NWC OT Cybersecurity Risk Management Procedure

Document Number:	A01001045-PRO-RM
Issue Date:	June 29, 2021
Revision Number:	00
Issued For:	Review

Revision Details

Name	Title/Dept.	Signature	Date
Prepared by:			
Sidrat Mehreen	Senior OT cybersecurity Analyst		June 27,2021
Reviewed by:			
Sameen Ullah Khan	OT Cybersecurity Lead		June 28,2021
Approved by:			
Farhan Rasheed	Operations Manager		June 28,2021

Issued by:			
Syed Ali Raza	Planning Engineer		June 29,2021

History Page

Issue No.	Issue Date	Prepared By (Name)	Reviewed By (Name)	Owned By (Name)	Endorsed By (Name)	Approved By (Name)
Change Description						
Change Description						
Change Description						

Reference Documents

Document Number	Document Title
ECC-1:2018	National Cybersecurity Authority Essential Cybersecurity Controls (NCA ECC)

Document Roles and Responsibilities

	Prepare/ Update/ Amend	Review	Approve	Publish
Owner	YES	YES		
Cybersecurity Steering Committee		YES		YES
Corporate Strategy & Performance Management VP			YES	

Table of Contents

Glossary

Word or Phrase	Explanation
Asset	General support system, major application, resources, high impact program, physical plant, or a logically related group of systems
Asset Inventory	Location, condition, owner, status, procurement dates, depreciation or values of the assets
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.
Compliance	Ensuring that a Standard or set of Guidelines are followed. A means of conforming to a rule, such as a specification, policy, standard or law.
Risk	The level of impact on organizational operations, organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk assessment	The process of identifying risks to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk.
Risk severity	Risk severity is defined as the degree of impact of a defect has on the development or operation of a component application being tested.
Risk mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process
Risk assessment report	The report which contains the results of performing a risk assessment or the formal output from the process of assessing risk.
Acceptable risk	The level of Residual Risk that has been determined to be a reasonable level of potential loss/disruption for a specific OT system.
Test environment	A controlled Environment used to test Configuration Items, Software Builds, OT/IT Services, Processes, etc.
SuC	Systems under consideration

1. Introduction

The role of this risk management procedure is to provide NWC staff, how to apply consistent and comprehensive risk management. This procedure provides information on how to identify, analyze, evaluate, and treat risks. This procedure is applicable to all NWC OT infrastructure.

2. Roles and Responsibilities

Roles	NWC Representative	Responsibilities
Request Initiator	Any OT Asset Owner, NWC Information Security, NWC Leadership/Management	Initiates the request for risk assessment
Risk Owner	Any OT Asset Owner, NWC Leadership/Management	Co-ordinate efforts to mitigate and manage the risk with other stakeholders who own parts of the risk
NWC Information Security	Information security officer	• Request Approval Authority • Perform risk assessment • Comply risk mitigation implementation with determined risk mitigation solution
Risk Assessment Team	All NWC representative who are in any way involve with OT asset and information security	Perform risk assessment

3. Risk Assessment Process

The criticality of NWC OT assets can be identified by evaluating its risk exposure (impact and probability) on the ability of NWC production.

Risk assessment process consists of following steps:

1. Risk Identification
2. Risk Analysis
3. Risk Mitigation
4. Reporting

3.1 Risk Identification

1. After the approval of risk assessment request from NWC Information Security team, Risk assessment team initiates risk assessment on approved SuC. After high level and detailed risk assessment, gaps/vulnerabilities are identified in NWC OT assets. Assets to be evaluated against the risk-based criteria, include all type of OT assets.

2. The risks will be identified by reviewing risk-based criteria as mentioned in Appendix A.

3.2 Risk Analysis

1. Identified risks will be analyzed based on likelihood of incident and the impact or consequences of that incident. Incident likelihood is affected by the availability and effectiveness of existing controls.

