|  |  |
| --- | --- |
| **Risk Threat Analysis, Assessment and Mitigation Plan** | **No. [Organization] IS-28** |
|  | **Effective Date:** October 23, 2023 |

# **Overview**

# A Risk Assessment is required to be conducted and then reviewed annually by top management in nearly every industry, critical infrastructure, and government agency. A Risk Assessment is required by nearly all Cybersecurity Frameworks, and state and federal regulations.

# **Purpose**

The purpose of the risk assessment is to systematically identify and assess cyber security risk to the organization’s strategy, operations, brand, reputation, assets, and resources. The path to improving the cyber security program begins by first determining current strengths and vulnerabilities. In the end, an effective risk assessment will identify information assets, estimate the value of those information assets based on their importance to the organization, identify internal and external threats and vulnerabilities to the organization, estimate the likelihood of an attack and impact if the information asset is no longer available or severely damaged and assign risk ownership.

# **Scope**

This policy document provides the [Organization] Risk Assessment Policy statements and commitment to develop, implement, maintain a Risk Assessment Policy, conduct annual risk and security assessments on all [Organization] information systems to help understand and identify all current threats, vulnerabilities and gaps within their process that may create critical risks availability, confidentiality and integrity for information systems and data of which the [Organization] is considered the owner.

# **Responsibilities**

All covered personnel that are included in the organization’srisk assessment activities are responsible for adhering to this policy and with any local Risk Assessment requirements.

|  |  |
| --- | --- |
| **Role** | **Definition** |
| **Senior**  **Management** | Senior [Organization] Management, the Chief Information Security Officer (CISO) are responsible for the sponsorship and support of the Risk Management Plan and process, participating on the Risk Management Team, the review and approval of risk assessments and control recommendations and reporting to the [Organization] what mitigation actions have been taken. |
| **[Organization] Chief Risk Officer** | The [Organization] Risk Officer as delegated by the [Organization] is assigned the responsibility for the continued development, implementation, and maintenance of the risk management program. |
| **Risk**  **Management** | The [Organization] Risk Officer is responsible for governing the overall Security and Risk Management process, reviews presented Risk Assessment Reports and approves risk treatment plans or recommended controls. |
| **Security Liaisons** | Security Liaisons are responsible for conducting risk assessments, analyzing the risk and recommends controls, presenting risks for approval, documenting the process, and managing and facilitating the implementation of recommended controls. |
| **System Owner / Administrator** | System Owners/Administrators are responsible for participating in the identification and analysis process, participating on the Risk Management Team and for the implementation of technical controls. |

All [Organization] information assets must meet the required security controls defined in this policy document that are based on the NIST Cybersecurity Framework. [Organization] shall manage risks appropriately. Risk management includes the identification, analysis, and management of risks associated with an [Organization]’s information technology infrastructure, the information itself, and physical security to protect the [Organization]’s information technology assets and vital functions:

1. The risk management program must identify and classify risks and implement risk mitigation as appropriate.
2. The program must include the identification, classification, prioritization, and mitigation processes necessary to sustain the operational continuity of mission critical information technology systems and resources.
3. In general, “risk” is defined as a condition or action that may adversely affect the outcome of a planned activity. Some types of risk are as follows:

* 1. Organizational risk – The direct or indirect loss resulting from one or more of the following:
     1. Inadequate or failed internal processes.
     2. People
     3. Systems or external events
  2. IT risk – The loss of an automated system, network or other critical information technology resource that would adversely affect processes.
  3. Legal risk – Parameters established by legislative mandates, federal and state regulations, policy directives and executive orders that impact delivery of program services.
  4. Reputational risk – General estimation, by the public, on how [Organization] services are delivered (integrity, credibility, trust, customer satisfaction, image, media relations, political involvement).
  5. Citizen Services risk – Program services mandated by charter, legislation, or policy that provides for the delivery of State of Ohio business (education, human services, highways, law enforcement, health and safety, unemployment benefits, vital records, etc.).

To meet the [Organization] requirement to complete an annual risk and security assessment of their critical systems and infrastructure and that there are ongoing processes in place to assess the current posture of the environment. The Monitoring Plan is designed to ensure that the [Organization] uses one or a combination of assessment methods identified below:

1. Third Party Independent Assessment
2. Self-Assessment

The [Organization] must complete a risk and security assessment annually per NEOLA policy 8305.

