



CYBER INCIDENT RESPONSE FRAMEWORK

DISCLAIMER

This document is the sole property of UAE Cyber Security Council and is approved by the UAE Cabinet.

The UAE Cyber Security Council reserves the right to amend, add, or delete any section of this Policy.

Neither the whole nor part of this document shall be reproduced without the prior written consent of the UAE Cyber Security Council.



VERSION CONTROL

Version 0.1

Date: 11 May 2022
Prepared by: CSC
Amendment Content: Initial Draft Document

Version 0.2

Date: 25 June 2022
Prepared by: CSC
Amendment Content: Updated based on initial feedback

Version 0.3

Date: 30 August 2022
Prepared by: CSC
Amendment Content: Updates as per review comments on the draft v0.2 of the document

Reviewed by

Approved by

Designation:	XXXXXXXXX	XXXXXXXXX
Name:	XXXXXXXXX	XXXXXXXXX
Signature:	XXXXXXXXX	XXXXXXXXX
Date:	XXXXXXXXX	XXXXXXXXX

Table of Contents


1. Introduction	05
1.1 Purpose	07
1.2 Scope & Applicability	08
1.3 Role of the Framework and the Plan	09
1.4 Guiding Principles	10
2. National Incident Response Governance Model	12
2.1 The Model	14
2.1.1 Cybersecurity Council (CSC)	15
2.1.2 National Cyber Response Group (NCRG)	16
2.1.3 Sector SOCs and CII operators	17
2.2 Integration with UAE National Crisis Management	18
3. Cyber Incident Alert Schema	19
4. Cyber Incident Management Lifecycle	22
4.1 Prepare	24
4.2 Protect	25
4.3 Detect	26
4.4 Respond	27
4.5 Recover	28
4.6 Learn and Improve	29



Table of Contents

5. Reporting Requirements and Information Sharing (Federation)	30
5.1 Technical Reporting (Federation)	32
5.2 Operational Crisis Management	33
5.3 International Information Sharing	34
6. Monitoring and Performance Management	35
7. Implementation	37
8. Appendices	39
8.1 Reporting and Information Sharing – Federation, Requirements and Point of Contact Network	40
8.1.1 Technical Reporting (Federation)	41
8.1.2 Operational Crisis Management	43
8.2 Activation Crosswalk (Dependencies overview)	
8.2.1 Steady-State – Level 4 Status	45
8.2.2 Significant Cyber Incident – Level 3 Incident declared	46
8.2.3 Significant Cyber Incident – Level 2 Incident declared	47
8.2.4 Significant Cyber Incident – Level 1 Incident declared	48
8.3 Acronyms	49





SECTION 1
INTRODUCTION

INTRODUCTION

Cyberspace supports diverse activities in the United Arab Emirates, including the national economy, national security, public health and safety, cultural and social life. The evolving information and communications technology of cyberspace provides numerous benefits but is increasingly a target of cyber threats that have the power to disrupt, damage, or destroy critical functions and services that enable our way of life. Because cyber threats are dynamic, incidents will inevitably occur. However, an effective incident response capability can help minimize the impact of these incidents and reduce the occurrence of other incidents.

The Cyber Incident Response Framework (CIRF) was established and revised in light of the National Cyber Security Strategy, defining how the UAE will prepare for, protect against, detect, respond to, recover from, and continuously learn from cyber incidents. At the heart of the CIRF are guiding principles, the national cyber response governance model, the incident level schema and management lifecycle, the reporting and information sharing requirements, as well as the monitoring and performance management components that together make up the cyber incident management capability. It is supported by the Cyber Incident Response Plan (CIRP) which further defines the cyber response capability by providing operational details.

The Council has developed this framework to establish a national incident management capability and defining how the UAE will prepare for, protect against, detect, respond to, recover from, and continuously learn from significant cyber incidents; aligned with the UAE's national priority to be a global leader in cyber security, and enhance the security posture of organizations and individuals within the UAE.

1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices

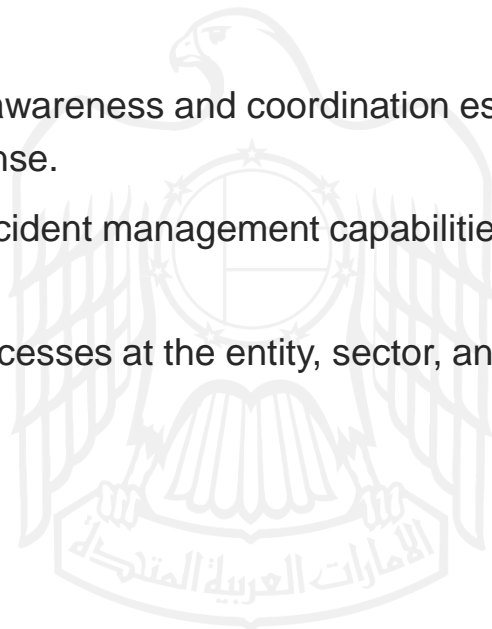


1.1 Purpose

The CIRF establishes the capability that enables the UAE, its government and CII sector entities to respond to significant cyber incidents in a coordinated manner, limiting their scope and impact, thus ensuring the stability of the UAE cyberspace and contributing to the security, well-being and global competitiveness of the nation.

The CIRF therefore:

- Institutionalizes and enforces cyber capabilities and establishes a cyber incident response community to manage significant cyber incidents and raising the readiness of entities to respond to cyber-attacks.
- Unifies the concept of managing cyber incident response between relevant entities at the federal level in the UAE and increases awareness by conducting exercises between entities to respond to cyber-attacks in coordination with the relevant stakeholders.
- Integrates this capability in the relevant UAE national security and national crisis management institutional context in coordination with the relevant stakeholders.
- Defines the cyber situational awareness and coordination essential for effective cyber incident response.
- Raises awareness of cyber incident management capabilities and processes; and
- Informs incident response processes at the entity, sector, and federal levels.



1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



1.2 Scope & Applicability

The CIRF and the CIRP are applicable to all government and private sector entities identified under the Critical Information Infrastructure Protection (CIIP) Policy of the United Arab Emirates. This overarching scope and applicability are necessitated by the nature of significant cyber incidents that, by definition, effect entity-level incident management capabilities and frequently span through multiple entities, sectors and jurisdictions.





1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



1.3 Role of the Framework and the Plan

The Cyber Incident Response Framework establishes the institutional framework and key processes constituting the UAE's incident response capability. This institutional setting shall infrequently change to provide stability enabling key stakeholders to effectively fulfil their roles as part of the cyber incident response capability.

The role of the Cyber Incident Response Plan is to add an operational context and interpretation to the general framework. The CIRP also plays a vital role in providing flexibility to the UAE's cyber incident response capability. Accordingly, the Cyber Incident Response Plan done by the Cyber Security Council should be reviewed and adjusted more frequently (2-3 years), ensuring it reflects significant changes in the global technology and threat environments.

The CIRF and the CIRP must be reviewed regularly to make sure they remain relevant and reflect global and UAE realities. Input from relevant stakeholders shall be collected during such reviews to further refine capabilities, share experiences and ensure buy-in of key organizations.

1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



1.4 Guiding Principles

The CIRF is predicated on internationally acknowledged guiding principles – high-level governing approaches – that describe the broad context in which response to significant cyber incidents takes place.

These principles are outlined to establish a shared approach amongst relevant stakeholders within the UAE cyber incident response community.

Situational Awareness Enabled by Information Sharing

- Achieving cyber situational awareness on an entity-level is enabled by continuous monitoring of information assets and maintaining visibility into threats, vulnerabilities and current cyber incidents. Developing cyber situational awareness on a sector and federal-level is established via structured information sharing aiming to support the formation of near real-time understanding and knowledge of the UAE cyberspace environment enabling stakeholders to warn of imminent or ongoing incidents and initiate incident response activities.
- Information sharing is thus essential to building cyber situational awareness and enables the exchange of data, insights and knowledge on threats, vulnerabilities, risks, mitigation strategies and best practices. This information, put together, serves as the bedrock of national cyber incident management, including incident response during a significant cyber incident.

Risk-Based Approach

- A risk-based approach as a guiding principle aims to connect risk levels (or incident severity levels) to appropriate responses, including mobilized resources, as a standard way of establishing a balanced, calculated relationship between incident severity and national resources. A risk-based approach is enabled in part by the progressive measurement of cyber incidents through the incident severity schema with the main goal of allocating adequate resources to corresponding incident levels to make sure that they are both resolved (required resource levels are mobilized) and resources are assigned in an efficient way (only necessary resources are mobilized).

