lead, with the U.S. Department of Homeland Security, on infrastructure protection activities specifically for the avionics subsector. The Federal Aviation Administration is responsible for the safety and oversight of commercial aviation, which includes the certification and oversight of all US commercial aviation products and commercial entities, while the Department of Homeland Security is responsible for coordinating federal government activities addressing aviation security.

- In the **financial services sector**, the U.S. Department of the Treasury is the sector risk management agency charged with coordinating the partnership between private sector firms and the federal government. However, Treasury works with other stakeholders, such as federal regulators and industry groups, to enhance the security of the financial services sector and assist members of the sector to collaborate to mitigate risks.

4.3.3 Identifying Potential Challenges or Audit Findings

In order to identify findings and areas for improvement, an audit team should use the information they gathered about the potential vulnerabilities, as well as the information about the regulatory or oversight framework, to determine how to design the audit and which methodologies to use.

If there is an oversight body, an audit team may work to identify how effective the cybersecurity oversight has been for that sector. If there is no oversight body, the audit team may consider evaluating the cybersecurity policies and procedures for key companies or organizations within the critical infrastructure sector.

Key Questions to Ask during an Audit

- If there is an oversight or regulatory body:
  - **Oversight**:
    - Have they established an oversight program that includes cybersecurity? Have they completed a risk assessment related to the sector? Have they defined program objectives based on that risk assessment? Do they have control activities related to the identified risks?
    - Do they oversee/evaluate the implementation of cybersecurity and data protection controls? If so, how? Did they produce oversight reports or other documents? If not, why not?
  - **Guidance**: Have government or other regulatory bodies identified guidance (such as the NIST cybersecurity framework), or developed guidance, that could be used in the particular sector(s)?
    - Have they taken steps to encourage the use of relevant guidance?

        - Have they taken steps to determine whether organizations in the sector follow the relevant guidance (e.g., by using surveys, reporting, assessments, or other mechanisms)?
        - If the oversight body has developed guidance, does that guidance reflect the current threat environment? Does the guidance reflect requirements in law or best practices from applicable standards (such as ISO/IEC 27001:2013, COBIT 2019, and the NIST *Framework for Improving Critical Infrastructure Cybersecurity*)?
    - **Enforcement**: Do they have enforcement authority? If so, do they take enforcement measures?
    - **Workforce**: Do they have the appropriate staff/skills to oversee cybersecurity and data protection policies and procedures? Do they provide appropriate training to staff, and how often?
    - **Collaboration**: Have supporting organizations assisted in identifying improvements that could be made? Have roles and responsibilities been identified? If applicable, have participating organizations documented their agreement regarding how they will collaborate? How do sector stakeholders share security-related information?
- If there is no government oversight body, an auditor may determine whether the critical infrastructure owner/operator has a cybersecurity risk management program and/or has performed a cybersecurity risk assessment using the criteria identified above and in chapter 3 of this document.

For example, in October 2020, the U.S. GAO reported that, as part of its responsibilities in the **transportation sector**, the U.S. Federal Aviation Administration (FAA) should prioritize oversight of evolving cyber threats and increasing connectivity between airplanes and other systems:[25]

- **Oversight**: FAA had not conducted an assessment of the risks to avionics systems to determine the relative priority of cybersecurity risks to avionics systems versus other safety concerns in its oversight program. Without such an assessment, the GAO reported that FAA may not be able to appropriately strengthen its oversight program specific to avionics systems cybersecurity issues;
- **Guidance**: FAA had established a process for the certification and oversight of U.S. commercial airplanes, including their operations;
- **Enforcement**: FAA's monitoring of the implementation of avionics cybersecurity controls in airplanes that are deployed in active service with air carriers does not include policies or procedures for periodic testing. The GAO reported that until FAA develops policies and procedures for periodic testing as part of its monitoring process, it may be unable to ensure that cybersecurity controls remain effective in mitigating evolving threats in deployed airplanes;
- **Workforce**: FAA did not have a staff training program specific to avionics cybersecurity, and none of the agency's certification staff are required to take cybersecurity training tailored to their oversight role. The GAO reported that until FAA establishes a staffing and training program appropriately tailored to avionics

[25]GAO, *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks*, GAO-21-86 (Washington, D.C.: Oct. 9, 2020).

cybersecurity, the agency may not have the expertise necessary to address the increasing cybersecurity risks to these systems; and

- **Collaboration**: The GAO also reported that FAA coordinated with other key federal agencies and industry to address aviation cybersecurity issues. However, FAA's internal coordination activities did not fully reflect key collaboration practices. For example, FAA had not established a tracking program for monitoring progress on issues raised at meetings, and the oversight was not supported through dedicated agency resources in its budget. The GAO reported that until FAA prioritizes coordination efforts based on that assessment, it may not be allocating resources and coordinating on risks as effectively as it could.

