**Risk Assessment**

[Start by saving a copy of this assessment template](https://sectara.com/free-plan/)

The criteria in this document represent a notional security risk assessment
however the template can be adapted to any type of risk assessment.

**Prepared for**: [SRMBOK](https://www.srmbok.com/)

**Prepared by**: Julian Talbot

**Dated**: 9 February 2023

# DISCLAIMER

This document is based on information gathered by the assessor during the risk assessment process. Observations and recommendations are based upon the assumption that any documented and other forms of information provided to the assessor was complete, factual, accurate and relevant in the circumstances and that processes observed during any inspection activities were indicative of regular practice (unless indicated otherwise).

The intent of this document is to provide an independent perspective on risks included within the scope of the assessment. Recommendations must therefore be reviewed by a suitably authorized person to ensure that each is suitable and appropriate for the organisation.

# TERMS AND DEFINITIONS

| **Term** | **Definition** |
| --- | --- |
| **Asset** | An item, process, or other thing that an individual, organization or community values as important in achieving outcomes and objectives. |
| **Consequence** | The outcome of an event affecting objectives.The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage, or gain. There may be a range of possible outcomes associated with an event. |
| **Control** | Any measure that modifies risk.This can include existing physical, operational, logical, behavioral, institutional, or cultural mechanism by which a risk is managed (compare with ‘treatment’ definition). |
| **Criticality** | The importance or dependence that an organisation has on a person, function, process, item or infrastructure or specific facility. |
| **Event** | An occurrence or change of a particular set of circumstances. |
| **Hazard** | A potential cause of harm in the environment or from non-deliberate actions. |
| **Likelihood** | Likelihood is the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively. |
| **Risk** | The effect of uncertainty on objectives.  |
| **Source** | An element which alone or in combination has the potential to give rise to risk.  |
| **Threat** | A potential cause of harm initiated by a deliberate action. |
| **Threat Act** | An act committed by a Threat Actor. |
| **Threat Actor** | An individual, or group of individuals, that could cause harm to an organisation. For example, an insider, petty or serious criminal, issue motivated group or a terrorist. |
| **Treatment** | The implementation of a risk control that is designed to modify the likelihood or consequence of a risk event occurring. |
| **Vulnerability** | A weakness that can be exploited to make an asset susceptible to change. |

# TABLE OF CONTENTS

[DISCLAIMER 1](#_Toc126926480)

[TERMS AND DEFINITIONS 2](#_Toc126926481)

[TABLE OF CONTENTS 3](#_Toc126926482)

[EXECUTIVE SUMMARY 4](#_Toc126926483)

[SCOPE, CONTEXT AND CRITERIA 5](#_Toc126926484)

[Scope 6](#_Toc126926485)

[Context 6](#_Toc126926486)

[External Context 6](#_Toc126926487)

[Internal Context 7](#_Toc126926488)

[Risk Management Context 7](#_Toc126926489)

[Criteria 7](#_Toc126926490)

[ANNEX A: ASSET CRITICALITY ASSESSMENT 8](#_Toc126926491)

[ANNEX B: THREAT / HAZARD ASSESSMENT 9](#_Toc126926492)

[ANNEX C: CONTROLS ASSESSMENT 13](#_Toc126926493)

[ANNEX D: RISK REGISTER 19](#_Toc126926494)

[ANNEX E: ASSESSMENT METHODOLOGY 23](#_Toc126926495)

[Asset Criticality Assessment Criteria 23](#_Toc126926496)

[Threat Assessment Criteria 24](#_Toc126926497)

[Hazard Event Assessment Criteria 26](#_Toc126926498)

[Risk Control Effectiveness Assessment Criteria 27](#_Toc126926499)

[Risk Assessment Criteria 30](#_Toc126926500)

[ANNEX F: INTERVIEWS 33](#_Toc126926501)

[ANNEX G: LOCATIONS VISITED 34](#_Toc126926502)

[ANNEX H: DOCUMENTS REFERENCED 35](#_Toc126926503)

[ANNEX I: DETAILED TREATMENT PLANS 36](#_Toc126926504)

[Treatment 1: Server Access Protection 37](#_Toc126926505)

[Treatment 2: <Next risk treatment in the risk register> 39](#_Toc126926506)

# EXECUTIVE SUMMARY

MODIFY OR DELETE THIS SECTION IF IT IS NOT REQUIRED.

NoSuch Corporation LLC is a leading technology company that provides innovative solutions to its clients. The company's focus on technology and innovation has driven its growth and success, but it has also created a significant need for strong cybersecurity measures to protect sensitive information and assets.

The purpose of this security risk assessment is to identify and evaluate potential security risks to NoSuch Corporation LLC and to provide recommendations to mitigate these risks.

The scope of this assessment includes an evaluation of NoSuch Corporation LLC's current security practices and systems, including network security, access controls, physical security, and data security.

The assessment identified several areas of risk to NoSuch Corporation LLC's security, including:

* Inadequate access controls, which could allow unauthorized access to sensitive information and systems
* Poor physical security, which could allow unauthorized access to sensitive information and equipment
* Insufficient data security measures, which could allow sensitive information to be stolen or compromised
* Lack of network security, which could allow cyberattacks to compromise NoSuch Corporation LLC's systems and data.