1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



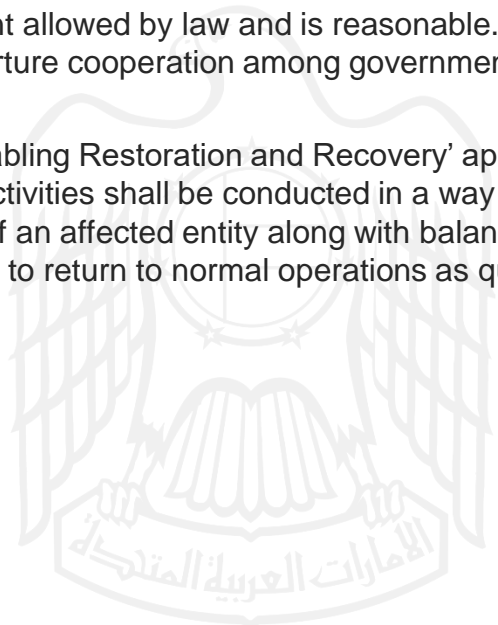
1.4 Guiding Principles

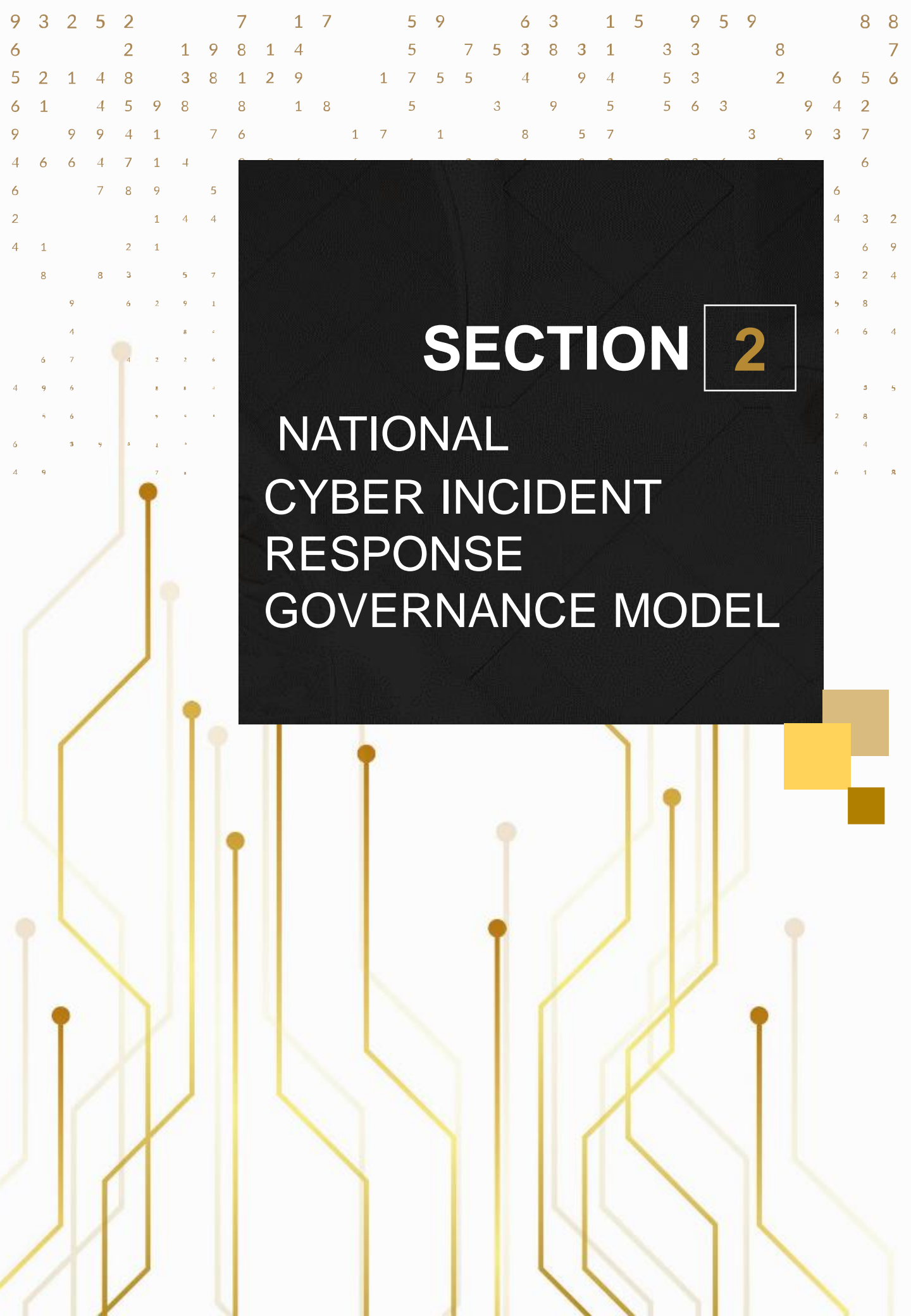
Shared Responsibility ('Unity of Effort')

- Stakeholders at the entity, sector, and national levels need to work together on a 'Unity of Effort' basis to be effective in maintaining the stability of UAE cyberspace and responding to significant cyber incidents. Entity (including critical infrastructure operators), sector (including sector regulators) and national (government ministries, agencies) level stakeholders are collectively responsible for collaborating through a framework led by CSC, the nationally mandated lead agency tasked to orchestrate cyber incident management on a UAE-level. Collaboration must be multi-directional to enable effective information sharing and surge response during crisis situations.
- In addition, a 'Whole of Government Approach' emphasizes the importance of cooperation between different government levels and entities – especially the national-federal and emirate levels – to deliver an effective incident response effort. This principle is highly relevant as modern governments are multi-layered and have a broad array of responsibilities, roles and priorities. Bureaucratic hurdles, unclear chains-of-command and, lack of clear ownership can cause serious damage during a severe real-life incident, but the principle is also important to prevent gaps and avoid duplications during a complex response effort.

Respecting Affected Entities

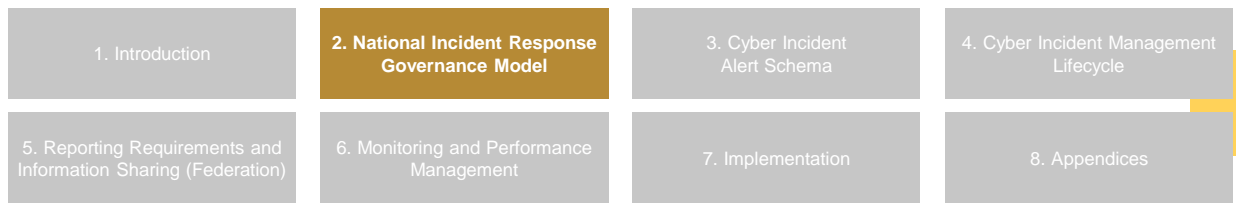
- This principle serves to reassure members of the UAE cyber ecosystem and other key stakeholders and community partners that their interests will also be considered during incident response to the extent allowed by law and is reasonable. Such principles or commitments aim to nurture cooperation among government and private sector entities.
- Complementing the above is an 'Enabling Restoration and Recovery' approach highlighting that incident response activities shall be conducted in a way that prioritizes restoration and recovery of an affected entity along with balancing governmental priorities and the need to return to normal operations as quickly as possible.





SECTION 2

NATIONAL CYBER INCIDENT RESPONSE GOVERNANCE MODEL



The ability of the UAE to successfully respond to significant cyber incidents is dependent on centralized coordination and decentralized execution following a ‘whole-of-nation’ approach. To form such a coordinating capability, two national/federal-level governing bodies were established: the tactical National (Cyber) Security Operations Center (NSOC) and the strategic National Cyber Response Group (NCRG), with the coordination of CSC as the national lead agency for cyber incident management. The strategic function of these institutions is to enable the coordination of UAE cyber incident management.

1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



2.1 The Model

The above listed entities and bodies have a common interest in effective cyber incident response. Accordingly, stakeholders shall work toward a common purpose in a collaborative way to develop collective incident response solutions to complex cybersecurity problems. Individual stakeholders are to perform the roles and responsibilities outlined in the National Cybersecurity Governance Framework to collectively mitigate the impacts of significant cyber incidents on the national security of the UAE and the stability of its cyber ecosystem.