4.4 Example Audit Reports on Critical Infrastructure

4.4.1 Government-Wide Critical Infrastructure Reviews

- GAO, *Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance*, GAO-22-105103 (Washington, D.C.: Feb. 9, 2022).
- GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021).
- GAO, *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, GAO-20-299 (Washington, D.C.: Feb. 25, 2020).
- GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 15, 2018).
- GAO, C*ritical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, GAO-16-152 (Washington, D.C.: Dec. 17, 2015).
- GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015).

4.1.1. Sector-Specific Critical Infrastructure Reviews

- *Communication:* GAO, *Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector,* GAO-22-104462 (Washington, D.C.: Nov. 23, 2021).
- *Energy:*
    - GAO, *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81 (Washington, D.C.: Mar. 18, 2021).
    - GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48 (Washington, D.C.: Dec. 18, 2018).

- *Transportation:* GAO, *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks*, GAO-21-86 (Washington, D.C.: Oct. 9, 2020).

- *Financial services:* GAO, Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts, GAO-20-631 (Washington, D.C.: Sept. 17, 2020).

Appendix – Acronyms and abbreviations

ANAO	Australian National Audit Office
BAI	Board of Audit and Inspection of Korea
CAF	Cyber Assessment Framework
CCPA	California Consumer Privacy Act
CEH	Certified Ethical Hacker
CERT	Computer Emergency Response Teams
CESG	Canada Education Savings Grant
CII	Critical information infrastructure
CIS	Center for Internet Security
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CMM	Cybersecurity Capacity Maturity Model for Nations
CNI	Critical National Infrastructure
COBIT	Control Objectives for Information and Related Technologies
CRISC	Certified in Risk and Information Systems Control
CSIRT	Computer Security Incident Response Team
CySA+	CompTIA Cybersecurity Analyst
DEDJTR	Australia Department of Economic Development, Jobs, Transport and Resources
DELWP	Australia Department of Environment, Land, Water and Planning
DHHS	Australia Department of Health and Human Services
DHS	U.S. Department of Homeland Security
DJR	Australia Department of Justice and Regulation
DORA	Digital Operational Resilience Act
DRS	Disaster Recovery System
DSP	Digital Services Providers
ENISA	The European Union Agency for Cybersecurity
FAA	U.S. Federal Aviation Administration
FEMA	U.S. Federal Emergency Management Agency
FIRST	Forum of Incident Response and Security Teams
GAO	United States Government Accountability Office
GCI	The Global Cybersecurity Index
GDPR	General Data Protection Regulation
GSEC	GIAC Security Essentials Certification
HVAC	Heating, Ventilation, and Air Conditioning
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IS	Information System
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITAF	Information Technology Assurance Framework
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
KLID	Korean Local Information Research and Development Institute
MMA	Military Manpower Administration
MOSPA	Ministry of Security and Public Administration
NATO	North Atlantic Treaty Organization

NCAF	National Capabilities Assessment Framework
NCCIC	National Cybersecurity and Communications Integration Center
NCS	National Cybersecurity
NCS	National Cybersecurity Systems
NDRF	National Disaster Recovery Framework
NIMS	National Incident Management Structure
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
OES	Operator of Essential Services
PII	Personally Identifiable Information
PMBOK	Project Management Body of Knowledge
PYME	Small and Medium Enterprise (for its acronyms in Spanish: *Pequeña Y Mediana Empresa*).
RSF	Recovery Support Function
SAI	Supreme Audit Institution
SCCs	Sector Coordinating Council
SETIC	Information Technology Infrastructure Secretariat
SIEM	security information and event management
SIM3	Security Incident Management Maturity Model
SQL	Structured Query Language
SSAs	Sector Specific Agencies
TCA	Turkish Court of Accounts
TCU	Tribunal de Contas da União (Federal Court of Accounts – Brazil)