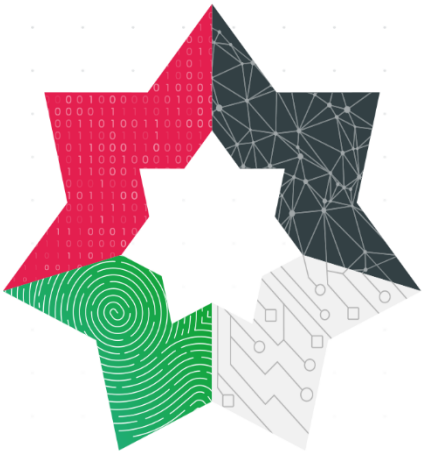
I



المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

Critical Infrastructure Cyber Security Controls

CICSC GUIDANCE

December 2024

CONTENTS

1 INTRODUCTION

Over the last five years, the number of cyber incidents in Jordan has risen dramatically. Critical infrastructure organizations – particularly those that rely on Operational Technology, such as energy, health, transport, and water – are increasingly being targeted, by hacktivist, criminal, and state-backed groups, threatening to disrupt Jordan's economy and way of life.

This implementation of appropriate security controls is a key component to securing information management and technology across Jordan's critical infrastructure. Accordingly, the controls contained in the Critical Infrastructure Cyber Security Controls (CICSC) set out core and advanced requirements to be applied to ensure a consistent level of cyber security across Jordan.

CICSC is derived from internationally recognised Information Technology and Operational Technology security standards developed by the National Institute of Standards and Technology (NIST). Specifically, CICSC draws its controls from NIST Special Publication 800-53 (revision 5), NIST Special Publication 800-82 (revision 3) which is applicable to Operational Technology in all industrial sectors, and the security baselines set out in NIST Special Publication 800-53B. As part of the NIST Cyber Security Framework, collectively the controls derived from NIST SP 800-53(rev.5), NIST SP 800-82 (rev.3) and NIST SP 800-53B provide a robust and comprehensive set of controls for critical national infrastructure organizations.

Within CICSC, specific control parameters set out in NIST SP 800-53 (rev.5) have been customised based on experience and good practice to offer clear and common guidance to all critical infrastructure organizations. References within NIST to specific US agencies, bodies, or publications have also been amended or removed to provide clear guidance to Jordanian organizations.

The 405 controls within CICSC are split into three Implementation Levels, with 135 Level 1 controls providing a baseline level of protection for all critical infrastructure operators. Depending on criticality of the organization or system to be protected, these can be built upon through the adoption of a further 161 Level 2 controls, and further enhanced with the application of 109 Level 3 controls to reduce the risk of significant disruption posed by more advanced threats. The allocation of controls to Implementation Levels has also been informed by a review of the Mitre Corporation's mapping of NIST SP 800-53 controls against common techniques used by activist, criminal and state-level threat actors. See the accompanying CICSC Threat Annex for more information.

To ensure a common level of protection across Jordan, critical infrastructure organizations are expected to adopt all Level 1 controls relevant to their organizations. Controls marked 'optional' should also be adopted unless protection is already provided by existing physical, maintenance or other mitigating controls. Operators of critical infrastructure can strengthen this common level of protection by drawing on additional controls from NIST SP 800-53 (rev.5) or other recognised standards to enhance this baseline further.

Adoption of CICSC by operators of critical services will increase cyber security resilience across Jordan's critical infrastructure, supporting public sector service delivery, sustainable digital transformation, and Jordan's economic stability.

1.1 Scope

The controls within CICSC are applicable to Operational Technology (OT) and Information Technology (IT) that is linked to or part of that environment. For the purposes of CICSC, OT

relates to a category of hardware and software that monitors and controls a physical process. It encompasses a broad range of programmable systems or devices that interact with the physical environment and software systems that are used to control and monitor physical processes, including:

- **Industrial Control Systems** - systems that manage and operate infrastructure-supporting functions like water, power, transportation, manufacturing, and other critical services.
- **Supervisory Control and Data Acquisition** - systems of software and hardware elements that allows organizations to control and monitor industrial processes by directly interfacing with plant-floor machinery and viewing real-time data.
- **Distributed Control Systems** - integrated control systems that manage complex processes within large-scale industries.
- **Programmable Logic Controllers** - specialised computers designed to operate in industrial settings, managing and automating the mechanical processes of factories and plants.
- **Industrial Internet of Things** – the ecosystem of intelligent devices connected to form systems that collect, monitor, and exchange data with one another, primarily for manufacturing and energy management.