Within 30 days of completion of an assessment, the [Organization] is required to the senior management team.

1. Accurate reporting on the status of corrective actions
2. Development of a process to evaluate supporting documentation and the time to monitor recommendations.

The [Organization] has adopted the Risk Assessment security principles established in NIST “Risk Assessment” control guidelines as the official policy for this security domain. The following subsections in this document outline the Risk Assessment requirements that the [Organization] must implement and maintain to be compliant with this policy. This policy shall be reviewed annually.

# **Risk Management Program Activities**

The Risk Management program at a minimum shall focus on the following four types of activities:

1. **Identification of Risks**: A continuous effort to identify which risks are likely to affect business continuity and security functions and documenting their characteristics.
2. **Analysis of Risks**: An estimation of the probability, impact, and timeframe of the risks, classification into sets of related risks, and prioritization of risks relative to each other.
3. **Mitigation Planning**: Decisions and actions that will reduce the impact of risks, limit the probability of their occurrence, or improve the response to a risk occurrence. For moderate or high rated risks, mitigation plans should be developed, documented, and assigned to managers. Plans should include assigned manager’s signatures.
4. **Tracking and Controlling Risks**: Collection and reporting of status information about risks and their mitigation plans, response to changes in risks over time, and management oversight of corrective measures taken in accordance with the mitigation plan.

**Business Continuity Risk Management Processes:**

For business continuity risk management, the focus of risk management is an impact analysis for those risk outcomes that disrupt the [Organization] organization. The [Organization] should identify the potential impacts to develop the strategies and justify the resources required to provide appropriate level of continuity initiatives and programs. The [Organization] should conduct organizational risk impact analysis activities that include the following:

Define the [Organization]’s critical functions and services.

1. Define the resources (technology, staff, and facilities) that support each critical function or service.
2. Identify key relationships and interdependencies among the [Organization]’s critical resources, functions, and services.
3. Estimate the decline in effectiveness over time of each critical function or service
4. Estimate the maximum elapsed time that a critical function or service can be inoperable without a catastrophic impact
5. Estimate the maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service
6. Estimate financial losses over time of each critical function or service.
7. Estimate tangible (non-financial) impacts over time of each critical function or service
8. Estimate intangible impacts over time of each critical function or service.
9. Document any critical events or services that are time-sensitive or predictable and require a higher- than-normal priority
10. Identify any critical non-electronic media required to support the [Organization]’s critical functions or services
11. Identify any interim or workaround procedures that exist for the [Organization]’s critical functions or services.
12. Assess the professional capability of third parties and ensure that they provide adequate contact with the [Organization] and meet the [Organization]’s Recovery Time Objective and Recovery Point Objective requirements. Review dependence on third parties and take actions to mitigate risk.
13. Provide direction on synchronization between any manual work data and the automated systems that occur during a recovery period.

**Security Risk Process**

The focus of security risk management is an assessment of those security risk outcomes that may jeopardize [Organization] assets and vital functions or services. The [Organization] should identify those impacts to develop the strategies and justify the resources required to provide the appropriate level of prevention and response. It is important to use the results of risk assessment to protect critical [Organization] functions and services in the event of a security incident. The lack of appropriate security measures would jeopardize [Organization] critical functions and services. Security risk impact analysis activities include the following:

1. Identification of the Federal, State, and Local regulatory or legal requirements that address the security, confidentiality, and privacy requirements for [Organization] functions or services.
2. Identification of confidential information stored in the [Organization]’s files and the potential for fraud, misuse, or other illegal activity.
3. Identification of essential access control mechanisms used for requests, authorization, and access approval in support of critical [Organization] functions and services.
4. Identification of the processes used to monitor and report to management on whatever applications, tools, and technologies the [Organization] has implemented to adequately manage the risk as defined by the [Organization] (i.e., baseline security reviews, review of logs, use of IDs, logging events for forensics, etc.).
5. Identification of [Organization]’s IT Change Management and Vulnerability Assessment processes.
6. Identification of security mechanisms in place to conceal [Organization] data (Encryption, PKI, etc.).