Specifically, the UAE Cyber Incident Governance Model and its constituent stakeholders are to:

- Develop and maintain cyber situational awareness of the state of the UAE cyberspace to proactively identify and analyze incidents;
- Make timely decisions to mitigate the impacts of significant cyber incidents and to restore 'steady-state' operations rapidly; and
- Foster timely collaboration, information sharing, and continuous learning and improvement.



1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices

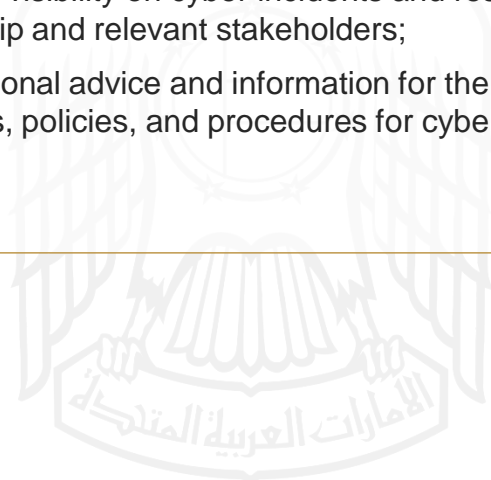


2.1 The Model

The entities, bodies and their responsibilities are enlisted below:

2.1.1 Cybersecurity Council (CSC)

- The Cybersecurity Council (CSC) of the United Arab Emirates is mandated as the Lead National Agency to defend and secure the UAE's cyberspace. Accordingly, the CSC is responsible for coordinating the response to significant cyber incidents. It is to fulfil its mandate on a tactical level through the NSOC, providing cyber situational awareness and surge capabilities to the national cyber incident response community and on a strategic level through acting as the coordinator of the NCRG as required.
- The National Security Operations Center, operating under the oversight of CSC, serves as the primary tactical incident response organization of the UAE and is tasked with the following responsibilities:
 - 2.1.1.1 Oversee response activities during 'Steady-state' and owns the decision to escalate incident levels from 'level 4' to 'level 3' and advises the CSC chair to escalate an incident to 'NCRG';
 - 2.1.1.2 Manage tactical response to incidents;
 - 2.1.1.3 Develop and maintain a common operational picture in its capacity as the national point of integration (federation) for all cyber information provided by government, critical infrastructure operators, and other relevant stakeholders related to threats, vulnerabilities, incidents and mitigation or response activities; providing visibility on cyber incidents and response activities to national leadership and relevant stakeholders;
 - 2.1.1.4 Provide technical and operational advice and information for the NCRG to synchronize cyber operations, policies, and procedures for cyber incident response.



1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



2.1 The Model

2.1.2 National Cyber Response Group (NCRG)

- The National Cyber Response Group (NCRG) is a strategic coordinating and decision-making body convened and chaired by CSC. The NCRG is convened following the advice of NSOC and upon the decision of the CSC chair.
- Its members include the relevant government stakeholders along with the relevant sector SOCs and CII operators.

1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



2.1 The Model

2.1.3 Sector SOCs and CII operators

Sector SOCs (national level) and CII operators (including relevant private sector entities) are fundamental components of the UAE cyber ecosystem and are also likely targets of cyberattacks. These stakeholders have a correspondingly important role to play in national cyber response efforts. Accordingly, they are:

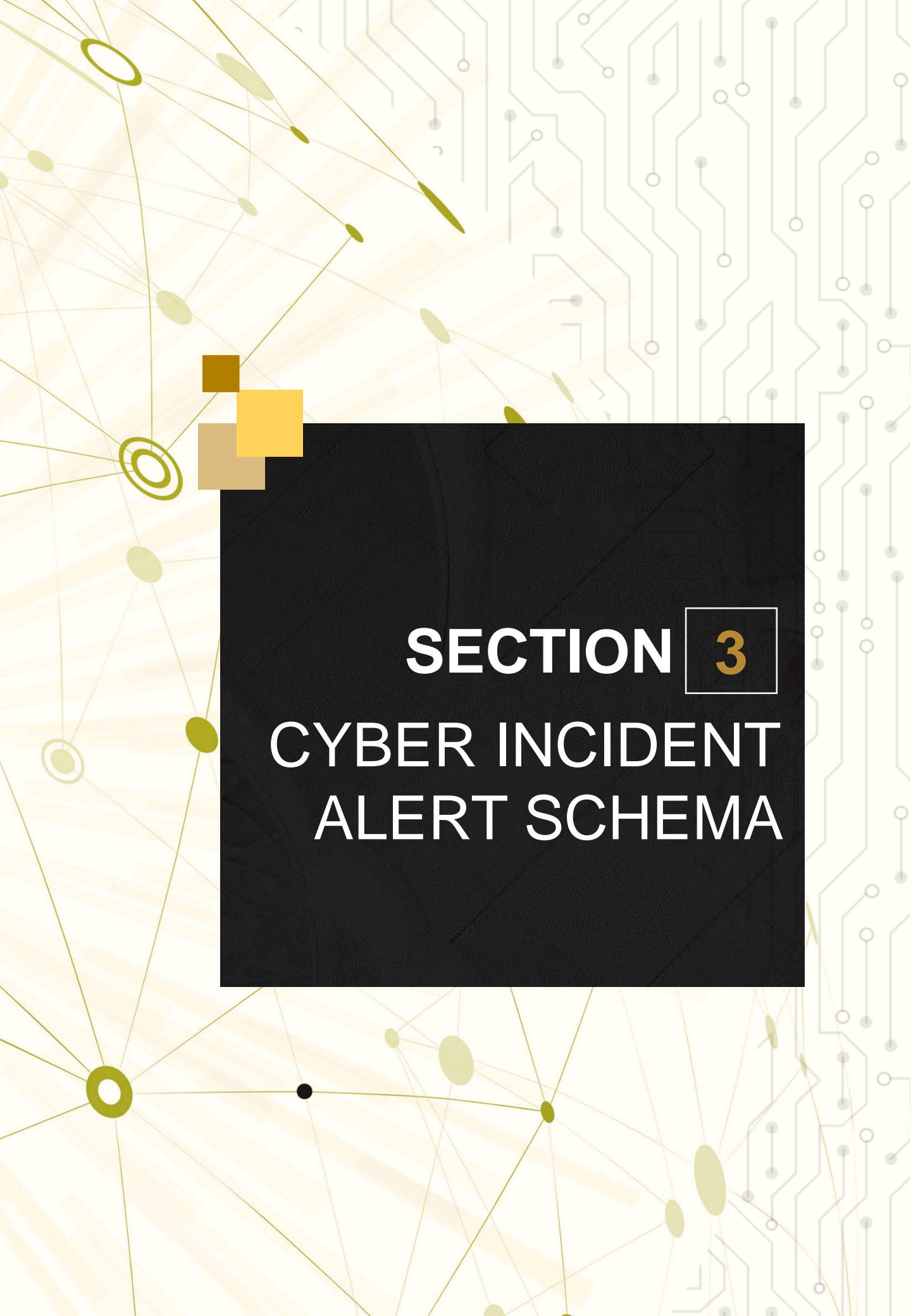
- 2.1.3.1 Responsible for the management and thus sole owners of 'low-level' incidents ('Normal status') following standard industry best practices, including the maintenance of adequate internal capabilities for incident management;
- 2.1.3.2 Required to fulfil their mandatory and voluntary incident reporting requirements, also to contribute to the maintenance of a common operational picture by NSOC; and
- 2.1.3.3 Tasked with the development and implementation of CII Sector-Specific Cyber Response Plans.