Based on the findings of this assessment, NoSuch Corporation LLC is recommended to implement the following security measures:

* Implement strong access controls to prevent unauthorized access to sensitive information and systems
* Improve physical security to prevent unauthorized access to sensitive information and equipment
* Implement robust data security measures to protect sensitive information from theft or compromise
* Implement network security measures to prevent cyberattacks and protect NoSuch Corporation LLC's systems and data.

NoSuch Corporation LLC faces significant security risks that must be addressed in order to ensure the protection of sensitive information and assets. The recommendations outlined in this report provide a strong foundation for improving the company's security posture and reducing its risk of exposure to potential security threats.

# SCOPE, CONTEXT AND CRITERIA

In the ISO 31000 risk management process, establishing the scope, context, and criteria is an important step, as it helps to ensure that the risk management process is aligned with the organization's goals and objectives and considers the relevant risks and stakeholders.

Establishing these elements ensures that the organization's risk management process is effective and meaningful.



Figure : ISO31000 Risk Management Process

The following text is for guidance only and should be customized.

Additional resources include:

* ISO 31000:2018 Risk Management - Guidelines detail a best-practice approach for documenting this stage of the assessment - click [here](https://sectara.com/knowledge-base/scope-context-and-criteria/) for a summary of recommendations from the SECTARA Knowledge Base.
* HB167:2006 Security risk management handbook (HB167)
* [Security Risk Management Body of Knowledge](https://amzn.to/3DYuzQm) (SRMBOK)
* [Security Risk Management Aide-Mémoire](https://www.srmam.com/) (SRMAM) – available [here](https://srmam.fyi.to/available-on-amazon-websites)

For more great templates and free books visit [www.juliantalbot.com](http://www.juliantalbot.com)

## Scope

In the context of ISO 31000, the term "scope" refers to the boundaries and limitations of the risk management process, including the risks that will be considered and the specific activities or decisions that the risk management process will apply.

**Inclusions**

The scope of this Security Risk Assessment (SRA) incorporates all security-related threats and risks associated with the NoSuch Industrial Corporation LLC.

As part of the discovery process, a broad, representative group of stakeholders were engaged (Annex F), and several facilities were visited (Annex G).

**Exclusions**

The scope excludes Antarctica and issues associated with firearms

**Objectives of the risk assessment**

The objectives of this SRA are to inform and improved the security risk management framework in support of organizational objectives.

The SRA objectives are based on the four elements of their Security Risk Management Framework:

* **Governance**: Manage security risks and support a positive security culture in an appropriately mature manner ensuring clear lines of accountability, sound planning, investigation and response, assurance and review processes and proportionate reporting.
* **Information**: Maintain the confidentiality, integrity, and availability of information, intellectual property, and knowledge.
* **Cybersecurity**: Protect network-connected systems, including hardware, software, and data, from attack or unauthorized access through a combination of technologies, processes, and practices.
* **Personnel**: Ensure employees and contractors are suitable to access the business resources and meet an appropriate standard of integrity and honesty.
* **Physical**: Provide a safe and secure physical environment for people, information, & assets.

## Context

The term "context" refers to the broader environment in which the risk management process will take place, including the organization's goals and objectives, the risks that are relevant to the organization, and the stakeholders involved in the risk management process.

The risk management context refers to the specific goals and objectives of the risk management process and the criteria used to evaluate risks and determine the level of risk acceptable to the organization.

### External Context

The external context includes the factors and influences that are outside the organization's control, such as the economic, political, and social environment.

Start with a list of bullet points using the PESTLE mnemonic. To develop a narrative about the external context, develop a paragraph about each of the following.

* Political influences such as legislation, trade tariffs, and policy changes.
* Economic factors, both global and local.
* Social influences, expectations, trends, and demographics.
* Technological changes and implications.
* Legal environment and requirements for compliance, etc.
* Environmental factors such as pollution, climate change, stakeholder expectations, etc.

### Internal Context

The internal context includes the factors and influences within the organization's control, such as its culture, policies, and processes.

MORTAR is a helpful mnemonic that can help organizations consider the internal context in which they operate. MORTAR stands for Management systems, Organization, Resources, Technologies, Accountability, and Relationships. Start with a sentence or paragraph based on each of the following bullet points:

* Management systems: policies, procedures, processes,
* Organization: culture, objectives, vision, ethics
* Resources: capabilities, cashflow, people, property, information, intellectual property
* Technologies: robotics, information, communication,
* Accountability: structure, ownership, governance
* Relationships: stakeholders, interconnections, dependencies

### Risk Management Context

SWOT analysis can be a good place to start when documenting the risk management context. A few dot points about each of the following can build into four short paragraphs.

* Strengths of the organization
* Weaknesses of the organization
* Opportunities that may present themselves
* Threats to the achievement of objectives

## Criteria

‘Criteria’ refers to the standards or guidelines used to evaluate risks and determine the risk acceptable to the organization. These criteria can include factors such as the likelihood and potential impact of risks, the potential consequences of risks, and the organization's risk tolerance or appetite.

The timeframe for this risk assessment is the project's life, approximately x years.

The risk management criteria in this risk assessment (Annex E) are examples of a security risk management framework (SRMF) criteria. They should be customized to reflect your organization’s requirements and SRMF.