# **Security Categorization**

[Organization] must address the following requirements:

1. Categorization of information and the information system in accordance with applicable State and Federal laws, policies, regulations, standards, and guidance. NIST SP 800-60 Volumes 1 and 2 serves as a guidance for the categorization process. The security categories are based on the potential impact on an [Organization] should certain events occur that jeopardize the confidentiality, integrity, and availability of the information and information systems needed by the [Organization] to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day to-day functions, and protect individuals. The impact on the organization, personnel, and other external entities must be considered during the security categorization process.
2. System Owners need to be involved with the security categorization of an information system if they are responsible for:
   * 1. Any interconnected system dependencies, i.e., systems that share information.
   1. A system that may inherit a security control from their respective system
3. Include the security categorization process as a part of the System Development Life Cycle (SDLC). The security categorizations shall be developed early in the initiation stage ensuring the planning and implementation of the appropriate security controls throughout the SDLC
4. Ensure the security categorization decision is reviewed and approved by the authorized or designated representative
5. Update documents to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments
6. The System Owner and supporting security liaison must assist with the development of the security categorization

Information includes all data, regardless of physical form or characteristics, made or received in connection with the transaction by the [Organization]. The [Organization]’s information shall be classified and handled in a manner that protects the information from unauthorized or accidental disclosure, modification, or loss. [Organization] must use the Data Governance Policy for detailed requirements for the storage, labeling, classification, and destruction of [Organization] data.

# **Risk Assessment**

Risk assessments take into account risks posed to the [Organization] operations and assets, or individuals from external parties, including but not limited to entities such as Service providers; Contractors operating information systems on behalf of the [Organization]; Individuals accessing the [Organization] data and information systems; and Outsourcing organizations.

The [Organization] must conduct security/risk assessments to evaluate the level of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores, or transmits.

The [Organization] shall conduct security/risk assessments at minimum annually, or whenever there are significant changes to the critical information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

An [Organization] third-party assessment of all critical systems (Restricted or Highly Restricted) and associated security controls will be conducted at a minimum annually.

1. All assessment results will be provided to the OHCRRO within thirty (30) days of completion.
2. The risk assessment must consider risks posed to [Organization]’s operations, assets, or individuals from external parties, including but not limited to the following:

* 1. Organizations such as foreign nations and others that may have an interest in information supplied to the [Organization].
  2. Service Providers:
     1. Contractors operating information systems on behalf of the [Organization]
     2. Individuals accessing the [Organization]’s information systems.
     3. Outsourcing entities (e.g. Cloud Service Providers (CSPs))
        1. [Organization] need to obtain prior approval from the OhCR CISO before contracting with cloud-hosted solutions or off-site hosting.
        2. [Organization] must ensure vendor compliance with OhCR security policies and obtain a Vendor Readiness Assessment Report (VRAR) from the vendor prior to contract approval.
        3. [Organization] shall ensure that contract language requires vendors to provide as attestation to their compliance, an industry recognized, third party assessment report. Examples of acceptable attestation reports include Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2 and ISO 27001.
        4. Procurement language must also require, in addition to initial validation, cloud/vendor must annually provide the [Organization] validation of their continued compliance to [Organization] policies and procedures. This requirement includes all vendors supporting Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and/or Software as a Service (SaaS). Examples of acceptable assessment reports include.
        5. Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2 and ISO 27001. CSPs must demonstrate to the [Organization] that continuous monitoring activities are in place and compliance is being met.

1. When planning and budgeting for security/risk assessments, the [Organization] must follow these requirements:
2. Multi-year planning and budgeting techniques must be used.
3. Annual assessments must be included in information system budgets and planning.
4. Other significant, planned activities must be considered in budgets and planning (e.g., life cycle activities, enhancements, audits) to ensure cost effective use of resources.
5. All information systems in the [Organization] must be considered to ensure resource efficiencies.
6. Assessments must be coordinated between information systems with security control inheritance and other relational dependencies.
7. [Organization] shall conduct an assessment using NIST 800-53 controls that includes at a minimum their critical systems shall be done.
8. An [Organization] may perform an annual self-assessment of their organization or system if they are storing, processing, or transmitting data that is classified as low or medium. An independent third-party assessment shall be completed every three years for systems storing, processing, or transmitting data classified as medium.
9. If an [Organization] or system stores, processes, or transmits data classified as highly restricted, the [Organization] shall use an independent assessor to conduct the annual assessment.
10. An independent assessor or assessment team shall assess the security controls in the information system using an OHCRRO provided assessment template.

