الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

NATIONAL INCIDENT MANAGEMENT FRAMEWORK

Public Version

Version 1.0

Disclaimer

The National Incident Management Framework (NIMF) is developed and maintained by the National Cyber Security Agency (NCSA) of State of Qatar. The NCSA is solely responsible for overseeing the development, update, and dissemination of the NIMF. The NCSA retains the right to make changes or amendments to the framework as it deems necessary.

Any reproduction concerning this document, or a part thereof, with the intent of commercialisation shall seek prior written authorisation from the NCSA. The NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The NCSA is committed to the continuous improvement and adaptation of the framework to effectively address the dynamic nature of cybersecurity threats.

The NCSA's decisions regarding the framework are final and binding. For further information and queries, please reach out to the NCSA.

Foreword from the President of NCSA

The issuance of the National Cyber Incident Management Framework marks a significant milestone in the execution of the second National Cyber Security Strategy, which emanated from the Qatar National Vision 2030.

This Framework has been designed to meet the emerging needs and challenges of the State of Qatar, by offering a comprehensive and coordinated approach to managing cyber incidents with national implications.

The framework aligns with the global best practices and lessons learned to ensure the state's full readiness to confront any challenges in the field of cyber security.

The framework equips the State of Qatar with a robust strategy for managing incidents involving information and operational technology that may pose a threat to national security. Furthermore, it guarantees the resilient restoration of reliable operation of critical services during cyber incident management, response, and recovery with high efficiency.

The National Cyber Incident Management Framework represents a qualitative step in safeguarding Qatar's cyber space, thereby reinforcing public confidence in the national capabilities in the field of cybersecurity through the unified efforts of all stakeholder, each of whom is entrusted with the responsibility of implementing the principles outlined in this Framework, as cyber security is a shared responsibility.

We are confident that the collective cooperation of entities within the State of Qatar will play a crucial role in building and strengthening the cyber security eco system, empowering the nation to effectively respond to and recover from cyber incidents.

His Excellency Eng. Abdulrahman bin Ali Al-Farahid Al-Malki
The President of National Cyber Security Agency

TABLE OF CONTENT

LIST OF FIGURES

01

Introduction

1. Introduction:

1.1 Overview

The NIMF is designed to strengthen the cyberspace of the State of Qatar by establishing a comprehensive approach for managing cyber incidents of national significance and minimising their impact. This will be achieved through coordinated decision-making and cooperation among multiple stakeholders.

NIMF has been developed to fulfil the following purposes:

- Establish a comprehensive framework for managing cybersecurity incidents of national significance, ensuring rapid detection, a coordinated response, and prompt restoration of national services.
- Articulate a holistic and integrated strategy that delineates the roles and responsibilities of all engaged stakeholders.
- Enhance stakeholders' comprehension of the NCSA's processes for mitigating cybersecurity incidents.
- Integrate improvements derived from lessons learned to reinforce future response capabilities.
- Strengthen the cyberspace of the State of Qatar through the implementation of proactive and responsive measures.

1.2 Scope and Intended Audience

The NIMF addresses the management of cybersecurity incidents of national significance within the cyberspace of the State of Qatar and is applicable to all entities within the country. It is important to note that this framework solely focuses on cyber incidents management while cyber crisis management is covered under the National Cyber Security Crisis Management Framework (NCCMF). The engagement of stakeholders and the delineation of their responsibilities are contingent upon the nature of the specific incident at hand.

This publication of the NIMF is intended for dissemination to all entities in the State of Qatar. It summarizes the key concepts delineated in the framework and provides an overview of the high-level incident management workflow. Detailed versions tailored to specific needs are available upon request, with such requests subject to evaluation to ensure alignment with the framework's overarching objectives.

1.3 Purpose of this Document

This publication of the NIMF outlines the approach for responding to and managing incidents of national significance in the State of Qatar. It aims to inform and educate the general public about the national plan for managing cyber incidents.