1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices

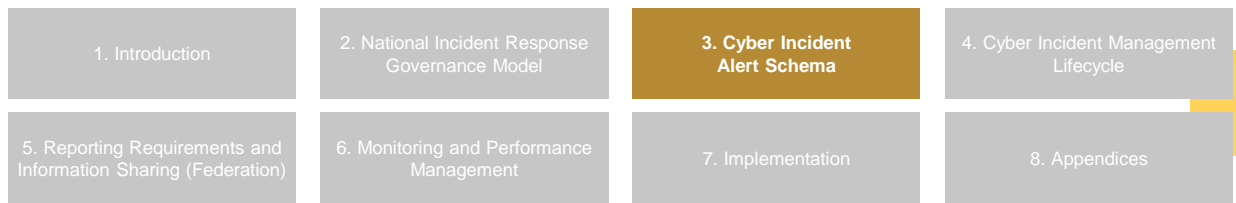


2.2 Integration with UAE National Crisis Management

Recognizing that cyber incidents can result in potential or actual physical consequences, CSC will share information on significant incidents with the National Emergency Crisis and Disaster Management Authority (NCEMA) and other relevant authorities and support NCEMA in fulfilling its physical emergency management responsibilities as appropriate. Similarly, physical emergencies and disasters can have significant cybersecurity-related consequences. Accordingly, NCEMA will support CSC in fulfilling its cyber incident management responsibilities. CSC and NCEMA shall also collaborate during ‘steady-state’ to harmonize planning efforts.

The background features a complex network of thin, light-colored lines connecting various nodes. Some nodes are represented by small circles, while others are larger, irregular shapes. The overall color palette is dominated by light beige and cream tones, with accents of olive green and gold. On the right side, there are vertical lines resembling a circuit board or data stream. A large, solid black rectangle is positioned in the lower-middle section, containing the title text.

SECTION 3
**CYBER INCIDENT
ALERT SCHEMA**



The Cyber Incident Alert Schema operates as a national-level alert and warning mechanism. This mechanism conveys information on current cyber incidents and their level of impact to Critical Information Infrastructure (CII) sectors, entities and government organizations of the United Arab Emirates.

The Schema is to convey information in a condensed form to key stakeholders through four alert levels (level 4, level 3, level 2 and ;level 1). The alert level will consider the actual cyber activity and its potential to escalate, its impact to CII sectors of the UAE and its effect on response capabilities. All-in-all alert levels are designed to contribute to overall cyber situational awareness providing an indication of the cyber incident status and impact in the UAE.

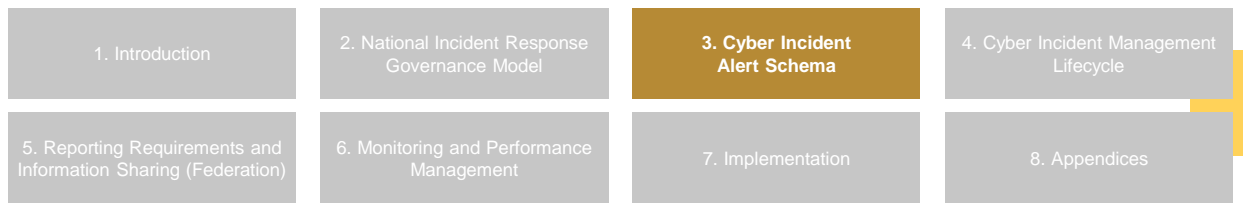
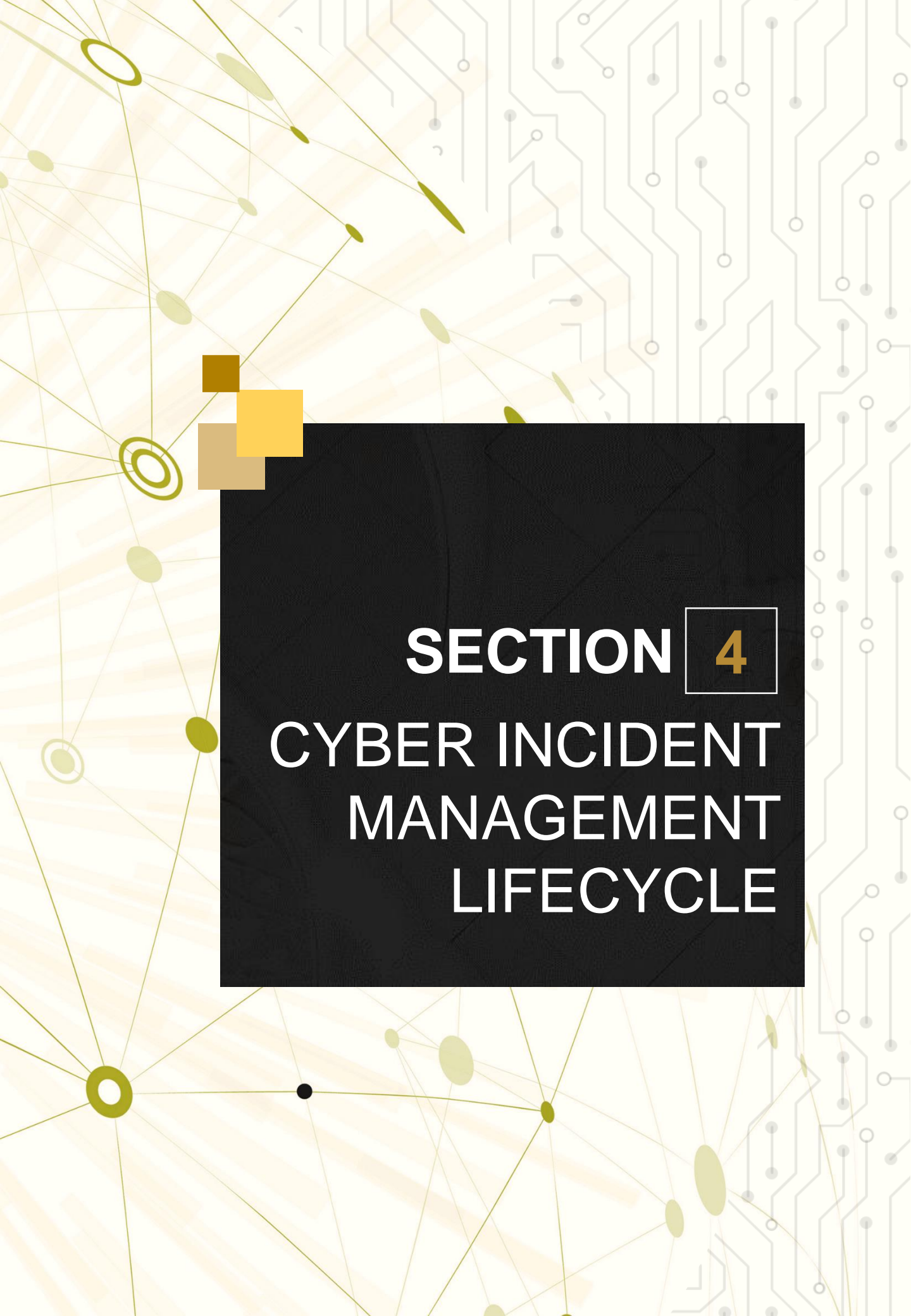


Table 1: National Cyber Incident Alert Levels

	Alert level	Activity	Impact
Significant Cyber Incident	Level 1 Highest-level impact	<ul style="list-style-type: none"> Threat of, or actual, malicious cyber activity that will disrupt, destroy, or degrade CII and/or government systems exists. Incident occurred, is imminent, or is ongoing. 	<ul style="list-style-type: none"> Potential or observed total or near-total destruction, degradation, or compromise of CII across one or more sectors. Potential or observed serious and widespread degradation or destruction, threatening continued operation of government or CII sector. Normal business operations and functions may be indefinitely suspended. Potential impact is managed by the NCEMA.
	Level 2 High-level impact	<ul style="list-style-type: none"> Threat of, or actual, increased malicious cyber activity directed at national critical services exists. Known or expected targeted intrusion or exploit of a CII providing a national critical service is present. 	<ul style="list-style-type: none"> Potential for or observed major degradation, disruption and/or destruction of or damage to CII across one or more sectors. Potential impact is managed by the NCEMA.
	Level 3 Medium-level impact	<ul style="list-style-type: none"> Threat of, or actual, elevated malicious cyber activity exists. Known or expected intrusion or focused attack is present. 	<ul style="list-style-type: none"> Potential for or observed compromise and/or degraded service in one or more CII sectors. Potential for or observed elevated level of degradation, disruption or damage. Potential impact is managed by the NSOC and NCRG when needed.
Steady-state	Level 4 Low-level impact	<ul style="list-style-type: none"> Threat of, or actual, malicious cyber activity presents only a general concern. 	<ul style="list-style-type: none"> CII sectors or government systems are not targeted or affected. Potential impact is manageable by the responsible owner/operator.