1. A Plan of Action and Milestones (POAAM) or Corrective Action Plan (CAP) for the system documenting the planned, remedial actions to correct weaknesses or deficiencies in security controls and to reduce or eliminate known vulnerabilities must be developed.
2. The existing POAAM or CAP must be updated weekly based on findings of weaknesses including, but not limited to, the following:
3. Reviews, tests, audits, or assessments
4. Security impact analyses
5. Independent verification and validation findings
6. Continuous monitoring activities
7. Incidents
8. All findings, recommendations, and their source must be tracked to the related item in the POAAM or CAP.
9. Findings must be analyzed as to their level of risk (i.e., high, medium, low) and a determination must be made for appropriate action(s) to be taken to correct or mitigate, as appropriate, the identified weaknesses to an acceptable level of risk.
10. One or more tasks to remediate a finding must be documented in the POAAM or CAP for any of the following:
11. Critical-level risks that are not remediated within 7 days.
12. High-level risks that are not corrected within 21 days.
13. Medium-level risks that are not corrected within 30 days.
14. Low level risks as required by the [Organization] CISO and that are not corrected within 90 days
15. f. All findings must be entered into a Corrective Action Plan (CAP).

# **Risk Assessment/Analysis**

Risk assessment or analysis is the act of determining the probability that a risk will occur and the impact that event would have if it does occur. This analyzes the cause and effect of each possible event. Once risks have been identified and documented, risk analysis must be performed. During the risk analysis process, each potential risk event will be evaluated for the following:

1. The probability that the risk will occur.
2. The impact of the risk if it occurs.

These two factors of assessing the risk involving probability and impact shall be measured for probability using a scale of Low, Medium, and High, and giving each an associated number.

For impact, the [Organization] shall use a qualitative method for analysis as it is typically a quicker and usually more cost-effective way to analysis risks. Analysis will be performed with the goal of gathering data on the following:

1. The likelihood of the risk occurring
2. The qualitative impact on the company, system, or data
3. The quality of the risk data being utilized

Risk Analysis of each system shall be utilized to assist in impact determination.

# **Risk Assessment Process**

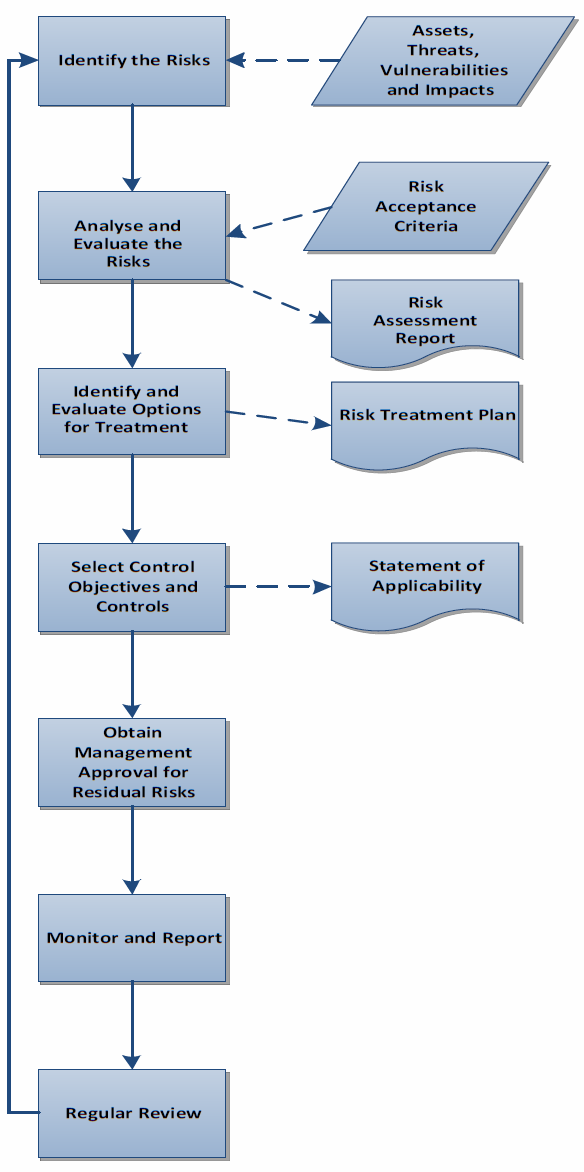
Risk is the happening of an unwanted event, or the non-happening of a wanted event, which affects a business in an adverse way. Risk is realized when:

