

**{customer} OT Risk Assessment Template**

Table of Contents

[1.](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688907) Executive Summary 4

[2.](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688908) Introduction 5

[2.1](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688909) Background 5

[2.2](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688910) Purpose 5

[2.3](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688911) Scope 5

[3.](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688912) Risk Assessment Approach 6

[3.1](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688913) Review Methodology 6

[3.2](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688914) Participants 6

[3.3](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688915) Techniques Used 7

[4.](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688916) System Characterization 10

[4.1](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688917) Technology Components 10

[4.2](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688918) Physical Location 10

[4.3](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688919) Data Used By System 10

[4.4](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688920) Users 10

[4.5](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688921) Architecture Drawing 11

[4.5.1](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688922) Security Level Target; 11

[5.](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688923) Risk Score Definition 12

[5.1](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688924) Likelihood of Threat Event Initiation (Adversarial) 12

[5.2](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688925) Likelihood of Threat Event Occurrence (Non-adversarial) 12

[5.3](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688926) Assessment Scale – Impact of Threat Events 12

[5.4](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688927) Assessment Scale – Level of Risk 13

[5.5](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688928) Risk Matrics 14

[5.6](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688929) Impact Assessment and Analysis 14

[6.](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688930) Risk and Impact Model 16

[6.1](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688931) Risk Model 16

[6.2](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688932) Severity Analysis 16

[7.](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688933) Summary of Assessment 17

[7.1](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688934) Controls Domains 17

[8.](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688935) Summary of Observation 18

[8.1](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688936) Maturity Index 18

[9.](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688937) Potential Vulnerability and Threat 20

[9.1](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688938) Vulnerability Assessment 20

[9.2](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688939) Risk Assessment 20

[10.](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688940) Key Observation 21

[11.](../../../../../../../C:/Users/Oz/Desktop/Plant%20OT%20Risk%20Assessment%20Template%20V1.0%20-%20Copy%20(1).docx" \l "_Toc60688941) Maturity Score 22

1. Executive Summary
2. Introduction
   1. Background

Our organization was engaged by {customer} organization to perform Information Security Risk Assessment based on the ISO {isoVersion} & NIST and IEC 62443 framework. As a part of this process we performed a risk assessment exercise at location 1 and location 2 plants. The review was conducted between the period of {dateOfPerform}

* 1. Purpose

Describe the purpose of the risk assessment in context of the organization’s overall security program

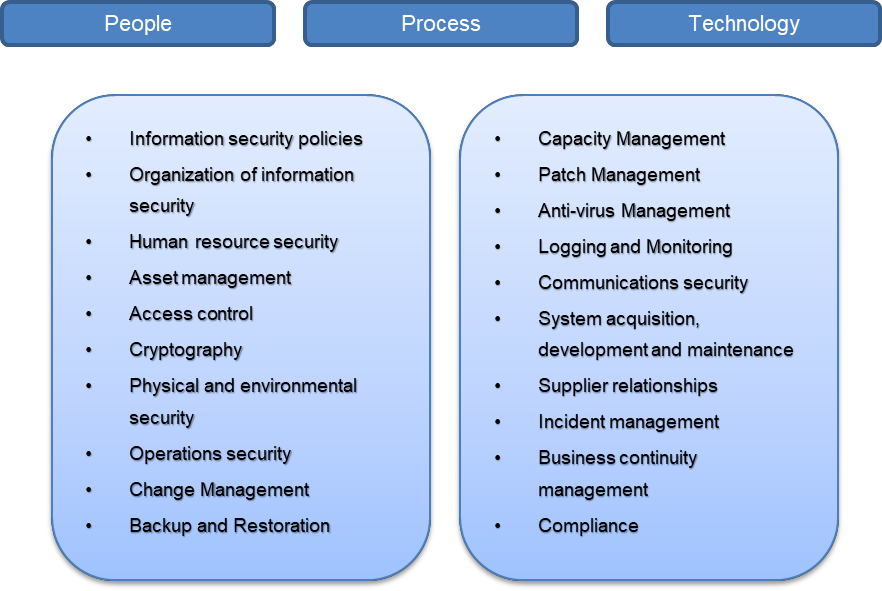
Example: This initial risk assessment was conducted to document areas where the selection and implementation of RMF controls may have left residual risk. This will provide security control assessors and authorizing officials an upfront risk profile

* 1. Scope

Scope of this Risk Assessment is to assess the risks in the OT devices such as Engineering Servers, HMI, Maintenance Servers, IO Servers, DA Servers, OT segmentation Firewall, Switches Routers and Network and provide key observation based industry standards framework

1. Risk Assessment Approach
   1. Review Methodology

Each of the 14 security domains were reviewed across the people, process and technology dimensions considering key XXXXX’s capabilities and areas of improvement, compared against NIST/IEC/ISO 27001, IT ACT, industry trends and leading practices.