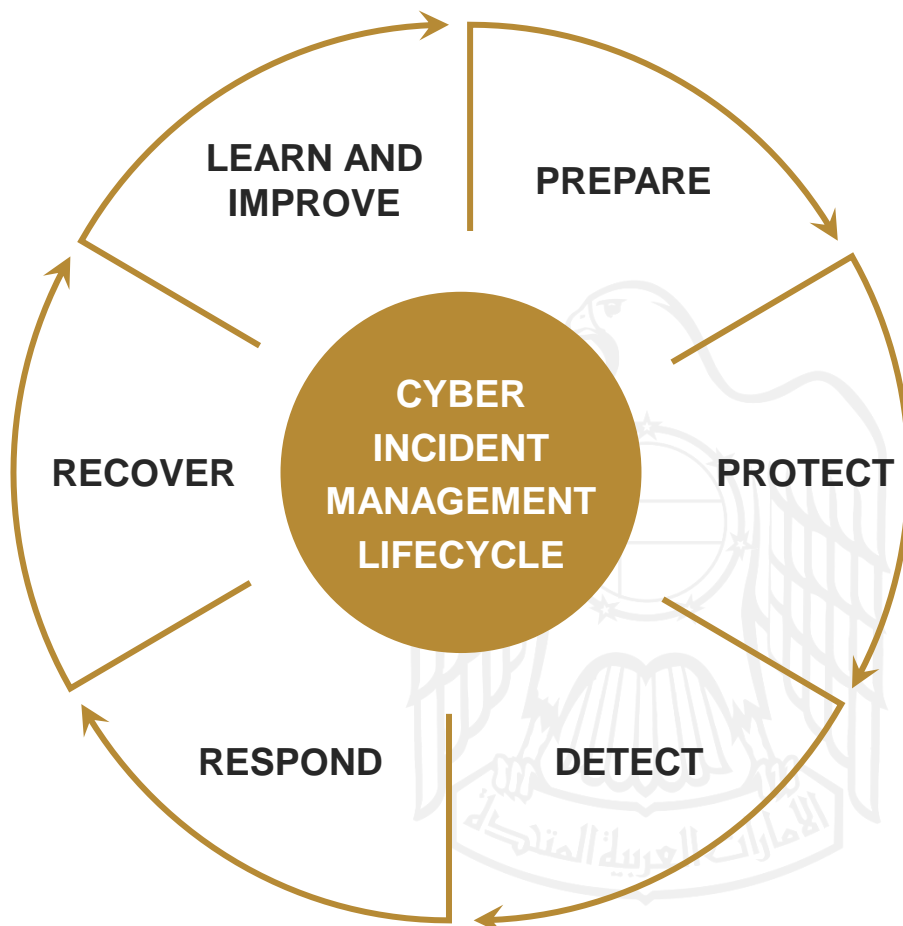
The background features a complex network of thin, light-colored lines connecting various nodes. Some nodes are represented by small circles, while others are larger, irregular shapes. The overall color palette is dominated by light beige and cream tones, with accents of olive green and gold. On the right side, there are vertical lines resembling a circuit board or data stream. A large, solid black rectangular box is positioned in the lower-middle section of the page, containing the main title text.

SECTION 4
**CYBER INCIDENT
MANAGEMENT
LIFECYCLE**

1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



The following section is to guide activities and assist CII entities, sector regulators, SOCs and national partners in establishing a common understanding of activities to be undertaken as part of the cyber incident management lifecycle. Each organization should consider their own activities in the context of its specific operating environment, ICT architecture and overall risk profile and maintain correspondingly tailored incident response capabilities in line with the SOC Baseline Framework. CSC will work with sector regulators and SOCs to ensure that sector- and federal-level cyber incident management plans are aligned. The Cyber Incident Management Lifecycle outlined below aims to establish a common approach and general alignment of incident response capabilities of relevant stakeholders within the UAE cyber ecosystem.





1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



4.1 Prepare

The Prepare Phase includes capabilities and activities (i.e. people, processes and technology) that position stakeholders to be able to respond to a cyber incident. Preparedness activities, including establishing and maintaining cyber situational awareness, are shared responsibilities across stakeholders at the entity, sector, and national levels. When coordinated response actions are needed during a Significant Cyber Incident, The Cyber incident response community must be trained in advance regularly to effectively manage cyber incidents and to ensure that most of incidents have been identified as potential incidents and responses practiced in advance. Conducting various incident response exercises are another good way to prepare an organization for a real incident.





1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



4.2 Protect

Incidents that never occur are easiest to handle. Protecting CII from incidents is therefore an essential element of an effective incident management capability. The Protect Phase includes preventative measures and strategies alongside analysis to predict when or if an incident might take place and designing and executing corresponding actions to protect systems from a potential incident.





1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



4.3 Detect

The Detect Phase includes identification of an event of interest, validation that the event of interest is an incident, and analysis of the extent of the compromise and escalation (if necessary). CII entities in this phase play an especially important role as they will often be the first to detect significant incidents on their respective networks, have credible intelligence or information pertaining to a potential activity or incident or be aware of vulnerabilities. Sector SOCs may also play a similarly important role. During this phase, affected stakeholders may also take steps to organize an initial response.





1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



4.4 Respond

During the Respond Phase investigative steps are taken to collect and analyze evidence associated with the incident to determine the extent of the compromise, root cause, impact, and other information needed to facilitate response actions. Mitigating measures are implemented to contain an incident aiming to decrease or eliminate the impact, longevity of, or damage caused by an incident. It should be noted that most cyber incidents are violations of UAE Cyber Crime Laws and the proper collection and handling of digital evidence can help support law enforcement and subsequent prosecution.





1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



4.5 Recover

The Recover Phase begins immediately after an incident is detected and may overlap with response efforts. Recovery aims to repair, remediate, and restore services and operations. It may include communicating with other stakeholders regarding recovery actions and the status of critical services. Ultimately during the Recover Phase, entity, sector, and national operations move from Significant Cyber Incident back to Steady-state.





1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



4.6 Learn and Improve

Continuous improvement occurs throughout the cyber incident management lifecycle and should focus on implementing proven processes and activities. In addition, following an incident, stakeholders should work to minimize the potential for future attacks through forensic investigation, hardening of infrastructure and outreach to raise awareness about risks and potential mitigating measures. Through the implementation of lessons learned at the entity, sector and national levels; an effective cyber incident management capability can be maintained and its maturity further enhanced over time.





SECTION **5**

REPORTING REQUIREMENTS AND INFORMATION SHARING (FEDERATION)





1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



Reporting and information sharing (federation) is a critical component of the Cyber Response Framework. The reporting process can include voluntary and mandatory elements while information sharing can be manual, person-to-person or automated (including machine-readable formats). All key stakeholders of the incident management system have an important role to play both to maintain an up-to-date common operational picture during a significant cyber incident. Cooperation focused on resolving crises occurring in highly complex technological environments can only take place if well-defined and well-established channels, process of reporting and information sharing are established in advance. It is paramount that all stakeholders are clearly aware of their responsibilities.

Accordingly, a relevant Point of Contact network is to be created and maintained under the oversight of CSC. This network is to focus on cyber incident-related reporting and information sharing (incl. technical) following a clearly defined process and firmly established requirements. Its membership shall consist of NSOC, aeCERT and sector SOCs and CII operators. A complementary network shall connect the broader cyber incident management community led by CSC (relevant authorities).





1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



5.1 Technical Reporting (Federation)

Reporting and sharing technical cyber incident-related data occurs through federation of SOCs as defined by the SOC Baseline framework. This channel follows a hierarchic model in which aggregation of relevant information (including threat intelligence, vulnerability management, incident indicators, etc.) is collected from CII entities to sector SOCs, from sector SOCs to the NSOC. Exact roles, responsibilities, and reporting requirements (including reporting timelines) are defined by the SOC Baseline Framework (see Appendix). This channel is owned and maintained by the CSC as National Lead Agency. CSC is also to establish and implement relevant information sharing framework with relevant stakeholders enabling both to fulfil their respective mandates.

An ‘activation crosswalk’-type of framework defining steps is to be taken (e.g. reporting requirements), limitations and dependencies for key actors during incident response are detailed in the Appendix.