Examples of critical operational technology include security systems (e.g. CCTV), climate control systems (such as heating, ventilation, and air conditioning systems), other Building Management Systems, and the software and hardware supporting Safety Instrumented Systems.

Unlike IT - which is designed to be networked, typically has a short life-span, and can benefit from mature support services, with frequent updates and testing – OT can comprise standalone, specialist systems, designed to run for 20 years or more. Though increasingly connected, updates can be complex to deliver and infrequent due to the disruption to services.

Within CICSC, any specific OT considerations relevant to the controls are included. Termed 'Overlays' by NIST, these are drawn from NIST SP 800-82 (rev.3). See Appendix C of NIST SP 800-53B for further information on the concept of Overlays.

Derived from NIST SP 800-53 (rev.5), the majority of controls within CICSC will also help provide a basis for securing Cloud environments, notably those controls relating to Access Control (AC), Incident Response (IR), and Risk Assessment (RA) to name a few

1.2 Critical Infrastructure

Critical infrastructure is defined in the Cyber Security Law No. (16) of 2019 as the:

> *Set of electronic systems and networks and material and non-material assets or cyber assets and systems the continuous operation of which is necessary to ensure the security of the state and its economy and the safety of the society.*

Many operators of critical infrastructure rely heavily on interconnected Operational Technology (such as industrial control systems) and IT to manage their key operations. This provides opportunities for threat actors to interfere with these systems for political, ideological, economic or financial gain.

Critical infrastructure sectors that rely on IT and OT are particularly vital to the Kingdom's security and economic well-being and include:

- Defence, Security, and Government Services

- Energy – overseen by the Energy and Minerals Regulatory Commission
- Finance – overseen by the Central Bank of Jordan
- Health – overseen by the Ministry of Health
- Telecommunications – overseen by the Telecommunications Regulatory Commission
- Transport - regulated by the Land Transport Regulatory Commission, Civil Aviation Regulatory Commission, and the Jordan Maritime Commission
- Water - overseen by the Jordan Water Authority
- Manufacturing – overseen by the Ministry of Industry and Trade

The Government of Jordan has leadership responsibility to ensure that critical infrastructure, whether public or privately owned, is protected against cyber threats. CICSC therefore is intended to apply to all operators of critical infrastructure in Jordan that depend on IT and OT, including the sectors highlighted above.

1.3 JNCSF Alignment

Published in June 2024, Jordan's National Cyber Security Framework (JNCSF) provides a comprehensive approach for all government entities on how to manage and mitigate cyber risk. CICSC supports JNCSF by providing specific controls that help to counter cyber threats, minimise disruption, and enhance resilience.

To support the implementation of the controls, a supporting CICSC Annex includes additional contextual information relating to the controls as provided by NIST SP 800-53 (rev.5), plus references to relevant JNCSF controls. The aim of this alignment is to help operators of critical infrastructure to establish their baseline when implementing JNCSF to comply with NCSC-Jordan requirements and ensure clear understanding of how they are building on this solid foundation to augment their IT and OT environments.

The diagram above illustrates the core inputs to CICSC, and shows the strong connection to Jordan's National Cyber Security Framework – which is at the heart of driving high-standards of cyber security in Jordan.

2 SOURCES AND DEFINITIONS

2.1 Sources

Republished courtesy of the National Institute of Standards and Technology, the controls included within CICSC are derived from the following publications:

> Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations, (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 800-53 Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5
>
> Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 3. https://doi.org/10.6028/NIST.SP.800-82r3
>
> Joint Task Force (2020) Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B. https://doi.org/10.6028/NIST.SP.800-53B

2.2 Important Terminology

The table below defines common terms used throughout CICSC. A summary of more general IT and OT terminology can be found in the CICSC Glossary.