1.4 Assumptions and Principles

The effective implementation and operation of the NIMF are based on the following key assumptions and principles:

- **Compliance and Adherence:** All stakeholders are expected to comply with the framework's guidelines and perform delegated activities within the required timelines.
- **Timely Reporting and Response:** It is required that all relevant cyber incidents be reported promptly to the NCSA by all entities in the State of Qatar to enable effective and timely response actions.
- **Adequate Resources:** The framework's success depends on the allocation of sufficient resources, including personnel, technology, and funding, to support its operations.
- **Communication and Coordination:** It is expected that there will be seamless communication and coordination among all stakeholders to ensure a unified and effective response to cyber incidents.

- **Active Stakeholder Engagement:** It is expected that all relevant stakeholders, including public and private entities, will actively support NCSA's incident management efforts and contribute to its success.
- **Continuous Improvement:** The framework will undergo regular reviews and updates based on emerging threats, technological advancements, and lessons learned to ensure its ongoing effectiveness and relevance.
- **Integration with Existing Policies:** The framework will be aligned with other existing national policies, plans, and procedures to ensure consistency and effectiveness.

1.5 Definitions

1.5.1 Information Security Incident

An information security incident as defined in the Qatar National Information Assurance Standard version 2.1 *is an event that impacts the confidentiality, integrity or availability of an information system or network, through an act that contravenes prescribed security policy and or applicable laws or regulations. For the purposes of this standard, an incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices*[1].

1.5.2 Cyber Incident of National Significance

Complementary to the general definition of an information security incident, a cyber incident of National Significance in the State of Qatar is defined as an Event with a negative impact on the information assets of the State of Qatar (including industrial control systems and other operational technology) and/or the infrastructure enabling them.

1.5.3 Crisis

As per the ISO 22361:2022, a crisis is defined as *an abnormal or extraordinary event or situation that threatens an organisation or community and requires a strategic, adaptive and timely response in order to preserve its viability and integrity*[2].

1.6 Categorisation of Cyber Incidents

When a potential cyber incident is identified, the NCSA conducts an analysis of the incident at hand and categorises it as an incident of National Significance (Red, Orange, Yellow) or an incident of no national significance (White) based on its impact, severity, spread and urgency for the correct course of action. The incident category will dictate the division of responsibilities between stakeholders (NCSA, Sectoral CERT and Affected Entity), process steps that will be taken throughout the lifecycle and the nature and level of involvement of partners.

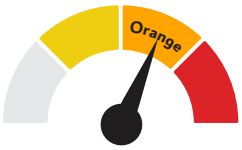
1 Cyber Security Policies and Standards | National Cyber Governance and Assurance Affairs (ncsa.gov.qa/ar/regulatory-tools)

2 ISO 22361:2022 - Security and resilience — Crisis management — Guidelines. International Organization for Standardization.

The NCSA will assign one of the following categories to any confirmed cybersecurity incident:

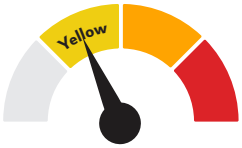
Nationally coordinated incident

A cyber security incident that poses significant threats or vulnerabilities, affecting government, public, or private sectors with potentially severe economic, social, national security, or reputational consequences, requiring a coordinated national response.



Sectorally coordinated incident

A major cyber security incident involving significant threats or vulnerabilities, with potentially severe consequences for a specific sector or large entity, where damage can be contained within a sectoral coordinated response.



Locally coordinated incident

A locally coordinated cyber security Incident of national significance that affects only a single entity, it is likely to be contained within that entity with no further spread, poses no significant broader impacts, but it should be monitored for potential escalation.

Incident of no national significance

A cyber security incident of no national significance that does not affect critical national services, can be contained by the affected entity, and has no national level impact, but can be recorded for future statistical analysis by the NCSA.

Figure 1: Categories of Incidents of National Significance

The categorisation of the cyber incidents is performed by the NCSA during the Notification & Categorisation phase described in the Incident Management Lifecycle as shown in Figure 4.

In a Period of Special Interest (PSI), the NCSA may proactively adjust the criteria for incident categories as part of their readiness efforts. A PSI is defined as a timeframe during which an event of economic, security, or cultural significance occurs within the State of Qatar that requires a heightened level of national alertness.