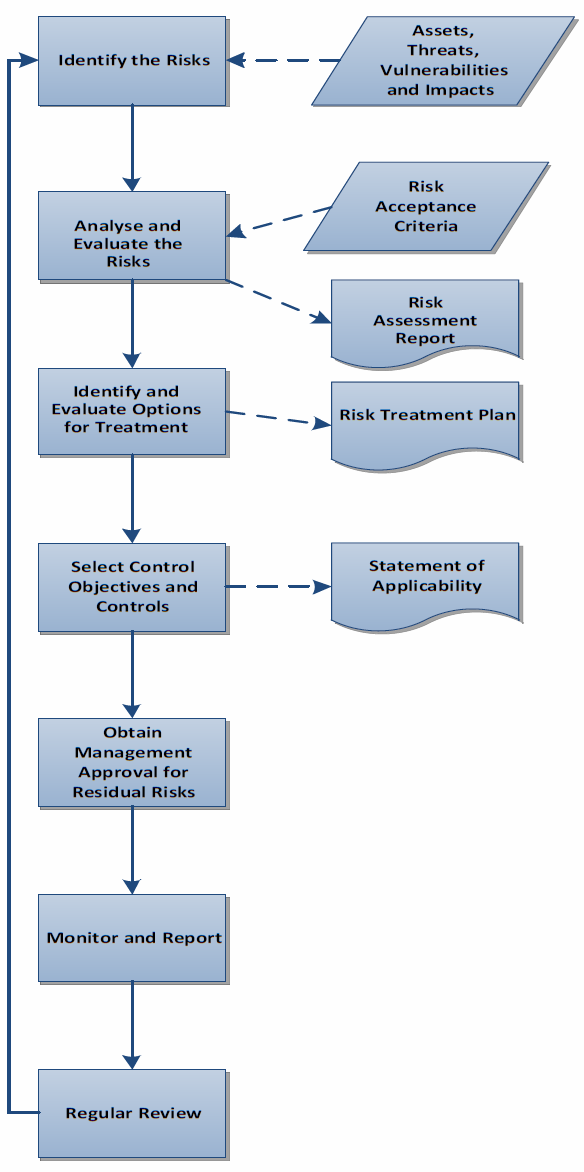
* The objectives of the business are not achieved.
* The assets of the business are not safeguarded from loss.
* There is non-compliance with organization policies and procedures or external legislation and regulation.
* The resources of the business are not utilized in an efficient and effective manner.
* The confidentiality, integrity and availability of information is not reliable.

It is important that [Organization] has an effective risk management process in place to ensure that potential impacts do not become real, or if they do, that contingencies are in place to deal with them.

# **Process Diagram**

The risk management process is shown in the following diagram:





***Fig 1 Risk Management Process***

# **Identification of Risks**

The process of identifying risks will consist of the following steps in line with the requirements of NIST and ISO/IEC 27001.

# **Assets**

A full inventory of assets will be compiled and maintained by [Organization]. The definition of an asset is taken to be “anything that has value to the organization” and is therefore worthy of protection. This will include physical assets such as IT servers and operational machinery as well as information assets such as customer lists and application databases.

# **Threats**

For each asset, the threats that could be reasonably expected to apply to it will be identified. These will vary according to the type of asset and could be accidental events such as fire, flood or vehicle impact or malicious attacks such as viruses, theft or sabotage.

# **Vulnerabilities**

Circumstances which may be capitalized on by any specific threat will be detailed. Examples of such vulnerabilities may include a lack of patching on servers (which could be exploited by the threat of hacking) or the existence of paper files in a data center (which could be exploited by the threat of fire).

# **Impacts**

Finally, an estimate of the impact that the loss of confidentiality, integrity or availability could have on the asset should be given.