Availability	Information is readily accessible to authorized users.
Confidentiality	Ability to protect information from unauthorized access.
Controls	The safeguards and protections needed to meet particular security objectives and adopted by organizations to meet their system requirements.
Integrity	The ability to ensure that data is an accurate and unchanged representation of the original secure information.
Must	In this document, "Must" and "Shall" have the same meaning.
Prohibit	To forbid or disallow. In cyber terms this may be through the application of technical controls (e.g. writing to USB prohibited by software) or by non-technical controls such as Policy or Guidance (e.g. an IT Acceptable Use Policy).
Requirements	This term is used broadly to refer to legal, policy or other external information and security requirements that an organizations must comply with.

Shall	The statement is an absolute requirement of the specification (equivalent to "Must"). Where compliance cannot be achieved, it is advisable to record why a control cannot be implemented.
Should	Compliance with the requirement is expected, however there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood, carefully weighed and documented before choosing a different course.

3 SCOPE & CONTROL STRUCTURE

3.1 CICSC Scope

CICSC contains a set of security controls and control enhancements providing additional protection that apply to the people, process, and technology related to IT and OT elements within critical infrastructure. In doing so, it aims to provide a suite of controls that address the IT-OT convergence and so will help to avoid potential silos in governance and accountability, bring unity across the teams that manage these systems, and foster collaboration towards common goals. The provision of a single, common set of controls to help counter the increasing cyber threats facing Jordan will help increase effectiveness and add extra value for operators of critical infrastructure.

Public and private sector organizations responsible for Jordan's critical infrastructure are required to apply Level 1 controls relevant to their organizations' IT and OT environments.

CICSC spans the following groups of controls, referred to in NIST as control families:

ID	Control Family	No. of Controls
AC	Access Control	52
AT	Awareness & Training	7
AU	Audit & Accountability	34
CA	Assessment, Authorization, & Monitoring	15
CM	Configuration Management	33
CP	Contingency Planning	37
IA	Identification & Authentication	29
IR	Incident Response	19
MA	Maintenance	13

ID	Control Family	No. of Controls
MP	Media Protection	10
PE	Physical & Environmental Protection	27
PL	Planning	8
RA	Risk Assessment	11
SA	System & Services Acquisition	24
SC	System & Communications Protection	39
SI	System & Information Integrity	30
SR	Supply Chain Risk Management	17

As organizations might follow alternative control guidance in relation to Maintenance and Physical & Environmental Protection, 18 enhancement controls in these two control families have been designated as optional. Where controls are optional, this is flagged clearly beneath the Control ID.

CICSC does not include the following NIST SP 800-83 (rev.5) control families that extend beyond the remit of IT and OT security teams:

- Program Management (PM)
- Personnel Security (PS)
- Personally Identifiable Information Processing and Transparency (PT)

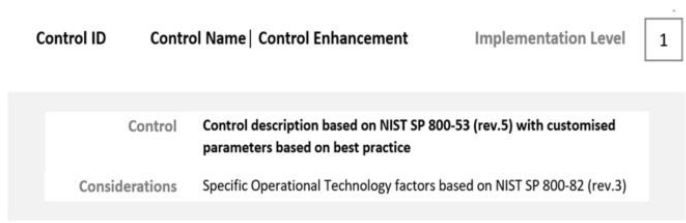
The selection of control families, controls, and control enhancements was informed by engagement with IT and OT stakeholders working across a range of Jordan's critical sectors – including energy, water, aviation, mining, and health during 2024. Additionally, the selection of NIST controls was informed by a review of the ISA/IEC 62443 series of standards – which provides best practice for securing industrial automation and control systems.

3.2 Control Structure

Combining elements of NIST SP 800-53 (rev.5) and NIST SP 800-82 (rev.3) and informed by NIST SP 800-53B, the controls in CICSC comprise a control definition, a section highlighting any specific OT considerations relevant to the control, and a recommended Implementation Level. Within CICSC, NIST SP 800-53 (rev.5) controls that have flexible parameters have been customised to define specific values associated with the appropriate control level. See section 3.4 for further details on customisation and use of examples.

The diagram below illustrates the structure of CICSC controls.

The *Control ID*, *Control Name* and *Control Enhancement* are drawn from NIST SP 800-53 (rev.5).