# ANNEX A: ASSET CRITICALITY ASSESSMENT

The following assets were identified as falling within the scope of the assessment. The categorization and criticality of each was also assessed to inform risk identification and treatment processes.

| **Asset Details**  | **Asset Category**  | **Criticality**  |
| --- | --- | --- |
| Reputation and Credibility | Reputation | VITAL |
| Cash, Budget, & Finances | Economic Assets | VITAL |
| Employees | People | VITAL |
| Information - Classified | Information | VITAL |
| Contractors | People | KEY |
| ICT Assets | Property | KEY |
| Buildings | Property | KEY |
| Intellectual Property | Information | KEY |
| Information - Commercial | Information | KEY |
| Equipment | Property | IMPORTANT |
| Information – Sensitive | Information | IMPORTANT |
| Personal items | Property | SUPPORTING |
| Vehicles | Property | SUPPORTING |
| Visitors | People | SUPPORTING |

**Table:** Asset Criticality Assessment

# ANNEX B: THREAT / HAZARD ASSESSMENT

The following sources of risk were assessed in support of risk identification and analysis.

| **Type** | **Actor / Hazard** | **Act / Event** | **Primary assets at Risk** | **Rating** |
| --- | --- | --- | --- | --- |
| Threat | **Cybercriminals** | Phishing/Spear Phishing attack |  |  |
| Identity theft |  |  |
| Hacking |  |  |
| Cyberstalking |  |  |
| Ransomware |  |  |
| DoS/DDoS attack |  |  |
| Man in the Middle attack |  |  |
| Password attack |  |  |
| Eavesdropping |  |  |
| XSS attack |  |  |
| Threat | **Issue Motivated Groups**  | Non-violent protest |  |  |
| Violent protest |  |  |
| Threat | **Petty Criminals** | Malicious damage |  |  |
| Disorderly conduct |  |  |
| Trespass |  |  |
| Break, enter and steal |  |  |
| Threat | **Serious & Organized Criminals** | Armed robbery | Cash, Budget, & FinancesContractorsVisitors | **Medium**ExpressedModerate |
| Assault |  |  |
| Arson |  |  |
| Kidnap |  |  |
| Hazard | **Economic Uncertainty** | Budget Allocation |  |  |
| Regulatory Changes |  |  |
| Currency Fluctuation |  |  |
| Threat | **State Intelligence Services** | Espionage | Information - ClassifiedInformation - Commercial |  |
| Human intelligence (HUMINT) |  |  |
| Cyber espionage |  |  |
| Technical surveillance |  |  |
| Physical surveillance |  |  |
| False flag operations |  |  |
| Deception operations |  |  |
| Covert operations |  |  |
| Threat | **Terrorists** | IED attack | Reputation and CredibilityVehiclesBuildingsContractorsVisitorsEmployees  | **High**CommittedDeveloped |
| Armed shooter attack |  |  |
| Vehicle ramming attack |  |  |
| Edged weapon attack |  |  |
| Hostage situation |  |  |
| Hazard | **Supply Chain** | Defective, sub-standard, or non-compliant security equipment |  |  |
| Critical security supplier failure |  |  |
| Non-delivery of security goods or services |  |  |
| Industrial action |  |  |

**Table:** Threat / Hazard Assessment

# ANNEX C: CONTROLS ASSESSMENT

Areas of vulnerability and the effectiveness of related risk controls were examined within the Controls Assessment stage; findings are documented within the table below, accompanied by Control Effectiveness ratings for each assessed control.

| **Controls** | **Control Comments** | **Rating** |
| --- | --- | --- |
| **Security Governance** |
| Security policies & procedures | To rate the control effectiveness of security policies and procedures based on their ability to provide secure and safe protection for their data and systems. Evaluation criteria for control effectiveness could include factors such as:* Policy: To what extent do the policies and procedures effectively address all security risks and threats
* Assurance: The extent to which the policies and procedures are effectively implemented and followed by all relevant parties
* Monitoring: The level of monitoring and enforcement of the policies and procedures

The overall rating should be the lowest of these three elements. It should also consider evidence regarding the level of success in preventing security incidents and protecting data and systems. | FAIR |
| Security Plan | - |  |
| Security risk management | - |  |
| Security risk assessments | - |  |
| Security appointments | - |  |
| Audit Processes | - |  |
| Business Continuity Management | - |  |
| Emergency Management | - |  |
| Crisis Management | - |  |
| Security reporting & investigations | - |  |
| Fraud & Corruption Management | - |  |
| Training | - |  |
| Training Needs Analysis (TNA) | - |  |
| Staff and contractor competency assessment and development | - |  |
| Security Alert Levels (Heightened Threat Procedures) | - |  |
| Travel approvals process | - |  |
| Travel briefings | - |  |
| **Personnel Security** |
| Security policies & procedures | When evaluating the effectiveness of security policies and procedures as a security control, it's important to consider the following factors:1. Relevance: Does the policy or procedure address the specific security needs and risks?
2. Clarity: Are the policies and procedures clearly written and easy to understand?
3. Implementation: Have the policies and procedures been effectively implemented and integrated into the organization's processes and systems?
4. Compliance: Are employees and stakeholders following the policies and procedures, and are they being enforced consistently?
5. Effectiveness: Are the policies and procedures reducing risk and improving the security of the organization's assets?
6. Review and update: Are the policies and procedures being regularly reviewed and updated to ensure they remain relevant and effective considering changing risks and technologies?
7. Communication: Have the policies and procedures been effectively communicated to all employees and stakeholders, and is there a mechanism for seeking feedback and addressing concerns?
8. Incident response: Have the policies and procedures been tested through simulated incidents and exercises, and have any gaps or weaknesses been identified and addressed?
9. Cost-effectiveness: Do the policies and procedures provide an appropriate level of security for the resources invested in their implementation and maintenance?