Risk = Likelihood x Consequences

2. Compare risks against risk evaluation criteria and prioritize the risks.

The criteria for evaluating the risks will be:

Risk Likelihood	
VERY UNLIKELY	Rare chance of an occurrence
UNLIKELY	Not likely to occur under normal circumstances
LIKELY	May occur at some point under normal circumstances
VERY LIKELY	Expected to occur at some point in time
CERTAIN	Expected to occur regularly under normal circumstances

And

Risk Consequences	
VERY LOW	Minor software/HW error, availability minimally affected.
LOW	Minor software error, workaround available, short availability problems.
MEDIUM	Operations halt staff cannot work. Affects customers. Some loss of data.
HIGH	Operations halt. Significant financial loss. Customer's leaver or breach of laws or regulations
VERY HIGH	Complete loss of operations, major data errors causing wrong decisions or faults.

3. Based upon the above factors, risk impact factor is analyzed using risk matrix.

Risk Severity Matrix					
LIKELIHOOD X CONSEQUENCES	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
CERTAIN	MAJOR	CRITICAL	CRITICAL	HIGHLY CRITICAL	HIGHLY CRITICAL
VERY LIKELY	MAJOR	MAJOR	CRITICAL	CRITICAL	HIGHLY CRITICAL
LIKELY	MINOR	MAJOR	MAJOR	CRITICAL	CRITICAL
UNLIKELY	MINOR	MINOR	MAJOR	MAJOR	CRITICAL
VERY UNLIKELY	VERY MINOR	MINOR	MINOR	MAJOR	MAJOR

3.3 Risk severity

Highly Critical:

- Security: Catastrophic; unrecoverable major system/facility loss or harm. Inability to perform multiple essential functions.
- Safety: Death or permanent disability. Lasting environmental or public health impact

Critical:

- Security: Major loss of OT assets, including subsystem loss, inability to perform essential functions or serious facility/system damage.
- Safety: Serious injury; temporary disability. Temporary environmental or public health impact

Major:

- Security: Moderate loss of OT assets or moderate impact to operations. More than slight facility/system damage or harm.
- Safety: Medical treatment beyond first aid required; lost workdays. More than routine cleanup.

Minor:

- Security: Limited loss of OT assets or temporary disruption to operations. Slight facility/system damage.
- Safety: Minor first aid treatment or routine cleanup.

Very Minor:

- Security: Minimal impact. Easily contained OT asset damage, loss, or harm. Near miss.
- Safety: Minimal treatment required.

3.4 Risk Mitigation

To reduce the assessed risks, appropriate and justified controls should be identified and selected by risk assessment team. The aim of control implementation is to reduce risk to acceptable level. Risks identified as Highly Critical, Critical and Major will receive a higher level of priority to reduce severity of risk.

While implementing countermeasures, asset owner will make sure that mitigation plans is followed so implantation will be completed within scope, time, and budget.

3.5 Risk Reporting

A comprehensive risk assessment report and risk register will be submitted to all stakeholders of risk assessment team for review.