1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



5.2 Operational Crisis Management

A distinct Point-of-Contact Network is to be maintained for the purposes of operational crisis management primarily to be leveraged during Significant Cyber Incidents when the cooperation of key stakeholders is critically important to enable effective crisis response – both from the cybersecurity community and the wider security and policy stakeholders of the UAE. This channel aims to enable response by connecting relevant ministries, law enforcement and disaster management and other relevant organizations as well as affected CII entities of the UAE. This channel is also owned and maintained by the CSC as National Lead Agency. Further details about the Point of Contact Network are provided in the Appendix.






1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



5.3 International Information Sharing¹

Regarding the response to significant cyber incidents, CSC is to maintain supporting policies and procedures outlining guidelines for engaging with international partners on cyber incident management and dissemination of cyber incident information, including type of data and mechanism of information sharing. The policy framework shall be aligned with the general Information Sharing Framework of CSC. Those policies are to govern issues related to initiating international outreach (incl. information sharing) by sector SOCs or CII operators; necessary approval of such cooperation from the NSOC, the Cyber Security Council, or the Ministry of Foreign Affairs and International Cooperation. Any conditionality, including data minimization; guidance on potential legal or classification obstacles and other critical issues. On an operational level, policies should clearly define documentation requirements (key roles, contact, scope, data sharing, etc) and a relevant POC system.



The background features a complex network of thin, light-colored lines connecting various nodes. Some nodes are represented by small circles, while others are larger, irregular shapes. The overall color palette is dominated by light beige and cream tones, with accents of olive green and gold. On the right side, there are vertical, circuit-like patterns consisting of small circles and lines, resembling a printed circuit board (PCB) layout. A large, solid black rectangular box is positioned in the lower-middle section of the page, containing the section title in white and gold text.

SECTION 6
**MONITORING AND
PERFORMANCE
MANAGEMENT**

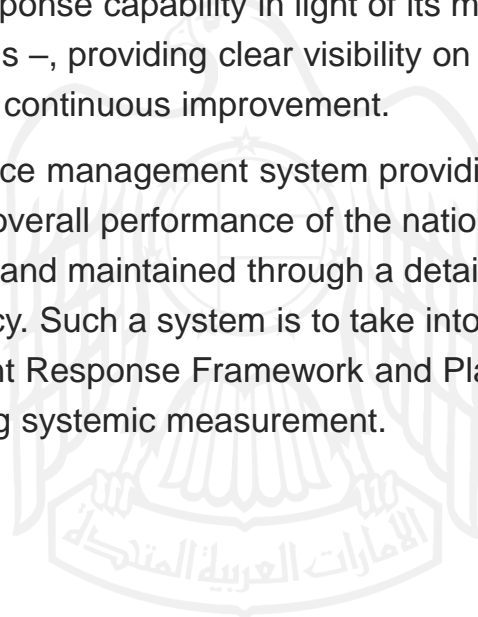
1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



Monitoring a cyber incident management system on a national level is a critically important, but highly complex task. Developing and enhancing such a monitoring component as part of the UAE incident management capability is necessary to make the Cyber Incident Response Framework and Plan measurable. Being able to measure incident response, in turn, is essential to create visibility and serves as the foundation for continuous improvement. Such a monitoring function shall have multiple components, including those providing asset visibility and key metrics for incidents covering the entirety of the cyber incident lifecycle. Such a monitoring capability shall be maintained by CSC and its details to be defined in the Cyber Incident Response Plan.

Performance management is another key element of the national cyber incident management system. On a fundamental level, it leverages data provided by the above monitoring function and compares that to pre-set Key Performance Indicators providing an objective basis for evaluating the performance of the national cyber incident management capability. Accordingly, data gathered as part of monitoring shall be clearly aligned with the KPIs defined by performance management. Ideally, such metrics can be connected to relevant risk assessments to aid governance. Ultimately the performance management system maintained by CSC shall provide a clear picture of the availability and efficiency of the national incident response capability in light of its main goals – operationalized through relevant KPIs –, providing clear visibility on implementation and a solid basis for continuous improvement.

A detailed monitoring and performance management system providing visibility and relevant metrics describing the overall performance of the national incident response capability shall be defined and maintained through a detailed SOP by the CSC as the Lead National Agency. Such a system is to take into consideration both the Cyber Incident Response Framework and Plan and provide detailed parameters enabling systemic measurement.





SECTION 7
IMPLEMENTATION




1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



Implementation and operationalization of the CIRF will be led by CSC as the Lead National Agency in consultation with key stakeholders of the UAE cyber ecosystem. This process at the entity, sector, and national levels will take time as processes and procedures will continue to evolve as capabilities mature and threat environments continue to change. Supporting procedures and enabling capabilities, tools, and systems will need to be developed, maintained, and updated. CSC will work with stakeholders across the cyber incident response community to implement the CIRF to establish a full operating capability and then continue to raise its maturity.



The background features a complex network of thin, light-colored lines connecting various nodes. Some nodes are represented by small circles, while others are larger, elongated ovals. The color palette is primarily light beige and cream, with accents of olive green and gold. On the right side, there are vertical lines resembling a circuit board or data stream, with small circles at various intervals. A large, solid black rectangle is positioned in the lower-middle section of the page, containing the text.

SECTION 8
APPENDICES



1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



8.1 Reporting and Information Sharing – Federation, Requirements and Point of Contact Network

Reporting and information sharing are defined as critical components of any national cyber incident response capability. The role of key stakeholders, channels for sharing technical and operational information as well as relevant processes must be firmly pre-defined and understood to make sure the cyber incident response capability can perform effectively in a crisis situation. There are two, distinct channels for reporting and information sharing with different functions and profiles.



1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



8.1 Reporting and Information Sharing – Federation, Requirements and Point of Contact Network

8.1.1 Technical Reporting (Federation)

Reporting and sharing technical cyber incident-related data occurs through federation of SOCs as defined in detail by the SOC Baseline framework. This channel follows a hierarchic model through which the aggregation of relevant information (including threat intelligence, vulnerability management, incident indicators, etc.) is collected from CII entities to sector SOCs and from sector SOCs to the NSOC.

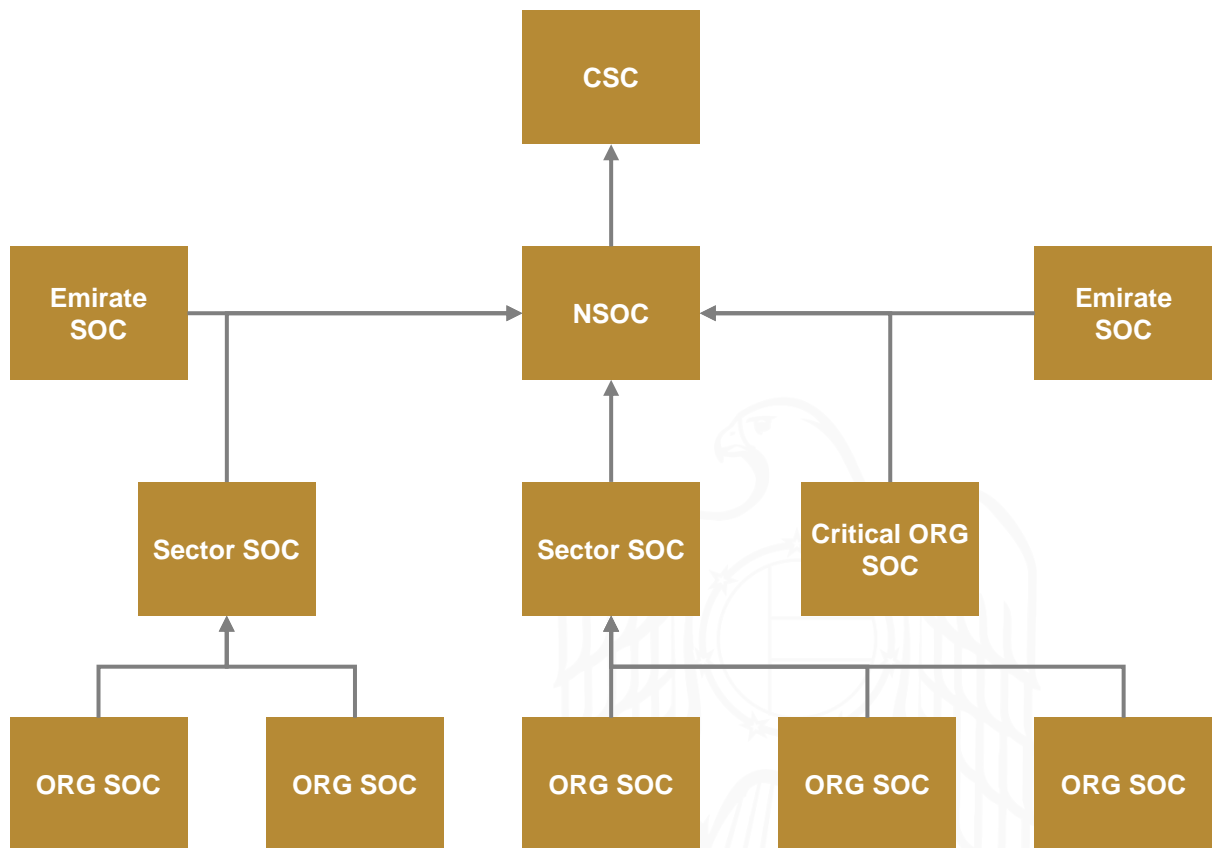


Illustration 1-A: Federation (SOC Baseline)