The *Implementation Level* is indicated from 1 to 3 and informed by NIST SP 800-53B and an understanding of specific threats facing Jordan.

If a control is *Optional*, this will be indicated beneath the Control ID.

The *Control* text is derived from NIST 800-53 (rev.5) and customised to include best practice.

The text next to *Consideration*, drawn from NIST SP 800-82, shows any specific considerations that relate to Operational Technology.

3.3 Control Interpretation

Derived from NIST SP 800-53 (rev.5), additional contextual information for each control in the form of a control explanation and interpretation is provided in a supporting CICSC Annex.

The Annex explains the control usability and practicality in the real world and includes references to related NIST SP 800-53 (rev.5) controls and the respective mappings to the Jordan National Cyber Security Framework (JNCSF).

- Related NIST controls are those that either impact or support the implementation of particular control/s or control enhancement/s.
- JNCSF mappings provide a high-level overview how controls and control enhancements are related and linked together, which will help organizations complement their compliance to JNCSF.

3.4 Control Parameters & Examples

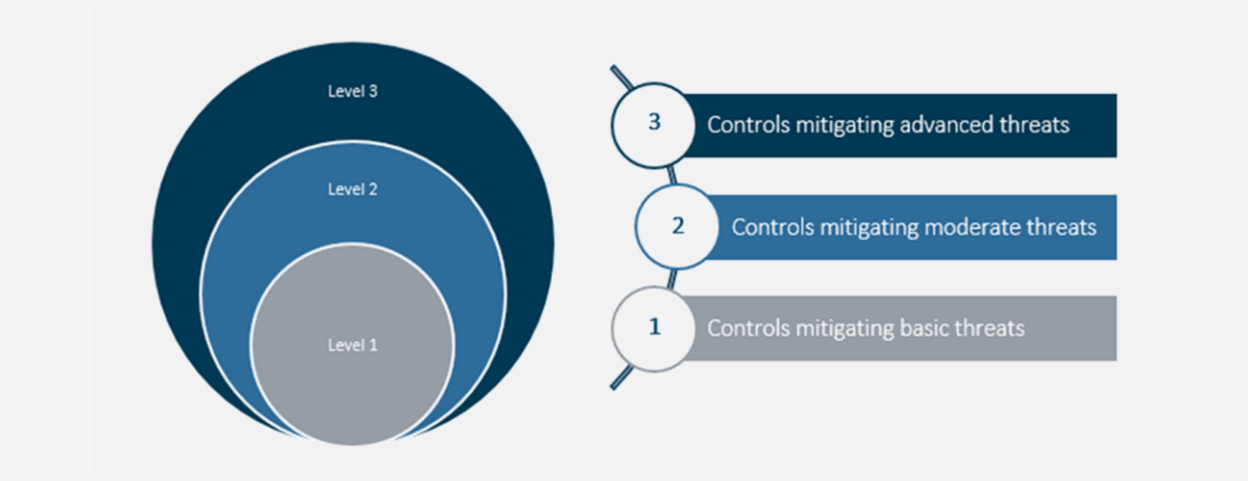
Many of the controls within NIST SP 800-53 (rev.5) include flexible parameters that allow organizations to define specific control values – such as actions (remove/disable) or the appropriate frequency of a control occurring (e.g. how long a device should be allowed to stay inactive before automatically locking).

Within CICSC, where NIST SP 800-53 (rev.5) controls included flexible parameters these have been customised to provide common guidance to all organizations. These customisations are intended to provide examples of best practice that illustrate how a control should be applied.

Organizations adopting CICSC are entitled to adjust these examples (e.g. to reduce or extend the frequency of a control occurring) to suit their specific organizational needs and should not be constrained by the examples provided.

3.5 Implementation Levels

The security controls within CICSC are split across three Implementation Levels. Each level builds on the previous one and is intended to counter increasing levels of threat as shown in the diagram below.



All organizations are expected to adopt Implementation Level 1 controls to provide a comprehensive security baseline.

- **Level 1: Basic Threats**[1] - The 135 controls in Implementation Level 1 are designed to protect against basic threats. At this level, threat actors have limited or very limited resources, expertise, motivation and opportunity to support a sustained successful attack.