4 Process

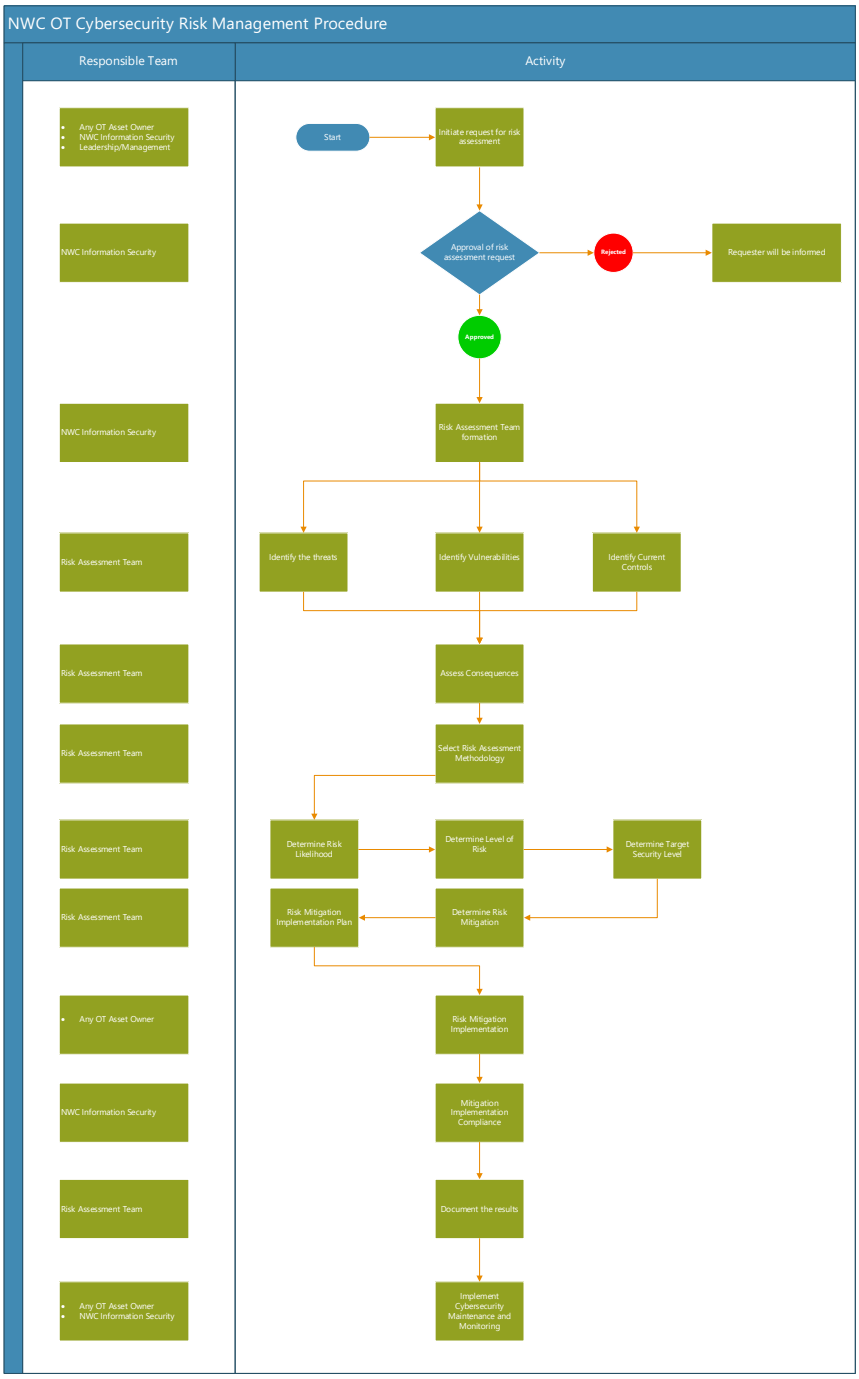
Activity		Responsible	Description
1.1	Initiate request for risk assessment	Any OT Asset Owner NWC Information Security NWC Leadership/Management	Initiator or Responsible person initiates the request for risk assessment • Define SuC • Define Risk assessment boundaries • Provide Relevant SuC documents
1.2	Approval of risk assessment request	NWC Information Security	NWC Information Security approves the risk assessment request
1.3	Risk Assessment Team formation	NWC Information Security	NWC Information Security form the Risk Assessment Team
Risk Identification			
1.4	Identify the threats	Risk Assessment Team	Risk assessment team identifies threats for all the assets in scope
1.5	Identify Vulnerabilities	Risk Assessment Team	Vulnerabilities are identified for all the assets in scope.
1.6	Identify Current Controls	Risk Assessment Team	Risk assessment team identifies current controls for risk mitigation
1.7	Assess Consequences	Risk Assessment Team	Based on threats and vulnerabilities, consequences will be determined.
Risk Assessment			
1.8	Select Risk Assessment Methodology	Risk Assessment Team	Qualitative or quantitative risk methodology is identified based on prior incidents, assets and vulnerabilities criticality
1.9	Determine Risk Likelihood	Risk Assessment Team	Based on identified vulnerabilities and existing countermeasures, risk likelihood is determined.
2.0	Determine Level of Risk	Risk Assessment Team	Severity of risk is identified by formally calculating likelihood of event occurring and consequences.
2.1	Determine Target Security Level	Risk Assessment Team	Target security level is set to reduce risk to acceptable level