1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



8.1 Reporting and Information Sharing – Federation, Requirements and Point of Contact Network

8.1.1 Technical Reporting (Federation)

All incident notification must contain industry standard information on:

- Local Priority
- Assigned Category Level
- Title
- Description
- Current Status
- Artefacts

Notifications must be communicated as the investigation unfolds and updates provided at an appropriate frequency. Expected notification times are from the moment the incident is declared as follows:

CII entities notification requirement

Category	Mean-Time-To-Notify (MTTN)
Level 4 Incident	1440 min
Level 3 Incident	60 min

Expected update times for CII entities are defined as follows

Category	Mean-Time-To-Notify (MTTN)
Level 4 Incident (Green)	1440 min
Level 3 Incident (Yellow)	120 min
Level 2 Incident declared (Orange)	60 min
Level 1 Incident declared (Red)	Near-Real Time

Sector SOCs and the NSOC shall define specific rules for federation in a SOP. Besides, to enhance detection capabilities of the NSOC, an SOP is to be developed to define specific requirements for CII entities determining the scope of incident indicators and other related information to be shared (e.g. perimeter firewall, internet facing proxies, Domain Name Resolution, etc). The SOP, developed by NSOC, is to be aligned with the requirements of the SOC Baseline. This channel is owned and maintained by the CSC (via NSOC) as National Lead Agency.

1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



8.1 Reporting and Information Sharing – Federation, Requirements and Point of Contact Network

8.1.2 Operational Crisis Management

A distinct Point-of-Contact Network is to be maintained for the purposes of operational crisis management primarily to be leveraged during Significant Cyber Incidents when the cooperation of key stakeholders is critically important to enable effective crisis response. The rationale for maintaining this distinct network is to connect the cybersecurity community and the wider security and policy stakeholders of the UAE mandated to manage physical (real world) security emergencies.

The liaison network to be set up and maintained by NSOC on behalf of CSC comprising of point persons appointed at relevant government entities.





1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



8.1 Reporting and Information Sharing – Federation, Requirements and Point of Contact Network

8.1.2 Operational Crisis Management

The aim of the liaison network is to enable the coordinated mobilization of relevant national resources based on ‘unity of effort’ and ‘whole of government’ approaches vis-à-vis cyber incident management on a federal level including preparedness, facilitating collaboration and enabling crisis response, including training, exercises and lessons learned activities.

A necessary Standard Operating Procedure, including a communication protocol is to be developed by NSOC under the guidance of CSC.

To develop a mature national cyber crisis management capability, regular exercises are to be prepared and organized by the NSOC under the umbrella of the CSC. Testing, gap and maturity assessments are to be carried out and identified gaps are to be remediated. Exercises are to be held at least annually in coordination with key stakeholders.





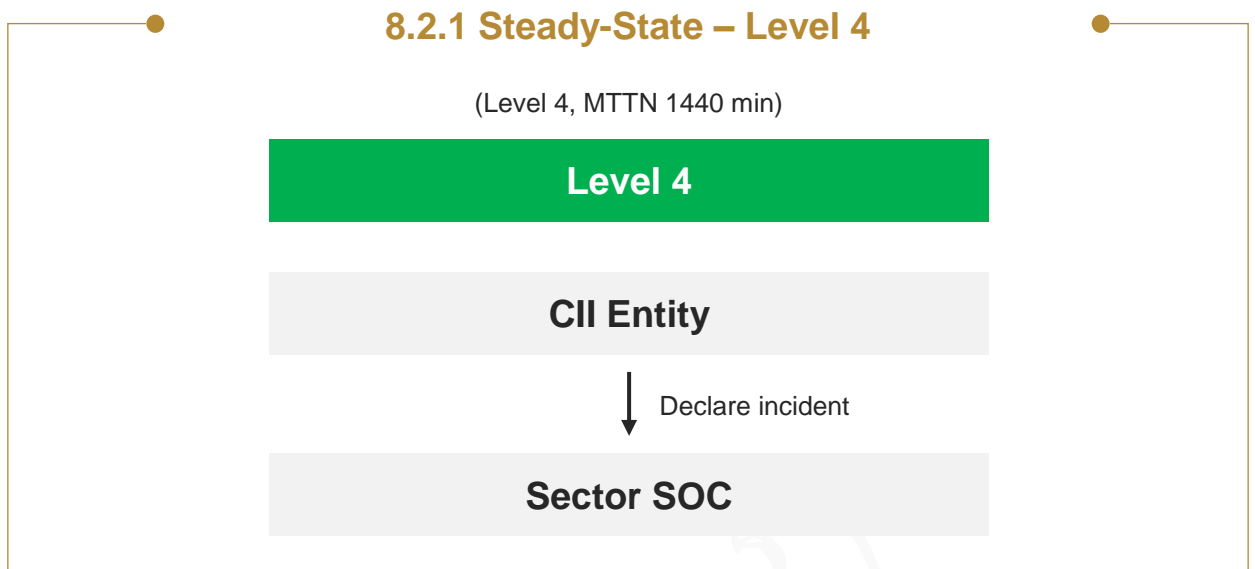
1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



8.2 Activation Crosswalk (Dependencies overview)

The below graphic serves as additional guidance aiding understanding the federation process (reporting and escalation) as well as the maintenance of the common operational picture of the UAE by the relevant actors of its cyberspace with the leadership of NSOC.

Arrows indicate direction of escalation by actors.





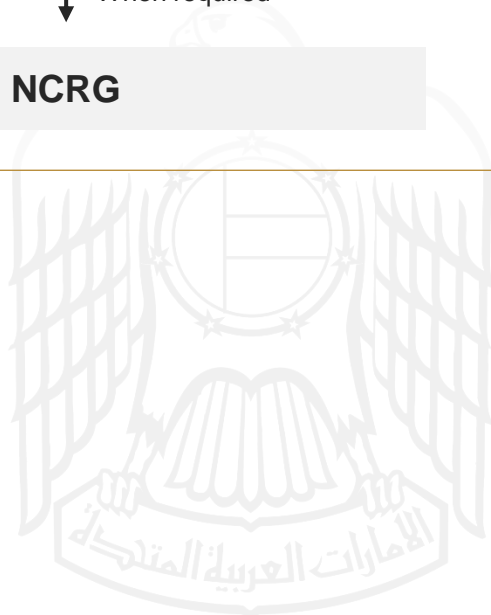
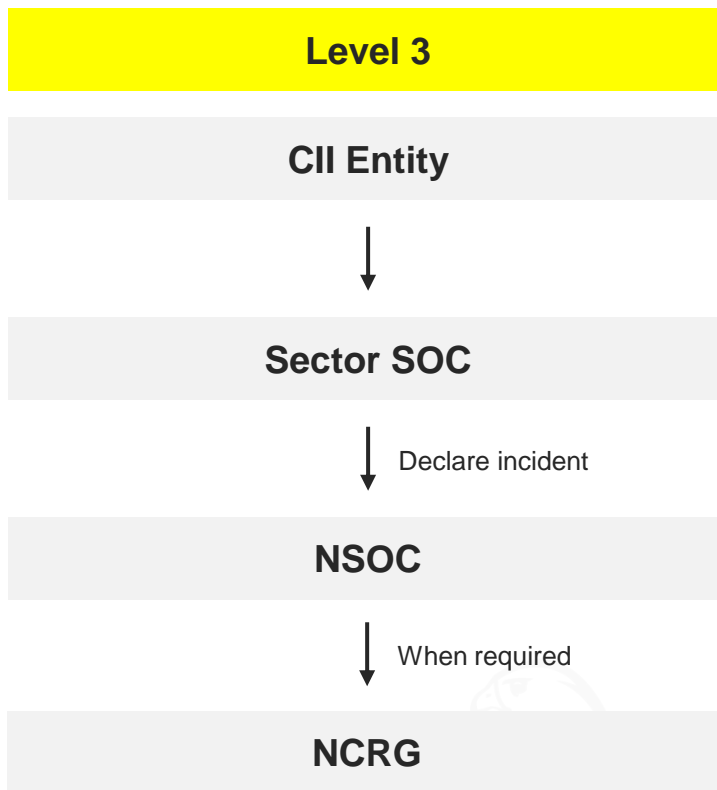
1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