1.6.1 Cyber Crisis Escalation

Where a cyber incident of National Significance escalates into a crisis, it is imperative to adopt a strategic and hierarchical response approach. To address this. The National Cyber Crisis Management Framework (NCCMF) provides the national cyber crisis management capability beyond the NIMF, as it demands extraordinary measures, coordinated efforts, and the mobilisation of resources to guarantee effective response, facilitate recovery, and encourage the adaption of concepts of agility and resilience on national, sectoral, and organisational levels.

If a cyber security incident results in a declared crisis, both frameworks will seamlessly cooperate to deliver the most effective and expedited operational and strategic response.

02

The Framework Governance

2. The Framework Governance

2.1 Authority

As per the Emiri Decree No. (1) of 2021, the NCSA is responsible for safeguarding the cyberspace of the State of Qatar. In order for the NCSA to fulfill its mandate, the NIMF was created with the purpose of detailing how cyber incidents are managed by the NCSA and stakeholders. The NCSA is responsible for incident management and response during incidents of national significance which are cybersecurity incidents that affect Critical National Organisations and critical services within the State of Qatar.

According to Article No. (3) of the aforementioned decree, NCSA is entitled within its authority to *"develop and implement a national plan for response and recovery from cybersecurity incidents in coordination and collaboration with other stakeholders* [3]*"*. This initiative aligns with the objective of the second national cybersecurity strategy which emerges from the Qatar National Vision 2030.

2.2 Services

The NCSA plays a pivotal role in safeguarding the State of Qatar's cyberspace by managing incidents of national significance. It implements proactive measures to mitigate risks and bolster the state's incident response capabilities.

The NCSA is responsible for investigating, analysing, and reporting on cybersecurity incidents with partner's support. It supports remediation efforts to ensure effective recovery and containment of threats. The agency issues, reviews, and participates in the creation of incident response-related guidelines, providing technical advice to enhance cybersecurity measures. Additionally, it conducts regular training programs on incident response to prepare stakeholders for handling incidents. The NCSA ensures timely and effective response services during incidents of national significance, providing essential support for recovery and remediation across critical sectors and government entities.

2.3 Criminal Investigation of Cyber Incidents

As per the Law No. (14) of 2014 of the State of Qatar promulgating the Cybercrime Prevention Law, a Cybercrime is defined as *"Any act involving unlawful use of an information technology technique, an information system or internet in violation of the provisions of this Law* [4]*"*.

Procedures for collecting evidence are carried out independently by the Ministry of Interior's Economic and Cyber Crime Combatting Department "MoI-ECCCD" and/or State Security Bureau "SSB" in coordination with Public Prosecution, regardless of the incident response determined by the NCSA.

In case a criminal investigation is initiated, in addition to standard NIMF procedures, NCSA will align with law enforcement and concerned authorities and support them technically in the criminal investigation.

MoI-ECCCD and NCSA will coordinate forensic data collection in accordance with international best practices and evidence principles.

3 Qatar, Amiri Decree No. 1 of 2021 Establishing the National Cyber Security Agency, Article 3, published in Al Meezan website , www.almeezan.qa.

4 State of Qatar, 2014. Law No. 14 of 2014 on Cybercrime Prevention. Qatar Legal Portal (Al-Meezan) https://www.almeezan.qa/LawPage.aspx?id=6016&language=en Accessed (FEB 2025).

03

NIMF Stakeholders

3. NIMF Stakeholders

The National Incident Management Framework developed by the NCSA requires cooperation from several stakeholders, which is necessary for efficient management, investigation and resolution of nationally significant cyber incidents. Additionally, several groups and teams are convened in response to the cyber security incident of national significance, during the initiation phase of the lifecycle. This section lists the stakeholders in NIMF. Figure 2 represents the incident stakeholders, and Figure 3 represents incident groups that are convened in response to the incident for the duration of the response.