Activity		Responsible	Description
Risk Mitigation			
2.2	Determine Risk Mitigation	Risk Assessment Team	According to the target security level, risk is mitigated by implementing countermeasures
2.3	Risk Mitigation Implementation Plan	Risk Assessment Team	Risk Assessment Team will develop risk mitigation implementation plan
2.4	Risk Mitigation Implementation	Any OT Asset Owner	Risk mitigation will be implemented as per implementation plan
2.5	Mitigation Implementation Compliance	NWC Information Security	NWC Information Security comply Risk Mitigation Implementation with determined risk mitigation solution
Risk Management Document			
2.6	Document the results	Risk Assessment Team	Results are documented in risk assessment report and risk register
OT Cybersecurity Maintenance and Monitoring			
2.7	Implement Cybersecurity Maintenance and Monitoring	Any OT Asset Owner NWC Information Security	OT Asset Owner and NWC Information Security will continuously monitor and maintain OT risk management

5 Audit and Compliance

1. Risk Register and risk assessment report will be maintained and used for audit purposes.
2. Risk Register and risk assessment report will be continuously reviewed and updated as per OT Cybersecurity Risk Management Policy.

6 Process Flow Chart



Appendices

Appendix A- Risk based criteria

Policy and Procedure

1. Inadequate security policy for the IACS
2. No formal IACS security training and awareness program
3. Absent or deficient IACS equipment implementation guidelines
4. Lack of administrative mechanisms for security policy enforcement
5. Inadequate review of the effectiveness of the IACS security controls
6. No IACS specific contingency plan
7. Lack of configuration management policy
8. Lack of adequate access control policy
9. Inadequate incident detection and response plan and procedures
10. Lack of redundancy for critical components

Physical

1. Unauthorized personnel have physical access to equipment
2. Lack of backup power
3. Loss of environmental control
4. Unsecured physical ports

Architecture and Design

1. Inadequate incorporation of security into architecture and design
2. Insecure architecture allowed to evolve
3. Inadequate defined security perimeter
4. Control networks used for non-critical traffic
5. Control network services not within the control net
6. Inadequate collection of event history data

Configuration and Maintenance

1. Hardware, firmware, and software not under configuration management
2. OS and vendor software patches may not be developed until significantly after security vulnerabilities are found
3. OS and application security patches are not maintained, or vendor declines to patch vulnerability
4. Inadequate testing of security changes
5. Poor configurations are used

6. Critical configurations are not stored or backed up
7. Data unprotected on portable device
8. Password generation, use and protection not in accord with policy
9. Inadequate access controls applied
10. Malware protection not installed or up to date
11. Malware protection implemented without sufficient testing
12. Improper data linking
13. Denial of Service (DoS)
14. Intrusion detection/prevention software not installed
15. Logs not maintained

Software Development

1. Improper data validation
2. Installed security capabilities not enabled by default
3. Inadequate authentication, privileges, and access control in software

Communication and Network

1. Flow controls not employed
2. Firewalls nonexistent or improperly configured
3. Standard, well-documented communication protocols are used in plain text
4. Authentication of users, data or devices is substandard or nonexistent
5. Use of insecure industry wide IACS protocols
6. Lack of integrity checking for communications
7. Inadequate authentication between wireless clients and access points
8. Inadequate data protection between wireless clients and data points