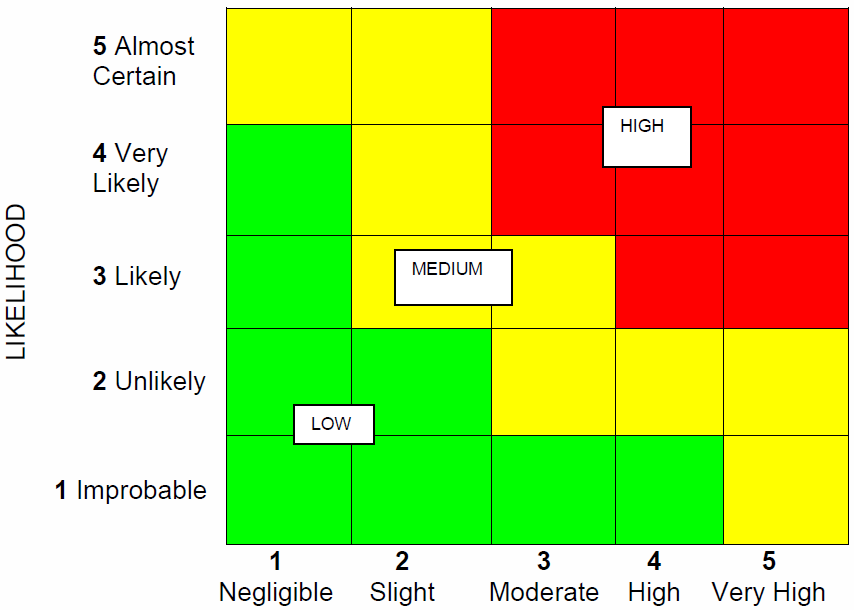
# **Risk Analysis and Evaluation**

# **Numerical Classification**

To assess the risk to an asset and determine the appropriate treatment, [Organization] will examine the threats, vulnerabilities, the likelihood that the threat will take place and the impact of it should it occur. A 5-point scale will be used to describe the likelihood of a risk-taking place and also to describe the impact that it is likely to have.

The 5-point scale for the likelihood ranges from 1=improbable to 5=almost certain; the 5-point scale for the impact ranges from 1=negligible to 5=very high. The risk matrix shown below illustrates the scales and allows us to prioritize our risks so that they can be managed more effectively.

The risk classification used will be the score obtained from multiplying the likelihood that the risk will occur and the impact it is likely to have. Both scales range from 1 to 5, so the minimum score will be 1 and the maximum score will be 25 as shown in the matrix below:



IMPACT

**Fig 2 Risk Matrix Chart**

Each risk will be allocated a classification based on its score as follows:

HIGH –12 or more

MEDIUM – 5 to 11 inclusive

LOW – 1 to 4 inclusive

The rationale for indicating the likelihood and impact ratings awarded will be given so that these can be assessed at a later date to see if they have materially changed. This will also assist in ensuring consistency and repeatability in risk assessments.

# **Risk Acceptance Criteria**

The matrix in Figure 2 shows the classifications of risk, where green indicates an acceptable threshold as the likelihood is minimal or/and the impact is minimal. The yellow indicates that the risk threshold is medium as the risk is larger as is the impact; so containing those risks is more important than addressing those in the green. The red area indicates the risks that are of the highest priority as both the impact and risk are relatively high, so measures to contain them must be of the highest priority and, if they cannot be reduced then countermeasures must be in place for these risks.

The overall intention of the risk assessment and proposed treatments is to reduce the classification of the risks to an acceptable level e.g. HIGH down to MEDIUM or MEDIUM down to LOW. This is not always possible as sometimes although the score is reduced, it remains in the same classification e.g. reducing the score from 8 to 6 means it still remains a MEDIUM level risk. The organization may decide to accept these risks even though they remain at MEDIUM rating.

The priorities of the items in the Continual Improvement Plan are determined by the highest priority of the Risk Assessment items addressed e.g. if three items are addressed by a single action and one is MEDIUM and two LOW, then the priority of the action will be MEDIUM.

# **Risk Assessment Report**

The output from the Risk Analysis and Evaluation stage is the Risk Assessment Report. This shows the following information:

* Assets
* Threats
* Vulnerabilities
* Controls currently implemented.
* Likelihood (Including rationale)
* Impact (Including rationale)
* Score
* Classification
* Whether the risk is accepted or needs treatment

This report is input to the Risk Treatment stage of the process and must be signed off by management before continuing.