By considering these factors, you can determine whether your security policies and procedures are providing an effective and efficient level of security. |  |
| Pre-employment vetting | - |  |
| Suitability checking | - |  |
| Designated Security Assessed Positions | - |  |
| Security clearances | - |  |
| **Information** |
| Information classification management  | - |  |
| Information holdings inventory and audits | - |  |
| Intellectual property registration |  |  |
| Documents and records management systems | - |  |
| Technical Surveillance Countermeasures (TSCM) |  |  |
| **Cybersecurity** |
| Multi-factor authentication | - |  |
| Backup & recovery | - |  |
| Operating system patching | - |  |
| Security policies & procedures | - |  |
| Application whitelisting | - |  |
| Macro management | - |  |
| Application patching | - |  |
| Application hardening | - |  |
| System architecture specifications and monitoring |  |  |
| Administrative privilege restrictions | - |  |
| **Physical Security** |
| Fixed communication systems | - |  |
| CCTV | - |  |
| Signs | - |  |
| Access controls | - |  |
| Duress system | - |  |
| Crime Prevention Through Environmental Design (CPTED) | - |  |
| Lighting | - |  |
| Perimeter security | - |  |
| Lock & key management | - |  |
| Guard force | - |  |
| Intrusion Detection System | - |  |
| Portable communications systems | - |  |
| Metal detectors - handheld | - |  |
| Electronic counter measures (ECM) | - |  |
| Vehicle barriers | - |  |
| Explosive trace detection (ETD) | - |  |
| Metal detectors – walk through | - | EXCELLENT |
| X-ray screening devices | - | GOOD |
| Armored vehicles (EV) | - | FAIR |
| Pedestrian screening processes | - | POOR |
| Vehicle screening processes | - | NON-EXISTENT |

**Table:** Controls Assessment

# ANNEX D: RISK REGISTER

| **ID** | **Threats / Hazards** | **Primary Assets** | **Current Controls** | **Risk Description** | **Current Risk** | **Recommended Treatments** | **Residual Risk** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | Threat:**Terrorists**IED attack(High) | Reputation and Credibility (VITAL). Vehicles (SUPPORTING). Buildings (KEY). Contractors (KEY). Visitors (SUPPORTING). Employees (VITAL).  | Security policies & procedures. Security Plan. Security appointments. Security risk management. Audit Processes. Security reporting & investigations. Training. Training Needs Analysis (TNA). Security Alert Levels (Heightened Threat Procedures). Travel approvals process. Staff and contractor competency assessment. Security risk assessments.  |  | **High**4. LikelyMajor |  |  |
| 1 | Threat:**Serious & Organized Criminals**Armed robbery(Medium) | Cash, Budget, & Finances (VITAL). Contractors (KEY). Visitors (SUPPORTING). | Security policies & procedures. Security Plan.  | The acronym or C.A.S.E. considers the following four characteristics when analyzing a risk:* **Consequence** – what is the likely impact of this risk?
* **Asset** – what asset(s) are at risk?
* **Source** – What hazards or threat actors might lead to the risk manifesting?
* **Event** – what incident is being considered?

For example, Failure to protect information (Asset) in transit from theft (Event) by opportunistic criminal elements (Source) resulting in an adverse impact on reputation (Consequence). | **Medium**3. PossibleModerate | Every risk in the risk register should specify at least one risk treatment, even if the treatment is to accept the risk. And every risk treatment should have at least four elements:* **Appropriate** - Does it address the root cause identified in the risk?
* **Actionable** - Can you see the specific timeframes, actions, resources, and accountable person to tell you how to implement the treatment/recommendation?
* **Achievable** - What are the criteria, individual judgment, or milestones by which you will know that the recommendation has been actioned and is now complete?
* **Agreed** - Who were the relevant stakeholders who were consulted, and do they support this recommendation?

EXAMPLE: *After consultation with the Head of HR and Chief Security Officer (AGREED), the team recommends that external contractors selected by the CSO will update all servers to the current software version (ACHIEVABLE) within seven days (ACTIONABLE) and that the additional full-time staff be recruited by HR (APPROPRIATE) to commence within 30 days.* | **Low**2. UnlikelyMinor |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Table:** Risk Register

# ANNEX E: ASSESSMENT METHODOLOGY

The International Standard for assessing risks is ISO 31000:2018 Risk Management - Guidelines. Multiple standards extend on the generic methodology espoused within the standard when examining function-specific risks, such as those associated with health, safety, and security. Those standards articulate the way assets, sources of risk (threats and hazards) and control effectiveness should be considered initially and throughout the risk management process.

The methodology applied in completing this assessment was consistent with both ISO 31000 and those other recognized standards, and the following criteria was applied during the assessment process.