Based on an organization's - or potentially a sector's - level of criticality to the Kingdom of Jordan, NCSC-JO may determine that organizations should also implement controls at Levels 2 or 3:

[1] Descriptions of Implementation Levels are adapted from NIST 800-30r1 characteristics of adversary capabilities.

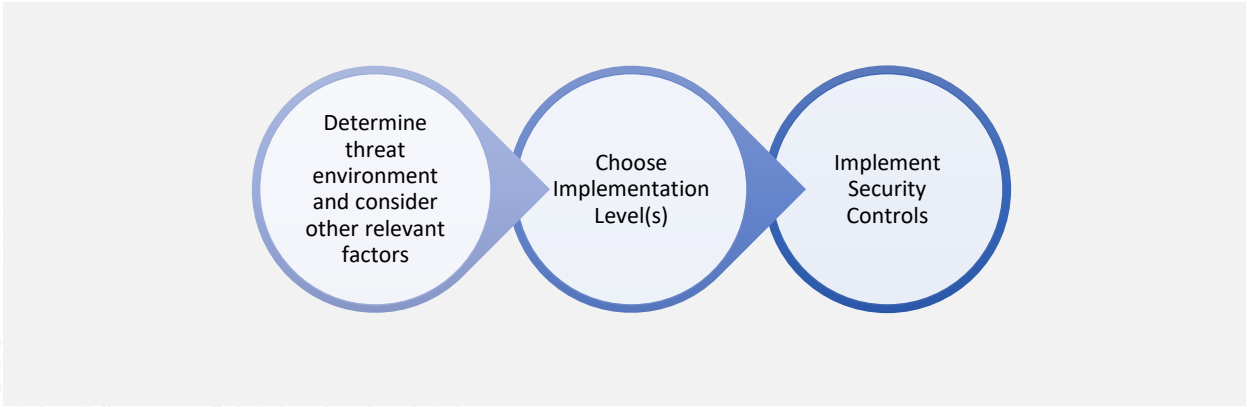
- **Level 2: Moderate Threats** - The 161 controls in Implementation Level 2 are designed to protect against moderate threats. At this level, threat actors have moderate resources, expertise and opportunities to support multiple successful attacks.
- **Level 3: Advanced Threats** - The 109 controls in Implementation Level 3 are designed to help protect against complex threats. At this level, threat actors have a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks – which could include espionage and destructive attacks. Adoption of these controls will make IT/OT difficult to attack successfully, but no controls can guarantee complete protection against the most persistent adversaries.

Each Implementation Level builds on the previous Level and should be implemented sequentially within Control Families to provide effective protection.

3.6 Applying Implementation Levels

The timeframe for implementing CICSC will vary by organization, but is likely to take between 6-18 months.

When applying CICSC, organizations should start by considering the appropriate Implementation Level to target for their IT/OT environment. A monolithic, segmented or a phased approach should help organizations to choose the best method for them based on their capabilities and expertise.



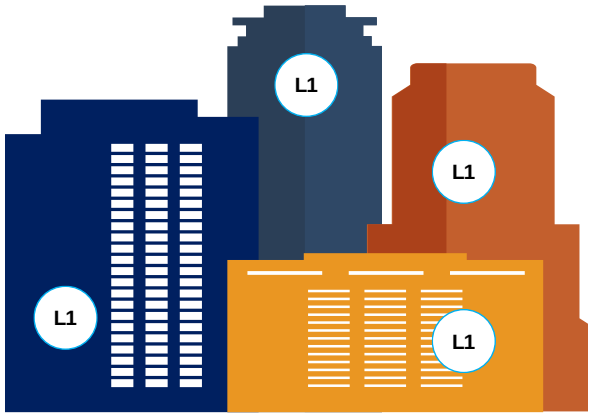
3.7 Monolithic Approach

In a monolithic approach, the organization uses its knowledge of the threat environment in which it operates to choose one of the three Implementation Levels that will counter the threats it faces. Budget, available resources and training may also be considered. This Implementation Level is then applied across the organization's IT/OT environment.

Illustrated in the diagram on the right, the advantage of the monolithic approach is that the Implementation Level can be chosen using a relatively simple analysis process, allowing for maximum investment in securing the IT/OT environment itself.