# **Risk Treatment**

For those risks that are judged to be above the threshold for acceptance by [Organization], the options for treatment will then be explored.

# **Risk Treatment Options**

The following options may be applied to the treatment of the identified unacceptable risks:

* Apply appropriate controls to lessen the likelihood and/or impact of the risk.
* Avoid the risk by taking action that means it no longer applies.
* Transfer the risk to another party e.g., insurer or supplier.

Judgement will be used in the decision as to which course of action to follow, based on a sound knowledge of the circumstances surrounding the risk e.g.

* Business Strategy
* Regulatory and legislative considerations
* Technical issues
* Commercial and contractual issues

The Risk Manager will ensure that all parties who have an interest or bearing on the treatment of the risk are consulted.

# **Risk Treatment Plan**

The evaluation of the treatment options will result in the production of the Risk Treatment Plan which will detail:

* Risks above the acceptance threshold.
* Assets affected.
* Recommended treatment option.
* Control Requirements

This document will be input to the next stage in the process where controls will be selected to meet the identified requirements.

# **Selection of Controls**

Appropriate controls will be identified to address the risk treatment requirements highlighted as part of the risk assessment exercise.

The Statement of Applicability document will set out those controls that have been selected and the reasons for their selection. It will also detail those that have been implemented and identify any that have been explicitly excluded together with a reason for such exclusion.

# **Management Approval**

At each stage of the risk assessment process management will be kept informed of progress and decisions made, including formal signoff of the proposed residual risks. Management will approve the following documents:

* Risk Assessment Report
* Risk Treatment Plan
* Statement of Applicability (SoA)

Signoff will be indicated according to [Organization] documentation standards.

# **Risk Monitoring and Reporting**

As part of the implementation of new controls and the maintenance of existing ones, key performance indicators will be identified which will allow the measurement of the success of the controls in addressing the relevant risks.

These indicators will be identified which will allow the measurement of the success of the controls in addressing the relevant risks.

These indicators will be reported on a regular basis and trend information produced so that exception situations can be identified and dealt with by management.

# **Regular Review**

In addition to a full annual review, risk assessments will be evaluated on a regular basis to ensure that they remain current and the applied controls valid. The relevant risk assessments will also be reviewed upon major changes to the business such as office moves, mergers and acquisitions or introduction or new or changed IT services.

# **Roles and Responsibilities**

Within the process of risk assessment there are a number of key roles that play a part in ensuring that all risks are identified, addressed and managed. These roles are shown on the RACI table below, together with their relative responsibilities at each stage of the process.

# **RACI Chart**

The table below clarifies the responsibilities at each step using the RACI model, i.e.:

­R=Responsible A=Accountable C=Consulted I=Informed

|  |  |  |  |
| --- | --- | --- | --- |
| **Role:** | **Business Continuity Manager** | **Business Management** | **Operational Staff** |
| **Step** |
| Identify the risks | A/R | C | C |
| Risk Acceptance Criteria | C | A/R | C |
| Analyze and Evaluate the Risks | A/R | C | C |
| Identify and Evaluate Options for Treatment | A/R | C | C |
| Select Control Objectives and Controls | A/R | C | C |
| Obtain Management Approval for Residual Risks | A | R | C |
| Monitor and Report | A/R | I | C |
| Regular Review | A/R | C | C |

Further roles and responsibilities may be added to the above table as the Risk Assessment Process matures within [Organization].

By following this process, [Organization] will ensure that the risks faced in the day-to-day operation of its business are effectively managed and controlled.