## Asset Criticality Assessment Criteria

| **Criticality Rating** | **Criteria** |
| --- | --- |
| VITAL | * Alternative services and/or facilities cannot be provided if asset is lost or severely damaged.
* Loss or compromise will result in abandonment or long-term cessation of the functions or core business practices.
* Loss or compromise will have a debilitating impact on the reputation of the organisation (international, permanent).
 |
| KEY | * Major restrictions to core business practices will result if asset is lost or severely damaged.
* Loss or compromise will result in long-term cessation/disruption of core business.
* Loss or compromise will have a major, widespread impact on the organisation’s reputation (national, sustained).
 |
| IMPORTANT | * Some minor restrictions to core business practices will result if asset is lost or severely damaged.
* Loss or compromise will result in short-term cessation/disruption of core business.
* Loss or compromise may have an impact on the organisation’s reputation (regional, short-term).
 |
| SUPPORTING | * Business as usual services and/or facilities can be provided if asset is lost or severely damaged.
* Loss or compromise will not result in cessation/disruption of core business.
* Loss or compromise will have no discernible impact on the organisation’s reputation.
 |

**Table:** Asset Criticality Assessment Criteria

## Threat Assessment Criteria

|  | **Intent** |
| --- | --- |
|  | **None** | **Implied** | **Expressed** | **Committed** | **Dedicated** |
| **Capability** | **Advanced** | Low | Medium | High | Extreme | Extreme |
| **Developed** | Low | Medium | High | High | Extreme |
| **Moderate** | Negligible | Low | Medium | High | High |
| **Emerging** | Negligible | Negligible | Low | Medium | High |
| **Undeveloped** | Negligible | Negligible | Negligible | Low | Medium |

**Table:** Threat Assessment Criteria

No entries were made within the Risk Register in relation to ratings for ‘Threat Acts’ that were assessed less than the Threat Tolerance threshold below, but these remain documented for future review.

|  |  |  |
| --- | --- | --- |
|  | Extreme | * Represents the highest level of risk and urgency for the organization
* Requires immediate and comprehensive countermeasures to mitigate the threat
* Threats at this level have the potential to cause severe harm, such as significant financial loss, operational disruption, or significant damage to the organization's reputation.
 |
|  | High | * Represents a significant level of risk that requires prompt attention
* Requires proactive countermeasures to prevent or minimize the impact of the threat
* Threats at this level have the potential to cause moderate harm, such as significant financial loss, operational disruption, or damage to the organization's reputation.
 |
| **SELECTED**:Threat Acts rated at this level (and higher) must appear within the Risk Register. | Medium | * Represents a moderate level of risk that requires attention
* Requires countermeasures to be implemented in a timely manner to prevent or minimize the impact of the threat
* Threats at this level have the potential to cause minor harm, such as minor financial loss, operational disruption, or damage to the organization's reputation.
 |
|  | Low | * Represents a low level of risk that requires minimal attention
* Requires minimal countermeasures to be implemented to prevent or minimize the impact of the threat
* Threats at this level have the potential to cause minor harm, such as minimal financial loss, operational disruption, or damage to the organization's reputation.
 |
|  | Negligible | * Represents a minimal or negligible level of risk
* Requires minimal or no countermeasures to be implemented
* Threats at this level have a minimal potential to cause harm to the organization.
 |

**Table:** Threat Tolerance Setting

| **Intent Rating** | **Intent Descriptor** |
| --- | --- |
| None | * No desire - absence of drive and purpose. Threat actor would not believe they have the capacity and competence to perpetrate the Threat Act.
 |
| Implied | * Some drive and commitment to achieve outcomes using generally peaceful means. Threat actor would believe they have limited capacity and competence to successfully perpetrating the Threat Act.
 |
| Expressed | * Highly motivated but with some flexibility in terms of method and capacity for compromise. Threat actor would have reasonable expectations of successfully perpetrating the Threat Act based on their capacity and competence.
 |
| Committed | * High degree of desire with limited room for compromise and potential to use extreme measures. Threat Actor competence and capabilities are such that they would have high expectations of successfully perpetrating the Threat Act.
 |
| Dedicated | * Extreme motivations with few if any limitations on perpetrating the Threat Act and no room for compromise. Threat actor would have a very high expectation of successfully perpetrating the Threat Act.
 |

**Table:** Threat Intent Criteria

| **Capability Rating** | **Capability Descriptor** |
| --- | --- |
| Advanced | * Fully funded and resourced. Highly skilled and comprehensively trained.
 |
| Developed | * Very skilled and trained in the use of tactics and techniques. Significant level of funding and/or resources.
 |
| Moderate | * Moderate level of financing and/or resources. Moderate level of training and skills.
 |
| Emerging | * Limited funding and/or resources. Limited knowledge and ability.
 |
| Undeveloped | * Few if any resources and/or funding. No knowledge or training.
 |

**Table:** Threat Capability Criteria

## Hazard Event Assessment Criteria

| **Event Rating** | **Criteria** |
| --- | --- |
| Critical | * Event would be of vigorous intensity.
* Event could materialize with minimal warning.
* Event would be prolonged.
* The event is within proximity.
* The event would be highly volatile.
* The event would be highly persistent.
 |
| Emerging | * Event would be of moderate Intensity.
* Event could materialize with manageable warning.
* Event would be of moderate duration.
* The event is within intermediate proximity.
* The event would be of medium volatility.
* The event would be moderately persistent.
 |
| Benign | * Event would be of low Intensity.
* Could materialize with ample warning.
* Event would be short-term.
* The event is distant.
* The event would be of low volatility.
* The event would not be persistent.
 |