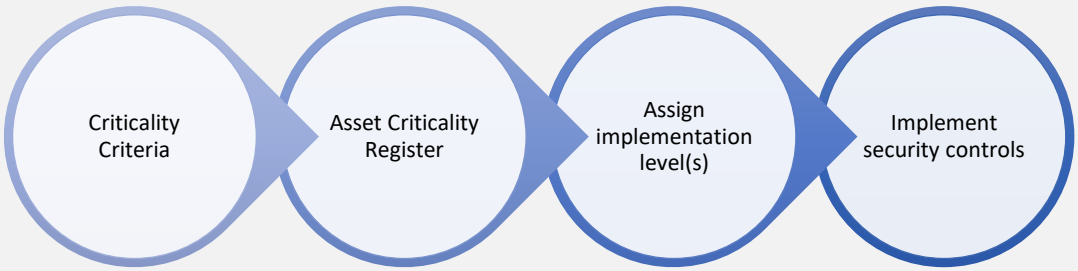
The disadvantage of this approach is that it does not consider other important factors such as the context in which specific IT/OT systems operate, their relative importance to the business in case of impact and their location within the network - which can affect their relative vulnerability to compromise. This could lead an organization to implement overly stringent or costly security controls in some IT/OT systems within its environment. At the same time, a limited number of highly critical IT/OT systems could be under protected.

Figure 1: Monolithic implementation



3.8 Segmented Approach

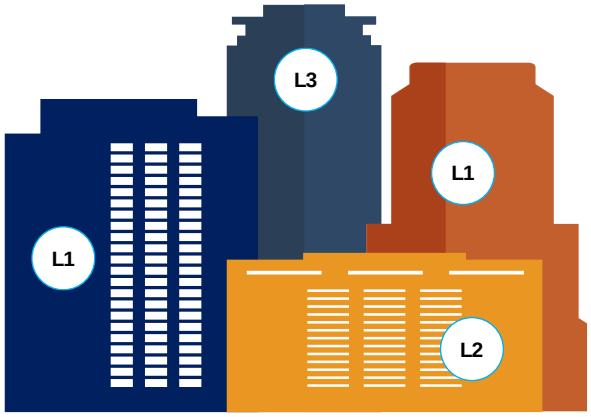
In a segmented approach, in addition to the factors considered in the monolithic approach, the organization reviews the criticality of their IT/OT environment and chooses the appropriate Implementation Level or Levels for different assets or parts of the environment. Using this approach, Implementation Levels can vary across the IT/OT environment based on the criticality of specific parts of the IT/OT environment. Criticality is determined using criteria that are appropriate to the organization's business, the threat environment, the IT/OT equipment's location in the network, and its exposure to threats.



Illustrated in the diagram on the right, the advantage of the segmented approach is that investment in security controls is made at an appropriate level without over or under investment.

This approach is, however, dependent on a good quality, fit for purpose asset criticality register. If there is an underinvestment in developing and maintaining the asset criticality register then a disadvantage of the segmented approach can be that the effectiveness of the investment in security controls is diminished.

Figure 2: Segmented implementation

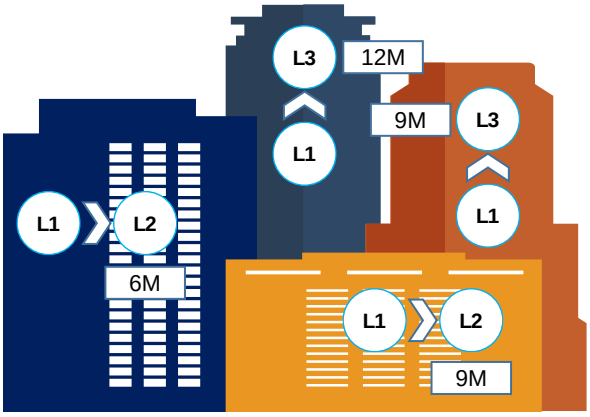


3.9 Phased Approach

A phased approach – illustrated on the right - combining both monolithic and segmented may also be used by an organization. This may be a pragmatic approach trading off the advantages and disadvantages of the two approaches.