3.1 Stakeholders

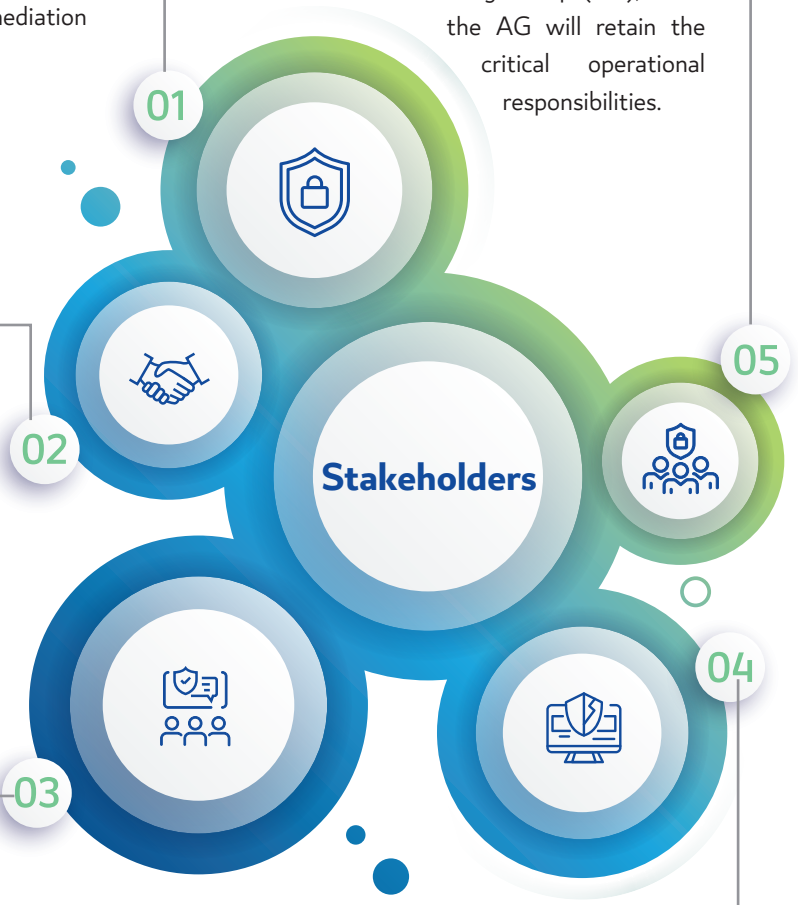
Stakeholders include all Partners, Sectoral CERTs, and other entities that collaborate with the NCSA on incident management and response.

NCSA

The NCSA is the central agency responsible for the maintenance and execution of the NIMF. NCSA is the core stakeholder responsible for incident response, remediation and management.

Crisis Management Team (CMT)

The CMT becomes involved only when a crisis is declared for a cyber incident. In the event of a crisis, CMT will take over the national strategic responsibilities from the Authorising Group (AG), while the AG will retain the critical operational responsibilities.



Partners

The term Partners includes selected governmental entities that are supporting the NCSA in incident management activities. Partners are responsible for their own areas of authority in the context of cybersecurity incidents.

Sectoral CERTs

The Sectoral CERT is an organisation that has regulatory powers within a sector with sufficient cybersecurity capabilities to perform cyber incident response activities and may be designated this role as determined by NCSA. The Sectoral CERTs must meet certain criteria and be able to support sectoral incident response. The NCSA coordinates the response to cyber incidents of national significance with the respective Sectoral CERT for the Affected Entity.

Affected Entities

An affected entity is any organisation or entity within the cyber space of Qatar which has encountered and is affected by a cyber security incident.

Figure 2: Stakeholders

3.2 Incident Response Management Groups

Incident response management groups are convened by the NCSA in response to a particular incident of national significance for collaboration and support. They support the cyber incident response and management for the duration of the cyber incident.

Authorising Group (AG)

The Authorising Group is an assembly of senior executives from within the government, responsible for oversight of the incident management process and strategic decision-making concerning the incident. The purpose of the AG is to gather strategic stakeholders' representatives in a single group, to allow for quick and effective decision-making. The AG is formed specifically for the duration of the incident

Affected Entity Support Team

The affected entity supports the IR team of NCSA or Sectoral CERT in their incident response activities during a cyber incident. The affected entity support team facilitates and provides the required physical and digital access, organisational knowledge, and logistical and administrative support.

Technical Working Group (TWG)

The Technical Working Group is an assembly of appropriately qualified and experienced technical specialists responsible for the technical oversight of the incident and is formed specifically for the duration of the incident.

Incident Response (IR) Team

The Incident Response team handles several phases of the incident management lifecycle.