The following provides a brief overview of the assessment and scoring model utilized throughout the project to identify key areas of improvement across the standard security domains:

We held discussions and reviewed policy and procedures at {customer} against the identified requirements to check test of design of these policy and procedure. Based on the discussions with the personnel and the records provided by them during the audit period, the status against each clause was evaluated.

* 1. Participants

|  |  |
| --- | --- |
| **Role** | **Participant** |
| System Owner | { systemOwner} |
| System Custodian | { systemCustodian} |
| Security Administrator | {securityAdministrator} |
| Network Manager | {NetworkManager} |
| Risk Assessment Team | {RiskAssessmentTeam} |
| Security Governing Body | {SecurityGoverningBody} |
| Security Awareness Trainers | {SecurityGoverningBody} |
| Business and Functional Managers | {BusinessFunctionalManagers} |
| Chief Information Officer | { ChiefInformationOfficer} |

* 1. Techniques Used

| **Step** | **Activity** | **Activity Description** | **Example** |
| --- | --- | --- | --- |
| Step - 1 | System Characterization | Characterizing an system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk | Hardware, Software, System interfaces (e.g., internal and external connectivity), Data and information, Persons who support and use the IT system, System mission (e.g., the processes performed by the IT system), System and data criticality (e.g., the system’s value or importance to an organization), System and data sensitivity |
| Step - 2 | Threat Identification | A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities, and existing controls | Natural Threats—Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events. Human Threats—Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information). Environmental Threats—Long-term power failure, pollution, chemicals, liquid leakage IT Related Threat - a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or purposeful, attempt to circumvent system security |
| Step - 3 | Vulnerability Identification | Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy. | Access control policies and procedures Third party access, Open ports |
| Step - 4 | Control Analysis | The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat’s exercising a system vulnerability | For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of harm |
| Step - 5 | Likelihood Determination | To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered: • Threat-source motivation and capability • Nature of the vulnerability • Existence and effectiveness of current controls | Likelihood is determined by using High, Low and Medium based on the risk score of each of the devices and identified risk in the device |
| Step - 6 | Impact Analysis | The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information: • System mission (e.g., the processes performed by the IT system) • System and data criticality (e.g., the system’s value or importance to an organization) • System and data sensitivity | An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization’s critical missions |
| Step - 7 | Risk Determination | The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of • The likelihood of a given threat-source’s attempting to exercise a given vulnerability • The magnitude of the impact should a threat-source successfully exercise the vulnerability • The adequacy of planned or existing security controls for reducing or eliminating risk. | Risk Description and Necessary Actions **High** - If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible. **Medium -** If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time. **Low -** If an observation is described as low risk, the system’s DAA must determine whether corrective actions are still required or decide to accept the risk. |
| Step - 8 | Control Recommendations | During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization’s operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level | The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks: • Effectiveness of recommended options (e.g., system compatibility) • Legislation and regulation • Organizational policy • Operational impact • Safety and reliability. |
| Step - 9 | Results Documentation | Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing | Risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation |

1. System Characterization
   1. Technology Components

|  |  |
| --- | --- |
| **Role** | **Participant** |
| System Owner |  |
| System Custodian |  |
| Security Administrator |  |
| Database Administrator |  |
| Network Manager |  |
| Risk Assessment Team |  |

* 1. Physical Location

|  |  |
| --- | --- |
| **Location** | **Plant Details** |
| Location – 1 | Plant details with respect to Production and capacity |
| Location – 2 | Plant details with respect to Production and capacity |
| Location – 3 | Plant details with respect to Production and capacity |
| Location – 4 | Plant details with respect to Production and capacity |
| Location – 5 | Plant details with respect to Production and capacity |
| Location – 6 | Plant details with respect to Production and capacity |

* 1. Data Used By System

|  |  |
| --- | --- |
| **Data** | **Description** |
| [Detail data elements included in scope] | [Describe characteristics of data elements] |

* 1. Users

|  |  |
| --- | --- |
| **Data** | **Description** |
| Include role based users list | Role and previllages of access and authentication |
| Remote Users |  |
| Third Party Users |  |
| Admin Users |  |
| Others |  |

* 1. Architecture Drawing



* + 1. Security Level Target;

|  |  |
| --- | --- |
| **Zone** | **Default Security Level Target** |
| Enterprise | 2 |
| DMZ | 3 |
| Operation Management | 3 |
| Supervisory Control | 4 |
| Basic Control | 4 |
| Safety | 4 |
| Remote | 4 |