For example a phased approach would start with monolithic application of the controls and progressively over time will move towards the segmented approach across different parts of the organization by timeframe set out in a company's security strategy.

Figure 3: Phased implementation



3.10 Determining Criticality

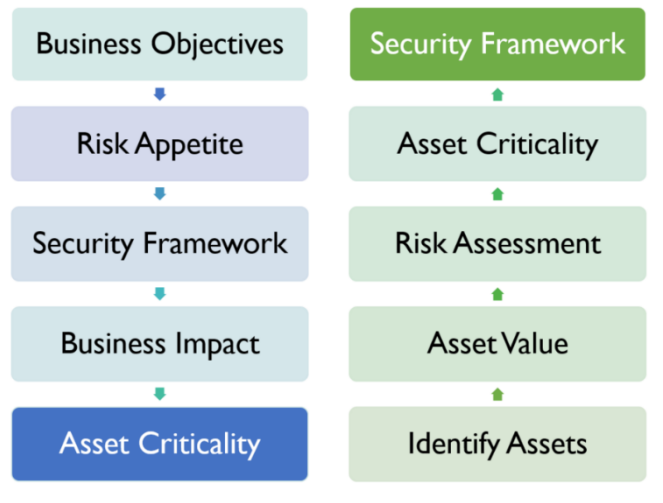
A key step in the segmented approach is to determine the criticality of the organization's IT/OT environments. Two approaches may be taken to determining the criticality: Top-down or Bottom-up.

The choice of which implementation approach to adopt will be based on organizations' needs. A Top Down approach might be more suitable for large critical infrastructure organization that has clear and specific business objectives, likely must adhere to defined industry regulatory requirements, has many assets, and can more readily draw on expertise. A Bottom Up approach might be more suitable for smaller organizations or those with less clear strategy, processes and expertise.

Top Down

This method is where classification and categorisation of critical business processes starts at the high level of the organization and work its way down to assets.

This approach ensures that asset categorisation aligns with organizational business objectives and risk management strategy.



Bottom Up

This approach is where classification begins with identification and then assessment of individual assets and builds up to the broader organizational context. This approach ensures that every asset is assessed before being categorised and classified and then integrated into a security framework.

4 METRICS & TRACKING IMPLEMENTATION

4.1 Measurement & Metrics

Taking a structured approach to measuring and monitoring controls will help organizations assess whether the controls are implemented correctly or not, whether they are performing as expected, and their impact on risk. When implementing CICSC, critical infrastructure organizations should carefully set quantitative metrics to help them track the performance of controls.

While a range of metrics are available, organizations should include Key Performance Indicators (which provide quantifiable measures of progress towards an defined goal) and Key Risk Indicators (which provide metrics to measure the likelihood and impact of an event) as part of their approach. This will help them define security goals, measure whether a control is implemented and running effectively, and recognise benefit realisation.

Further information on identifying measures and metrics and tracking security effectiveness can be found in a range of NIST publications, including NIST SP 800-55 Measurement Guide for Information Security Volume 1 and Volume 2.

4.2 Self-Assessment Tracking

To support the tracking of CICSC implementation, organizations adopting the controls should complete a self-assessment to record and evidence their progress on a regular basis. This will help organizations monitor their implementation and measure their baseline security and defensive posture.

A self-assessment tracker is provided to support this and ensure a consistent route for organizations to document their control implementation status. It aims to help track the number of controls implemented in each control family, their overall control status, and the validation of the implementation by an assessor or NCSC-JO. The tracker will provide system owners and security teams with complete picture of where they are on their journey to adopt relevant CICSC controls.

4.3 Control Compliance & Deviation

To be fully compliant with the controls, organizations would be expected to address each point within a control – not just some of them.

Deviations in relation to control implementation are permitted, however – for example because a control is not relevant to an operating environment or has been mitigated via other means. In such cases, any deviations should be documented in the self-assessment tracker.

Where operators of Critical Infrastructure opt to deviate from recommended best practice, for example in relation to control frequency, this is also permitted. Again, any such deviation should be documented in the self-assessment tracker with an explanation of why the approach adopted is appropriate.

المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

National Cyber Security Center
Amman - 7th Circle +(962) 6 900 500 +(962) 65 300 265 Info@ncsc.jo