The NCSA always takes the role of the initial IR team after the incident is initiated. After forensic data has been collected, the role of the IR team can be delegated to the Sectoral CERT (in Orange incident) or to the Affected Entity (in Yellow incident).

Figure 3: Incident Response Management Groups

04

Incident Management Lifecycle

4. Incident Management Lifecycle

The incident management lifecycle is a structured approach to handling cybersecurity incidents, encompassing five phases. This lifecycle represents the comprehensive process involved in effectively managing incidents of national significance, ensuring a swift and coordinated response. The incident management lifecycle outlines the streamlined process that is followed when an incident occurs. The five phases of the incident management lifecycle are shown in Figure 4 below:

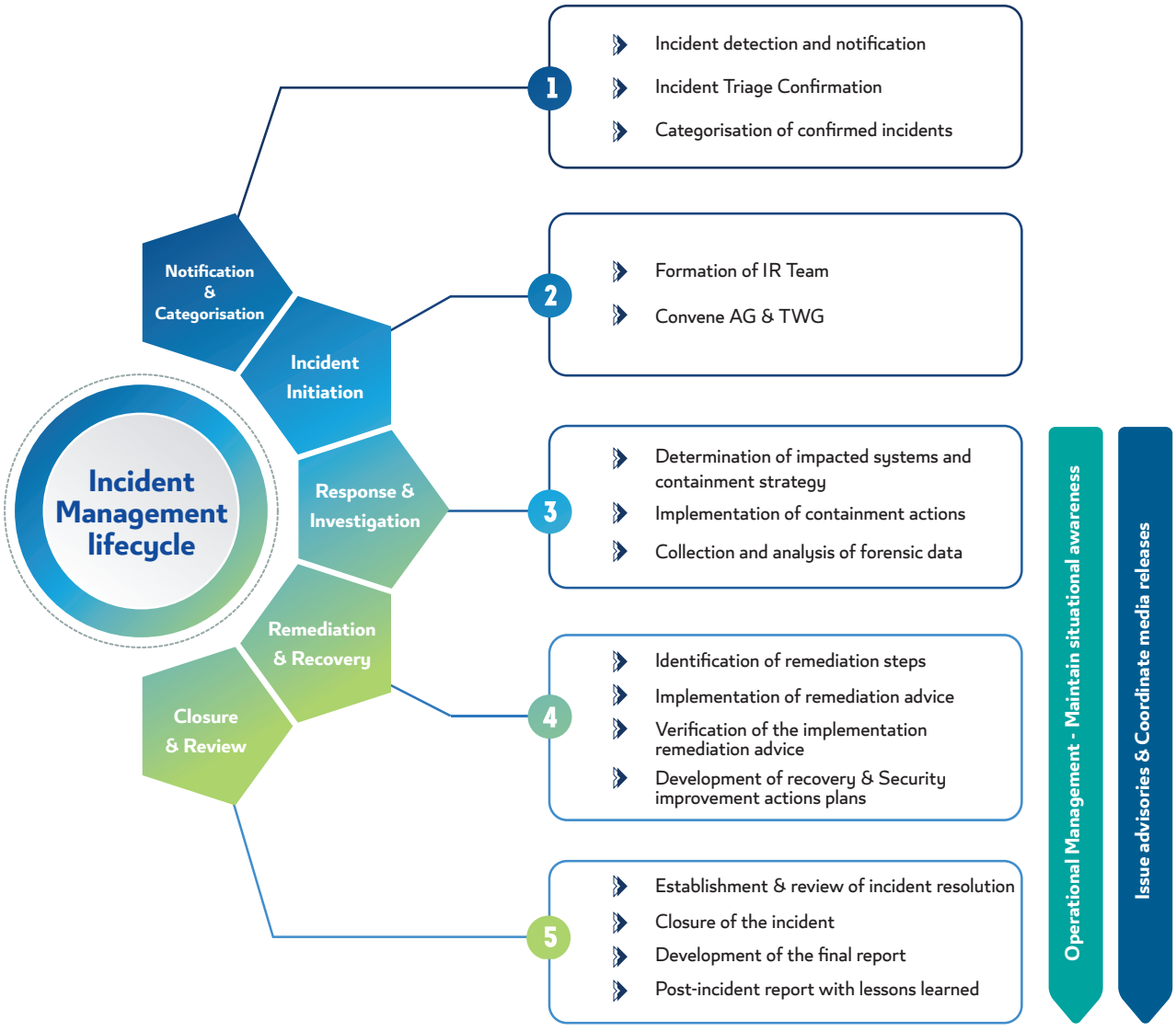


Figure 4: Incident Management Lifecycle

The Incident Management Lifecycle begins with the Notification & Categorisation phase and ends with the Closure & Review phase. In addition to these phases, NIMF includes Operational Management activities, which take place in parallel to the last three phases.

Operational Management Activities

The operational management activities commence after the Initiation phase is completed. This phase runs in parallel and includes all the management and coordination activities up until the incident closure. As part of the operational management the authorising group takes strategic decisions regarding the response activities, supported by the technical working group.

Depending on the incident category, NCSA directs the response and the allocation for activities as required. The NCSA may also partially delegate this responsibility to Sectoral CERT or the affected entity.

As part of operational management, the NCSA may issue advisories and media releases. Shown below is a summary and comparison of the two communication forms:

NCSA Advisory

- **Technical advisory:** Threat Intelligence or vulnerability focus.
- **Target Audiance :** Restricted recipients, adhering to Traffic Light Protocol (TLP).

Media Release

- Public statement about the incident.
- **Target Audiance :** The general public.
- Approved and released by the AG, NCSA, and other relevant authorities.
- May have a form of a media statement, TV interview, press release, social media post or others.

4.1 Notification & Categorisation Phase

The prompt reporting of incidents of high severity is critical to ensure timely and effective response. Stakeholders are urged to utilise the NCSA contact information available on the NCSA website[5]. Timely incident notifications ensure a rapid response by NCSA to mitigate the spread and adverse impact of the incident and can prevent further escalation.