1. Risk Score Definition

Risk score definition is taken from **NIST SP800-30** is used for evaluating risk and its impact;

* 1. Likelihood of Threat Event Initiation (Adversarial)

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualitative Values** | **Semi-Quantitative Values** | | **Description** |
| Very High | 96-100 | 10 | Adversary is **almost certain** to initiate the threat event. |
| High | 80-95 | 8 | Adversary is **highly likely** to initiate the threat event. |
| Moderate | 21-79 | 5 | Adversary is **somewhat likely** to initiate the threat event. |
| Low | 5-20 | 2 | Adversary is **unlikely** to initiate the threat event. |
| Very Low | 0-4 | 0 | Adversary is **highly unlikely** to initiate the threat event |

* 1. Likelihood of Threat Event Occurrence (Non-adversarial)

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualitative Values** | **Semi-Quantitative Values** | | **Description** |
| Very High | 96-100 | 10 | Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times per year**. |
| High | 80-95 | 8 | Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times per year**. |
| Moderate | 21-79 | 5 | Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times per year**. |
| Low | 5-20 | 2 | Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year,** but **more than once every 10 years**. |
| Very Low | 0-4 | 0 | Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**. |

* 1. Assessment Scale – Impact of Threat Events

| **Qualitative Values** | **Semi-Quantitative Values** | | **Description** |
| --- | --- | --- | --- |
| Very High | 96-100 | 10 | The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| High | 80-95 | 8 | The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries. |
| Moderate | 21-79 | 5 | The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries. |
| Low | 5-20 | 2 | The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. |
| Very Low | 0-4 | 0 | The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. |

* 1. Assessment Scale – Level of Risk

| **Qualitative Values** | **Semi-Quantitative Values** | | **Description** |
| --- | --- | --- | --- |
| Very High | 96-100 | 10 | Threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| High | 80-95 | 8 | Threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| Moderate | 21-79 | 5 | Threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| Low | 5-20 | 2 | Threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| Very Low | 0-4 | 0 | Threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |

* 1. Risk Matrics

Assessment of initial risk is often accomplished using a risk matrix that establishes the relationship between likelihood, impact, and risk. Risk matrixes are used to qualitatively establish the SL. Starting with a reasonable estimate of SL (or none at all), the cyber security risk is evaluated considering the countermeasures implied by the SL. If the risk is not acceptable, the Security Level is raised (i.e. additional countermeasures are added) until the cyber security risk is acceptable. The SL derived from this analysis becomes the Security Level ‐ Target.

| Risk Level | Risk Description |
| --- | --- |
| High | The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| Moderate | The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. |
| Low | The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. |

* 1. Impact Assessment and Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Likelihood** | **Level of Impact** | | | | |
| **Very Low** | **Low** | **Moderate** | **High** | **Very High** |
| **Very High** | Low | Moderate | High | Very High | Very High |
| **High Moderate** | Low | Moderate | Moderate | High | Very High |
| **Moderate** | Low | Low | Moderate | Moderate | High |
| **Low** | Very Low | Low | Low | Moderate | Moderate |
| **Very Low** | Very Low | Very Low | Low | Low | Low |



1. Risk and Impact Model
   1. Risk Model

Risk modelling is about modeling and quantification of risk. For the financial industry, the cases of credit-risk quantifying potential losses due, e.g., to production loss, or market-risks quantifying potential losses due to product quality or major equipment failure

Threat & adversary characteristics

Organization’s locale & sector

Network vulnerabilities detected

Mitigation controls installed

**X**

Assessment of the

damage caused by a

cyber‐attack, per zone

and network‐overall

**=**

Used by CISOs / stakeholders to assess the state of the network and the effectiveness of security measures

**Impact**

**Likelyhood**

**Risk**

* 1. Severity Analysis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Score | Severity | | |
|  | A | B | C |
| **Likelyhood** | **5** | High | High | Med-High |
| **4** | High | Med-High | Medium |
| **3** | Med-High | Medium | Med-Low |
| **2** | Medium | Med-Low | Low |
| **1** | Med-Low | Low | Low |

1. Summary of Assessment

The risk assessment was conducted based on the NIST SP800-30 and IEC 62443-1/2/3 and ISO 27001 for information security. Controls were reviewed across the people, process and technology dimensions considering key organization’s capabilities and areas of improvement, compared against industry trends and leading practices;

|  |  |
| --- | --- |
| **Control Category** | **Number of Controls Reviewed** |
| People | 12 |
| Process | 52 |
| Technology | 50 |
| Total Controls Reviewed | 114 |