**Table:** Hazard Event Assessment Criteria

No entries were made within the Risk Register in relation to ratings for ‘Events’ that were assessed less than the Hazard Event Tolerance threshold below, but these remain documented for future review.

|  |  |  |
| --- | --- | --- |
|  | Critical | Hazard events rated at this level must appear within the Risk Register. |
|  | Emerging | Hazard events rated at this level (and higher) must appear within the Risk Register. |
| Selected | Benign | Hazard events rated at this level (and higher) must appear within the Risk Register. |

**Table:** Hazard Event Tolerance Setting

## Risk Control Effectiveness Assessment Criteria

The effectiveness of current risk controls was assessed using the criteria below.

| **Rating** | **Criteria** |
| --- | --- |
| EXCELLENT | * Controls are properly designed and operating as intended. Management activities are effective in managing and mitigating risks.

POLICY CONTROL EFFECTIVENESS ASSESSMENT* Policies and procedures are robust, up to date, and have been through several iterations.
* Relevant standards and guidelines have been identified or created.
* The management framework is regularly reviewed, and any identified gaps are addressed within one review cycle.
* Documentation supporting the management system is controlled with accountabilities and review dates specified.

ASSURANCE FRAMEWORKS ASSESSMENT* Competency-based training is delivered is based on a comprehensive training program with >98% compliance.
* Training delivery and assessment records are comprehensive and current for all staff, contractors, and visitors.
* The training program is based on a current training needs analysis.
* Business plans specify budget and resource requirements and are based on documented analysis.
* Evidence shows that resources have been funded, and >98% are implemented within agreed timeframes.
* Exercise and training cycles are fully documented and integrated with >98% compliance.

COMPLIANCE AND FEEDBACK MECHANISMS* A structured audit plan addresses all elements of the management system.
* Audit schedules are risk-based and completed in >98% compliance with the plan.
* Recommendations from corrective action reports, audit findings and investigations are documented, and >98% of accepted actions are completed within agreed timeframes.
* Systems are mature, and continuous improvement processes have been in place for several years of review cycles.
 |
| GOOD | * Limited improvement is needed. Controls and/or management activities are properly designed and operating somewhat effectively, with some opportunities for improvement identified.

POLICY CONTROL EFFECTIVENESS ASSESSMENT* Core policies and procedures are current and have been through at least one review.
* Identified standards and guidelines support most procedures.
* The management framework is regularly reviewed and substantively completed.
* Documentation supporting the management system is controlled with accountabilities and review dates specified.

GUIDANCE FOR ASSURANCE FRAMEWORKS ASSESSMENT* Competency-based training and assessment are delivered per a comprehensive training program with >80% compliance.
* The training program is based on a current training needs analysis.
* Training records are current and comprehensive.
* Business plans specify budget and resource requirements.
* Evidence shows that resources have been funded, and most are in place.
* Communication plans are documented.

COMPLIANCE AND FEEDBACK* A structured audit plan addresses critical elements of the management system.
* Audit schedules are risk-based and completed in >80% compliance with the plan.
* Recommendations from corrective action reports, audit findings and investigations are documented, and >80% of accepted actions are completed within agreed timeframes.
* Systems are mature and have been in place for at least two review cycles.
 |
| FAIR | * Significant improvement is needed. Key controls and/or management activities are in place. However, significant opportunities for improvement were identified.

POLICY CONTROL EFFECTIVENESS ASSESSMENT* Policies and procedures are in place but may be partially documented and inconsistently applied.
* The management framework is in draft or incomplete.
* The management system is incomplete or outdated, but plans are in place to develop policies, procedures, and guidelines to address these deficiencies.
* Procedures and guidelines are in place but are inconsistent in format or content across business areas.

ASSURANCE FRAMEWORKS* Competency-based training is ad hoc or not fully documented.
* The training program is based on a training needs analysis that is out of date or greater than three years old.
* Business plans sometimes specify budget or resource requirements.
* Evidence is available to show that some resources have been funded, and >60% are in place.
* Communications are ad hoc, and plans are specified, but compliance is <50%.

COMPLIANCE AND FEEDBACK* An audit plan is evident but is not risk-based or does not address all areas.
* Audit schedules are completed in >60% compliance with the plan.
* More than 60% of corrective action reports, audit findings, and investigations are completed within agreed timeframes.
* Policies and procedures may be new, but at least one review cycle has occurred with approved systems and structures.
 |
| POOR | * Limited controls and/or management activities are in place, high level of risk remains. Controls and/or management activities are designed and somewhat ineffective in mitigating risk or driving efficiency.

POLICY CONTROL EFFECTIVENESS ASSESSMENT* Policies and procedures are not documented coherently.
* Action needs to be taken to review or update management documents of the framework.
* Review cycles are specified but are not complied with.

ASSURANCE FRAMEWORKS* Training is ad hoc, inconsistent, or not assessed.
* Training records are incomplete.
* Resources and budgets may be in place but are not documented in formal plans.
* Management controls are not formally communicated.