As per the Qatari National Information Assurance (NIA) Standard[6], all organisations within the State of Qatar must report critical cyber incidents to the NCSA within two hours of identification.

The NCSA provides several notification channels, through which incident notifications can be reported. Upon receipt, the NCSA assesses the notification to confirm the incident. NCSA categorises confirmed incidents based on their severity, spread, urgency, and impact on the national level.

The incident categorisation performed by the NCSA assesses the impact of the cyber incident at a national level and is independent of the classification performed internally by the affected entity.

4.2 Initiation Phase

After categorisation, the incident response process is initiated by notifying the relevant stakeholders, assembling the IR team, and collecting preliminary information about the incident. During this phase, NCSA starts initiating both internal resources and external stakeholders for incident management and response. In particular, the following groups are initiated for every incident of national significance:

- Incident Response Team of the NCSA
- Affected Entity Support Team
- Authorising Group
- Technical Working Group

5 https://www.ncsa.gov.qa

6 Cyber Security Policies and Standards | National Cyber Governance and Assurance Affairs (ncsa.gov.qa/ar/regulatory-tools)

4.3 Response & Investigation Phase

The response & investigation phase begins after the initiation phase is complete. In this phase, the IR team takes immediate action to contain and mitigate the incident. The IR team conducts a thorough investigation that consists of several steps with the focus on preventing damage and spread of the incident.

Depending on the category of the incident and other factors the incident analysis is conducted by either the NCSA, the relevant Sectoral CERT, or by the Affected Entity itself and will be determined and communicated by the NCSA, as such.

4.3.1 First Response

As part of the first response, the incident response (IR) team of NCSA takes immediate actions to secure (limit physical and digital access) the impacted systems, contain the attack and mitigate the incident to prevent further damage or spread. The primary goal during containment is to stabilise the situation, ensuring that the incident does not escalate further, and setting the stage for thorough investigation and resolution.

4.3.2 Forensic Data Collection and Investigation

The investigation phase involves collection and analysis of forensic data. The forensic data collection is performed only by the NCSA and MoI-ECCCD to ensure that it meets legal requirements. Collected forensic data is analysed to determine the root cause of the incident, assess the extent of the damage, and to remediate and mitigate the threat.