* 1. Controls Domains

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Domain** | **Total Controls** | **Compliant** | **Non-Compliant** |
| Access control | 14 | 12 | 2 |
| Asset management | 10 | 6 | 4 |
| Communications security | 7 | 3 | 4 |
| Compliance | 8 | 4 | 4 |
| Cryptography | 2 | 1 | 1 |
| Human resource security | 6 | 5 | 1 |
| Business Continuity Management | 4 | 0 | 4 |
| Information security incident management | 7 | 0 | 7 |
| Information security policies | 2 | 0 | 2 |
| Operations security | 14 | 1 | 13 |
| Organization of information security | 7 | 3 | 4 |
| Physical and environmental security | 15 | 9 | 6 |
| Supplier relationships | 5 | 2 | 3 |
| System acquisition, development and maintenance | 13 | 8 | 5 |
| **Total** | **114** | **54** | **60** |

1. Summary of Observation

Here is the summary of observations based on the category;

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Category** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| **People** | **1** | **2** | **3** | **1** | **7** |
| **Process** | **1** | **10** | **9** | **2** | **22** |
| **Technology** | **2** | **6** | **11** | **3** | **22** |
| **Total Observations** | **4** | **18** | **23** | **6** | **51** |

* 1. Maturity Index

| **Domain** | **Total Controls** | **Compliant** | **Partial** | **NC** | **Maturity Index** |
| --- | --- | --- | --- | --- | --- |
| Access control | 14 | 12 | 2 | 0 | 4.29 |
| Asset management | 10 | 6 | 4 | 0 | 3.00 |
| Communications security | 7 | 3 | 4 | 0 | 2.14 |
| Compliance | 8 | 4 | 4 | 0 | 2.50 |
| Cryptography | 2 | 1 | 1 | 0 | 2.50 |
| Human resource security | 6 | 5 | 1 | 0 | 4.17 |
| Information security aspects of business continuity management | 4 | 0 | 2 | 2 | 0.00 |
| Information security incident management | 7 | 0 | 7 | 0 | 0.00 |
| Information security policies | 2 | 0 | 2 | 0 | 0.00 |
| Operations security | 14 | 1 | 12 | 1 | 0.36 |
| Organization of information security | 7 | 3 | 4 | 0 | 2.14 |
| Physical and environmental security | 15 | 9 | 6 | 0 | 3.00 |
| Supplier relationships | 5 | 2 | 3 | 0 | 2.00 |
| System acquisition, development and maintenance | 13 | 8 | 5 | 0 | 3.08 |
| **Total** | **114** | **54** | **57** | **3** | **2.37** |

1. Potential Vulnerability and Threat
   1. Vulnerability Assessment

Compile and list potential vulnerabilities applicable to the system assessed

|  |  |
| --- | --- |
| **Vulnerability** | **Description** |
| [List vulnerabilities] | [Describe vulnerability and its impact] |

* 1. Risk Assessment

Compile and list potential threats applicable to the system assessed

|  |  |
| --- | --- |
| **Threat Source** | **Description** |
| [List threat sources] | [List and/or describe actions that can be taken by threat source e.g., identity theft, spoofing, system intrusion] |