COMPLIANCE AND FEEDBACK* An audit plan is not evident or <60% compliance with the plan.
* Greater than 40% of continuous improvement activities (corrective action reports, audit findings, or investigations) are implemented within specified timeframes.
* At least one review cycle has occurred with >80% of existing Policies and procedures and structures.
 |
| NON-EXISTENT | * Controls and/or management activities are non-existent or have major deficiencies and do not operate as intended. Controls and/or management activities as designed are highly ineffective in mitigating risk or driving efficiency.

POLICY CONTROL EFFECTIVENESS ASSESSMENT* Policies and procedures are not documented, remain in the draft, or do not address the requirements of the indicator.
* Policies and procedures are reviewed but remain in draft for more than one review cycle.
* Review cycles are not specified.

ASSURANCE FRAMEWORKS* Evidence of assurance activities is limited or non-existent.
* Training, capability, communication, or logistics activities are ad hoc or non-existent.
* Training needs analysis is not evident.
* Resourcing plans and budgets do not reflect requirements.

COMPLIANCE AND FEEDBACK* Little or no evidence of continuous improvement.
* Audits are ad hoc, limited in scope, or non-existent.
* Feedback systems are not evident.
* No review cycles are evident.
 |

**Table:** Risk Control Effectiveness Assessment Criteria

## Risk Assessment Criteria

| Increasing Likelihood -> | **Likelihood Rating** | **Threat Information Descriptor** | **Threat Rating Descriptor** | **Historical Occurrences** | **Probability Descriptor** |
| --- | --- | --- | --- | --- | --- |
| **5. ALMOST CERTAIN** | There is credible and specific information to indicate that an event will occur. | Extreme | Has occurred on a regular basis in the organization during the timeframe being considered or circumstances are in train that will cause it to happen  | 90% or greater chance of occurrence. |
| **4. LIKELY** | There is credible and assessed information to indicate that an event is likely to occur. | High | Has occurred in the organization within 3 multiples of the timeframe being considered. | 65% up to 90% chance of occurrence. |
| **3. POSSIBLE** | There is plausible information to suggest that an event could occur. | Medium | Has occurred previously in the history of the organization in other similar organizations or circumstances | 35% up to 65% chance of occurrence.  |
| **2. UNLIKELY** | Information exists that an event might occur but is of low quality or quantity. | Low | Has never occurred in the organization but has occurred infrequently in other similar organizations. | 10% up to 35% chance of occurrence.  |
| **1. RARE** | There is limited chance of occurrence based on available evidence. | Negligible | Is possible but has not occurred to date in the organization or any similar organization. | <10% chance of occurrence.  |

**Table:** Risk Likelihood Criteria

|  | Increasing Consequence -> |
| --- | --- |
|  | Limited | Minor | Moderate | Major | Severe |
| Objectives | Minimal damage to people, information and assets or objectives. | Could be expected to cause minor damage to people, information and assets or objectives. | Could be expected to cause significant damage to people, information and assets or objectives. | Could be expected to cause serious damage to people, information and assets or objectives. | Could be expected to cause exceptionally grave damage to people, information and assets or objectives. |
| People | Could endanger or cause limited harm to a worker, associate, or client, including injuries that are not serious or life-threatening | Could lead to harm of a worker, associate, or client | Could lead to significant harm or injury to a worker, associate, or client | Could reasonably be expected to lead to life-threatening or serious injuries to multiple people or loss of 1 or 2 lives | Could lead directly to loss of life of three or more workers, associates, or clients |
| Information | Catastrophic compromise of sensitive or classified information pertaining to key organizational objectives | Major compromise of sensitive or classified information pertaining to key organizational objectives | Moderate compromise of sensitive or classified information | Minor compromise of sensitive information sensitive | Compromise of information otherwise available in the public domain |
|  Property  | Localized damage to property or assets | Minor damage to property, systems, or assets | Significant damage to property, systems, or assets | Extensive damage to property, systems or key assets that affects business continuity | Extensive and widespread damage to property, systems or key assets that affects business continuity |
|  Economic assets (cash & finances) | Impact would be less than 10% of budget or assets (per scope of the assessment) | 10% to 35% of budget or assets | 35% to 65% of budget or assets | 65% to 90% of budget or assets | Greater than 90% of budget or assets |
| Reputation | Limited short-term impact on reputation and status | Minor impact on reputation and status with some degradation of engagement/relations with partners, clients, and key stakeholders | Significant impact on reputation and status with degradation of engagement/ relations with partners, clients, and key stakeholders. Significant community/ media criticism and dissatisfaction | Major impact on reputation and status with serious longer-term degradation of engagement/relations with partners, clients, and key stakeholders. Serious community or media criticism and dissatisfaction | Loss of confidence in by the Government, partners, clients, and key stakeholders. Extreme community/media criticism and dissatisfaction |
| Capability | Cause limited delays or disruptions to operations or functions | Cause a loss of, or degradation of, a primary enabling service function for 24 hours | Cause a loss of, or major degradation of, one or more primary enabling service functions for 24-72 hours | Cause a loss of, or serious degradation of, one or more primary enabling service functions for more than three days | Cause a critical failure of capability resulting in a prolonged period of outage and/or inability to perform one or more of the agency’s key functions for an extended period |
| Compliance | Impedes compliance with operational policies or requirements, including protective security requirements | Infringement of or government requirement or policy | Breach of legislation or significant breach of or government requirement or policy | Major breach of legislation or government requirement or policy. A violation of security policy | Critical breach of legislation or government requirement or policy. A violation of security policy |