The IR team assesses the impact of the incident on systems, data, and operations. Understanding the full impact helps prioritise recovery efforts and directs communication with stakeholders.

4.3.3 Communication and Reporting

Throughout the incident response phase, maintaining clear communication is essential. The IR team provides regular updates to stakeholders including management, affected departments, and external partners, ensuring transparency and coordinated efforts. Detailed reports are generated to document the incident, actions taken, and lessons learned, contributing to the continuous improvement of the organisation's cybersecurity posture.

4.4 Remediation & Recovery Phase

The remediation & recovery phase is activated as soon as the initial response & investigation actions have been performed by the IR team. The purpose of the remediation & recovery phase is to remediate the consequences of the incident and recover operational readiness. In this phase, the NCSA or Sectoral CERT will provide remediation advice, and verify the completeness of remediation activities.

Depending on the category of the incident and other factors the remediation and recovery advice is provided by either the NCSA, the relevant Sectoral CERT, or by the Affected Entity itself.

4.5 Closure & Review Phase

Once the IR team concludes its response and investigation activities, and the critical activities of the remediation and recovery phase are verified, the final phase involves formally closing the incident and conducting a comprehensive post-incident review. The process includes evaluating the effectiveness of the incident response, identifying areas for improvement, and documenting lessons learned. The insights gained from this review are crucial for refining incident response procedures, strengthening the organisation's overall security posture, and enhancing cooperation among all stakeholders involved. This systematic approach ensures continuous improvement and preparedness for future incidents.

05

Appendix

5. Appendix

5.1 Glossary Tables

5.1.1 Glossary - General Terms

Term	Explanation of Term
Cyber Incident	A cyber incident of National Significance in the State of Qatar is defined as an Event with a negative impact on the information assets of the State of Qatar (including industrial control systems and other operational technology) and/or the infrastructure enabling them[7].
Computer Emergency Response Team (CERT)	A CERT is a group of cybersecurity experts responsible for responding to and mitigating computer security incidents, providing guidance on best practices, and facilitating coordination among organisations to enhance overall cybersecurity.
Evidence	Information used by MoI-ECCCD (or other law enforcement authorities) for criminal investigation or when data collected and analysed is attributed to the root cause or the timeline relating to the incident. If the criminal investigation has been initiated all the forensic data should be treated as potential evidence in a criminal investigation.
Forensic Data	The body of facts or information related to the incident, that may contain factual evidence. All evidence principles apply to forensic data.
Incident of National Significance	Cybersecurity incidents that affect Critical National Infrastructure and Critical Services within the State of Qatar.
Qatar National Incident Management Framework (NIMF)	Qatar National Incident Management Framework is the overall framework and capabilities to effectively and efficiently prepare for, mitigate where possible, respond to, and recover systems from Incidents of national significance.
Period of Special Interest (PSI)	A PSI is defined as a timeframe during which an event of economic, security, or cultural significance occurs within the State of Qatar that requires a heightened level of national alertness.
Stakeholders	Organisations involved in the execution of National Incident Management processes.
System	Any endpoint, server, cloud infrastructure, software tool, web portal, or another entity from which the forensic data can be collected.

7 Cyber Security Policies and Standards | National Cyber Governance and Assurance Affairs (ncsa.gov.qa/ar/regulatory-tools)

5.1.2 Glossary - Stakeholders

Stakeholder	Description of stakeholder
Affected Entity	A government or private organisation that was impacted by a cyber Incident of National Significance
Authorising Group (AG)	The AG is convened in response to the incident and is tasked with oversight and strategic decision-making within the national incident management process.
Critical National Organisations (CNO)	CNOs are organisations that offer critical services in the State of Qatar.
Incident Response (IR) Team	The IR Team handles the operational aspects of the incident management process. The role of the IR team can be taken by the NCSA, Sectoral CERT or Affected Entity.
MoI-ECCCD	Ministry of Interior's Economic and Cyber Crimes Combatting Department is Qatar's national law enforcement department involved in the processing of crimes involving the use of modern telecommunication networks such as the Internet.
NCSA	National Cyber Security Agency under his H. E. the Prime Minister.
Public Prosecution	An independent judicial body which considers criminal cases on behalf of the community. It oversees law enforcement and ensures the enforcement of laws. It has exclusive jurisdiction to conduct criminal proceedings of laws[8].
Sectoral CERT	An organisation within a sector that may be designated this role as determined by NCSA and with sufficient cyber capabilities to perform incident response activities. The NCSA approves Sectoral CERTs based on particular criteria and ability to support sectoral incident response.
State Security Bureau (SSB)	A governmental bureau in the State of Qatar. Within NIMF, SSB is responsible for national security and criminal investigations working in coordination with MoI-ECCCD.
Technical Working Group (TWG)	The TWG is tasked with technical oversight and decision-making. The TWG advises the incident response team and escalates any concerns that arise to AG.