8.2 Activation Crosswalk (Dependencies overview)

8.2.2 Significant Cyber Incident – Level 3 Incident declared

(Level 3, MTTN 60 min)



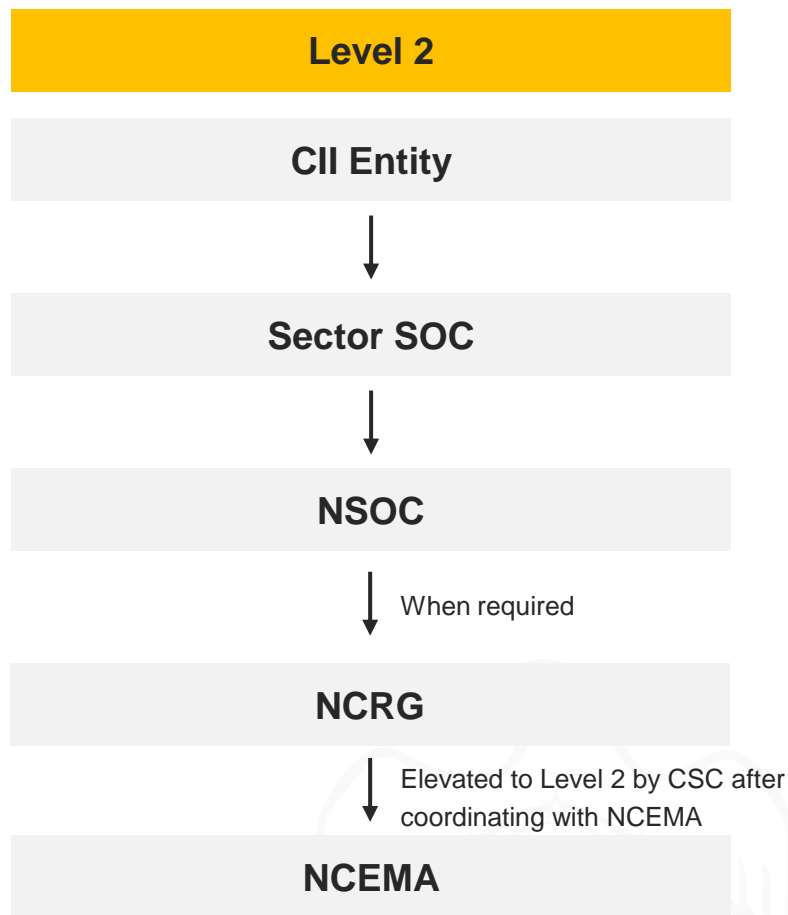
1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



8.2 Activation Crosswalk (Dependencies overview)

8.2.3 Significant Cyber Incident – Level 2 Incident declared

(Severe Incidents, Updates every 60 min)





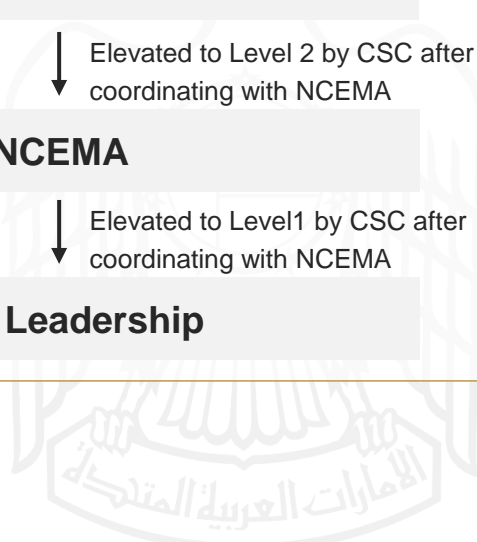
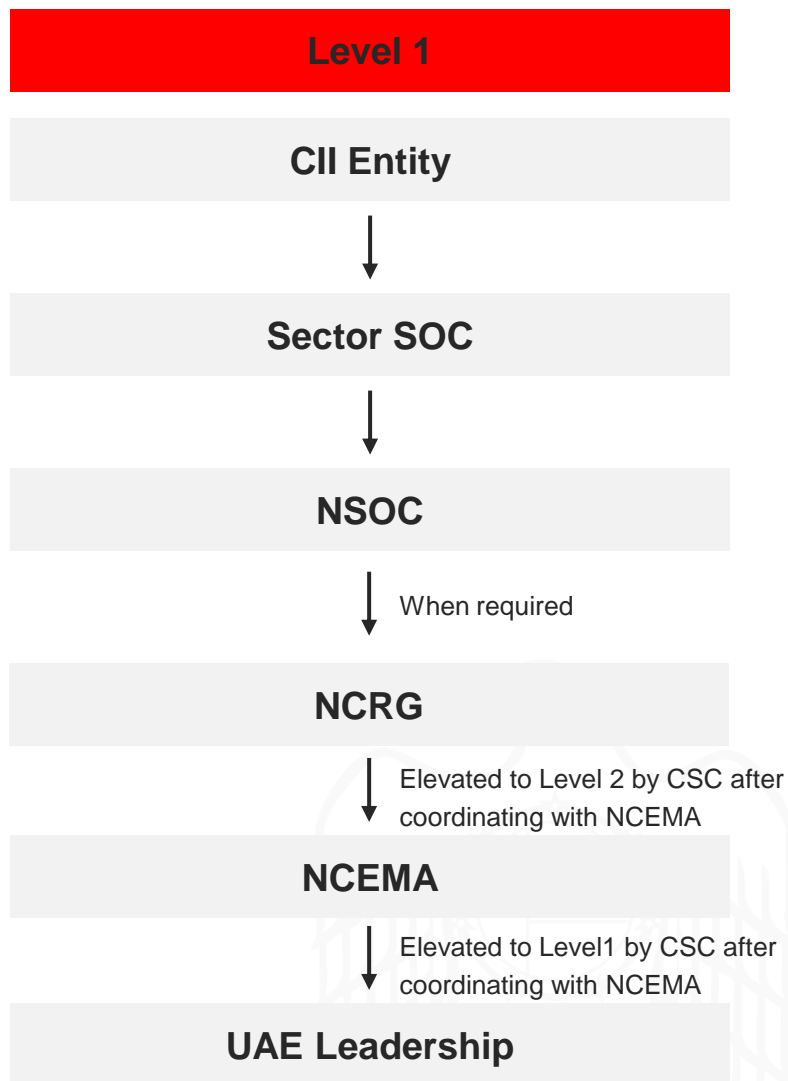
1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



8.2 Activation Crosswalk (Dependencies overview)

8.2.4 Significant Cyber Incident – Level 1 Incident declared

(Level 1 Incidents, Updates real-time)



1. Introduction	2. National Incident Response Governance Model	3. Cyber Incident Alert Schema	4. Cyber Incident Management Lifecycle
5. Reporting Requirements and Information Sharing (Federation)	6. Monitoring and Performance Management	7. Implementation	8. Appendices



8.3 Acronyms

Abbreviation	Description
aeCERT	Computer Emergency Response Team of the UAE
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CSC	Cybersecurity Council of the UAE
MTTN	Mean-Time-To-Notify
NCEMA	National Crisis and Emergency Management Authority
CIRF	Cyber Incident Response Framework
NCRG	National Cyber Response Group
CIRP	Cyber Incident Response Plan
NCSGF	National Cybersecurity Governance Framework
NCSS	National Cybersecurity Strategy
NSOC	National (Cyber) Security Operations Center
POC	Point of Contact
SOC	Security Operation Center
SOP	Standard Operating Procedure