**Table:** Risk Consequence Criteria

|  | Limited | Minor | Moderate | Major | Severe |
| --- | --- | --- | --- | --- | --- |
| 5. Almost Certain | Medium | Medium | High | Very High | Very High |
| 4. Likely | Medium | Medium | High | High | Very High |
| 3. Possible | Low | Medium | Medium | High | High |
| 2. Unlikely | Low | Low | Medium | Medium | High |
| 1. Rare | Low | Low | Low | Medium | Medium |

**Table:** Risk Matrix

Once assessed, risks were then evaluated against thresholds within the table below and considered for treatment within the Risk Register.

| **Tolerance Level** | **Risk Rating** | **Risk Treatment Requirements** |
| --- | --- | --- |
|  | Very High | Immediate action by executive management and Board with detailed planning, allocation of resources, and monitoring. |
|  | High | Risk exceeds the organisation’s tolerance threshold and must be reduced. Senior management attention required. |
| Selected | Medium | Risk should be reduced if cost effective to do so. If not monitoring arrangements must be established and the risk must be reviewed periodically. Management attention required. |
|  | Low | Risk is within acceptable tolerances and should be managed by standard procedures and business practices but also monitored and reviewed for changes.  |

**Table:** Risk Tolerance Setting

# ANNEX F: INTERVIEWS

Enter list of persons interviewed and their roles or delete if not required.

# ANNEX G: LOCATIONS VISITED

Enter a list of sites and facilities visited or delete this section.

# ANNEX H: DOCUMENTS REFERENCED

Enter list of document and materials that inform this risk assessment here or delete if not required.

# ANNEX I: DETAILED TREATMENT PLANS

Treatments listed in the risk register are one sentence summaries. Risk treatments are described in sufficient detail in this section to provide the basis for the following:

* request for quotation (RFQ)
* business case for funding
* implementation of the risk treatment to a high standard commensurate with the relevant risks

## Treatment 1: Server Access Protection

|  |  |
| --- | --- |
| **Description** | Upgrade the server and network communications racks. |
| **Accountability** | CIO |
| **Actions** | Identify location of all servers and communications infrastructure such as routers which are not currently stored in compliance with organizational standards. This includes all secure comms including faxes, classified computing resources and telephones.Select and install server cabinets that designed to meet the specific needs of each location:* Physical Security: The server rack cabinets should be designed to prevent unauthorized access, including features such as lockable doors, pick-resistant keyed locks, and tamper-proof hinges.
* Cooling: Server racks should provide adequate ventilation and cooling to prevent overheating of the servers and other equipment.
* Cable Management: The cabinets should have a structured cable management system to organize and secure cables so that cables do not inhibit the secure closure and locking of cabinet doors.
* Accessibility: The cabinets should allow for easy access to the servers for maintenance, upgrades, and replacements. This may include features such as removable side panels, adjustable shelves, and cable cut-outs.
* Strength and Stability: The cabinets should be designed to support the weight of the servers and other equipment and be sturdy enough to prevent tipping or other structural failures.
* Power Distribution: The cabinets should have an integrated power distribution system to provide power to the servers and should include features such as surge protection and circuit breaker protection.
 |
| **Outputs** | Detailed report specifying all locations of servers and communications equipment including the type of server rack, key management equipment and processes, zoning certification of the area.Replacement of all non-compliant, damaged, or substandard server, router, and communications racks. |
| **Scope** | All network servers, routers, and communications hubs at NoSuch Corporation. |
| **Risks treated** | Refer to ***risks 1, 8, & 15*** from the risk register for additional guidance and specifications during design and implementation. |
| **Criteria** | 100% compliance for all servers and routers.All critical communications systems. |
| **Resources** | CIO Group plus outsourced providers |
| **Organisation** | CIO Group |
| **Quality and standards** | The cabinets should meet industry standards and regulations, such as those set by organizations like the Electronic Industries Alliance (EIA) and the National Electrical Manufacturers Association (NEMA).All server and communications rack should be locked at all times when not in use |
| **Achieved when** | Project outputs are completed and signed off by CIO. |
| **Notes:** | Key safes with two factor authentication and auditable electronic access logs should be fitted at all locations that have a server or router rack.Hazards such as flammable items (e.g.: cardboard boxes, non-essential equipment, spare cables), liquids, and hand tools should be removed from co-location to server and comms racks.Area managers, ICT staff, and security staff should be trained to understand the importance and correct application of security protocols such as key storage and registration, housekeeping inspections, and server access management. |

## Treatment 2: <Next risk treatment in the risk register>

|  |  |
| --- | --- |
| **Description** | <Copy this template and insert details as required> |
| **Accountability** |  |
| **Actions** |  |
| **Outputs** |  |
| **Scope** |  |
| **Risks treated** |  |
| **Criteria** |  |
| **Resources** |  |
| **Organisation** |  |
| **Quality and standards** |  |
| **Achieved when** |  |
| **Notes:** |  |