8 https://www.pp.gov.qa/English/Pages/default.aspx

5.2 Contact Details

The following contact details and guidelines can be used to contact the NCSA in case of a cyber incident's:

Team Name	Communication Coordination Command Office
Address	PO Box 24100, Wadi Al Sail Street, Doha State of Qatar
Time Zone	Arabian Standard Time, GMT+3
Phone Number and Availability	16555 Available 24/7
Email address	NCSOC@ncsa.gov.qa
International Phone Number and Availability	+974 51016555 Available 24/7
International Email	Cert@ncsa.gov.qa
Public Keys and Encryption	Use the NCSA public key when you want/need to encrypt messages that you send to the NCSA. When due, the NCSA will sign messages using the same key. To receive the public key, please contact the NCSA through the information provided above. When due, please sign your messages using your own key– it helps when that key is verifiable using the public key servers.
Website	https://www.ncsa.gov.qa

5.3 Related Materials

National Information Assurance Standard [9]

Qatari standard that aims to regulate and govern the data assurance and security in the organisations of the State of Qatar and identify the basic principle in understanding the data governance and covering the important controls of protecting data through its lifecycle.

National Information Security Compliance Framework [10]

Regulatory framework created to validate and assure security that is driven and guided by the National Information Assurance Standard.

5.4 Forensic Readiness

The readiness of an organisation to effectively collect, preserve, analyse, and present digital evidence when needed, ensuring that such processes are efficient and cost-effective. This readiness involves the implementation of processes and procedures that enable the organisation to maximise the utility of digital evidence while minimizing the time and costs associated with digital investigations. Forensic readiness is crucial for enabling swift and effective responses to cyber incidents, ensuring that the evidences are handled properly to support legal and regulatory requirements.

Key Benefits of Forensic Readiness

- **Enhanced Incident Response:** Facilitates swift and effective evidence collection and analysis, reducing the impact and recovery time of national security incidents.
- **Improved Business Continuity:** Reduces interference with business processes, ensuring critical national infrastructure and services remain operational.
- **Enhanced Security Posture and Collaboration:** Strengthens overall security, supports national cooperation, and enables continuous improvement through strategic insights and lessons learned.
- **Cost Efficiency:** Minimises both direct and indirect costs of digital investigations by having established processes in place.

9 Cyber Security Policies and Standards | National Cyber Governance and Assurance Affairs (ncsa.gov.qa)
10 National Information Security Compliance Framework | National Cyber Governance and Assurance Affairs (ncsa.gov.qa)

06

Conclusion

6. Conclusion

The National Incident Management Framework has been developed to address the evolving challenges confronting the State of Qatar by establishing a comprehensive and coordinated strategy for managing cyber incidents of national significance. This pioneering initiative significantly enhances the nation's capacity to detect, respond to, and recover from cyber threats with unparalleled efficiency and effectiveness.

Developed by the National Cyber Security Agency in accordance with globally recognized cyber security governance standards, the framework promotes seamless collaboration among all state organizations, regardless of technological variations. This ensures the protection of the nation's critical assets and guarantees the continuity of essential services. The framework sets a global standard for effective leadership in managing incidents that threaten national security, ensuring uninterrupted services and the swift restoration of operations during and after any incident.

Furthermore, the framework is designed with a dynamic, forward looking mechanism designed to adapt continuously to emerging and evolving risks. This flexibility ensures that Qatar remains at the forefront of cyber security preparedness, enabling the nation to proactively address the rapid pace of global technological developments.