# **List of Typical Threats**

The following list may be used as a starting point for creating a relevant list of threats which may apply to the information assets identified in the inventory.

| **Threat Category** | **Threat** | **Example** |
| --- | --- | --- |
| Human | Malicious outsider | Someone launches a denial-of-service attack on your ecommerce website |
|  | Malicious insider | An employee or trusted third party accesses information in an unauthorized manner from inside your network |
|  | Loss of key personnel | One or more people with key skills or knowledge are unavailable perhaps due to extended sickness |
|  | Human error | An employee accidentally deletes the customer database |
|  | Accidental loss | A manager loses a memory stick with customer bank details on it |
| Natural | Fire | Your main office burns down due to an electrical fault |
|  | Flood | The nearby river breaks its banks, and your main office is severely flooded |
|  | Severe weather | No-one can get into the office due to the weather |
|  | Earthquake | The area of your main office is affected by an earth tremor that damages all your servers |
|  | Lightning | All your servers are fried by a lightning strike on the data center building |
| Technical | Hardware failure | A key server has a processor failure |
|  | Software failure | Your financial system processes invoices incorrectly due to a bug |
|  | Virus/Malicious code | A virus spreads throughout your network preventing access to your data |
| Physical | Sabotage | A disgruntled ex-employee takes an axe to your server room |
|  | Theft | You come in on Monday morning to find all your PC's have been stolen |
|  | Arson | Someone with a grudge against your organization starts a fire during the night |
| Environmental | Hazardous waste | A lorry carrying hazardous waste has an accident outside your office |
|  | Power failure | The sub-station supplying your area has a meltdown |
|  | Gas supply failure | There is a suspected leak, and all supplies are turned off |
| Operational | Process error | Your new data transfer procedure doesn't cater for unexpected circumstances and data is lost or sent to the wrong destination |
|  | Crime scene | A crime happens in or near your office and the area is sealed off by police |

## **Risk Response**

For each identified risk, a response must be identified. The Security Liaison will select a risk response for each risk. The probability and impact of the risk will be the basis of recommending which actions should be taken to mitigate the risk. During response planning, strategies and plans are developed to minimize the effects of the risk to a point where the risk can be controlled and managed.

Avoid: Risk avoidance involves changing aspects of the overall process or system architecture to eliminate the threat.

**Transfer:** Risk transference involves shifting the negative impact of a threat (and ownership of the response) to a third party. Risk transference does not eliminate a threat it simply makes another party responsible for managing it. This would include identifying avenues of insurance, etc.

**Mitigate:** Risk mitigation involves reducing the probability and/or the impact of risk threat to an acceptable level. Taking early and pro-active action against a risk is often more effective than attempting to repair the damage a realized risk has caused. Developing contingency plans are examples of risk mitigation.

**Accept:** Risk acceptance should normally only be taken for low-priority risks. All risks should have a recommendation of control(s) and / or alternative solutions to mitigate risk.

|  |  |
| --- | --- |
| **Risk Level** | **Risk Description and Necessary Actions** |
| **High** | Mandatory need for corrective measures. CAP must be in place for 60 days. |
| **Medium** | Plans must be developed to mitigate corrective measures within 90 – 120 days. |
| **Low** | Decision on whether to implement corrective measures or accept the risk. |

## **Use of Independent Assessors**

When assessments must be conducted by an entity with an explicitly determined degree of independence to the organization, independence must be determined by the [Organization] CISO based on the security categorization of the information system and/or the risk to [Organization] operations and assets, and to individuals.

To make an informed, risk-based decision, the selection of independent assessors must consider the following criteria to ensure credibility of the security assessment results and to receive the most objective information possible. Preserving the impartial and unbiased nature of the assessment process including, but not limited to, freedom from any perceived or actual conflicts of interest with respect to the following:

1. The development, operation, and/or management of the information system
2. The chain of command associated with the information system.
3. The determination of security control effectiveness
4. A competitive relationship with any organization associated with the information system being assessed or impacts on their reputations
5. Undue influence because of a contractual or other related relationship
6. The assessor’s technical expertise and knowledge of State and federal requirements

# **5**. **Policy Compliance**

* 1. **Compliance Measurement**

The [Organization] management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, tool reports, internal and external audits, and feedback to the policy owner.

* 1. **Exceptions**

Any exception to the policy must be approved by the [Organization] IT team in advance.

* 1. **Non-Compliance**

An end user found to have violated this policy may be subject to disciplinary action, up to and including termination of appointment to the [Organization].

# **Related Standards, Policies and Processes**

Data Governance Policy

# **Definitions and Terms**

None

# **Revision History**

|  |  |  |
| --- | --- | --- |
| Date of Change | Responsible | Summary of Change |
| October 23, 2023 | [Organization] | Created initial draft |
|  |  |  |