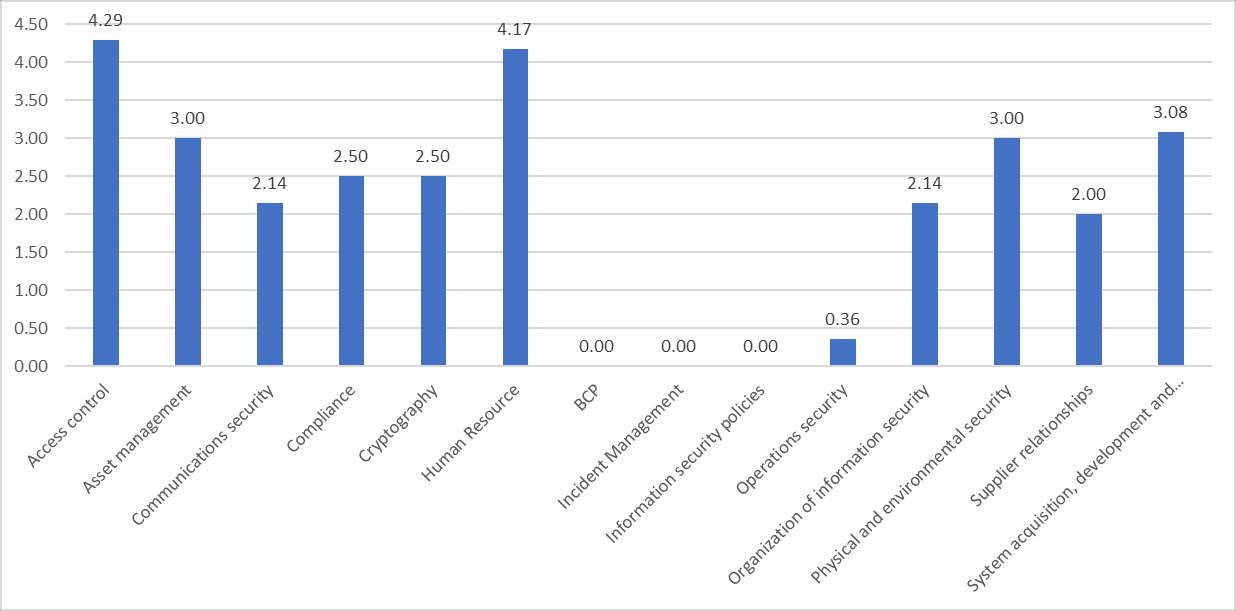
1. Key Observation

| **Risk Level** | **Observation** | **Category** | **Impact** | **Recommendation** |
| --- | --- | --- | --- | --- |
| **Critical** | It has been observed that some of the plant (project) laptops are used to connect directly to the PLC and HMI for updates and maintenance. These laptops are once again used to connect to open internet once outside the plant network. It has also been observed that there are no Antivirus installed in these laptops. Also, these laptops are provided with USB access. These laptops are also used for remote connectivity with OEM vendors. Further these laptops are not inventoried to the central asset database CMDB. | Technology | * Non-inventory of assets is a compliance breach to organizational asset management policy. * These laptops without adequate security controls and updates installed are vulnerable as they have open connectivity with internet. * PLC might get affected with the malicious code from the laptop thereby causing malfunction of the control logic embedded in the software * The open USB access can increase the risk of leakages, infect computers, PLCs controllers and can potentially cause plant networks to be compromised. * Untracked hardware or software presents a significant security risk to the plant environment. | Use a dedicated and hardened laptop solely for usage with PLC and restrict its usage to other activity. Ensure the antivirus definitions are periodically updated. Also, all these assets need to be included in Asset database and periodic reviews of logs and access needs to be done. |
| **Critical** | It has been observed that HMI touch screens have no provisions to auto lock during inactivity. | Technology | * This may lead to unauthorized access to controllers and PLCs resulting to security hazards, production loss and system malfunction. * Disgruntled employees having wrong intentions may tamper the production line or the product being manufactured | It is recommended that the service credentials for HMI be managed in a secure fashion to avoid any disclosure or abuse. Also, these credentials need to be reviewed and changed on a periodic basis. |
| **Critical** | It has been observed that though the organization chart is present but there is no detailed RASCI documented to clearly identify the activities to be performed by different business functions | People | * Each functional role in the process is assigned an expectation of responsibility, accountability, consultation or informing without which there is an Impact on effective and efficient resource management. * Also without a detailed RASCI there is a chance of conflict of interest and segregation of duties not performed diligently | To Align with business strategy and to meet the organization’s strategic objectives, a detailed org structure needs to be developed along with a detailed RASCI matrix to avoid unauthorized access and also to ensure that there is no conflict of interest. |

1. Maturity Score

The detailed results of benchmarking based on the ISO27001 standard and DSCI Controls, the method used to measure the maturity level for each security control domain, and the improvement recommendations are presented.

Maturity level is calculated based on the number of controls reviewed from ISO 27001 & DSCI and the control compliant status.



Overall Maturity Score is 2.37 out of 5

|  |  |  |
| --- | --- | --- |
| **Maturity Index** | **Maturity Level** | **Description** |
| 0 – 0.49 | 0 – Non-Existent | There is no recognition of the need for internal control. Processes  unpredictable, poorly controlled and reactive. |
| 0.51 – 1.50 | 1 – Initial / Adhoc | There is some recognition of the need for internal control. |
| 1.51 – 2.50 | 2 – Repeatable but Intuitive | Processes characterized and its often reactive. Controls are in process of  implementing and require documenting. |
| 2.51 – 3.50 | 3 – Defined Process | Controls are in place and are adequately documented. |
| 3.51 – 4.50 | 4 – Managed and Measurable | There is an effective internal control and risk management environment |
| 4.51 – 5.00 | 5 - Optimized | An organization wide risk and control program provides continuous and  effective control and risk mitigation. |