# Security Risk Governance Responsibilities & RACI Template

# Introduction: How to Use This Template

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

This document is meant to outline the organizational risk governance responsibilities. This includes the responsibilities of the board of directors, senior management, the IT security team, and other major stakeholders.

Use this document to establish expectations for how the different groups will evaluate and mitigate against security risks and to determine how identified risks can be escalated.

# High-Level Responsibilities

## Risk Executive

Senior leaders/executives, in consultation and collaboration with the senior security steering committee, will define the organizational risk frame, including the types of risk decisions supported (e.g. risk responses), how and under what conditions risk is assessed to support those decisions, and how risk is monitored (e.g. to what level of detail, in what form, and with what frequency).

The risk executive as a function coordinates across organization leaders to:

* Establish risk management roles and responsibilities.
* Develop common understanding of the organization’s approach to risk management.
* Delegate risk decision-making functions to various roles within the organization by specifying the scope of risk-based decisions and when to escalate.
* Promote collaboration among risk decision-making roles to include information security sign-offs.
* Act as the primary group to evaluate risks and make associated decisions, including escalation to the board if needed.

The risk executive will meet monthly [update frequency to your preference] to perform their above responsibilities.

The primary members of the risk executive function are:

* Senior leadership and executives
* Senior security steering committee
  + Chief information officer
  + Chief information security officer
  + Chief risk officer
  + Chief legal officer
  + VP of audit and compliance
  + VP of human resources
  + VP of finance

The risk executive provides common risk management resources for:

* Senior leaders/executives
* Mission/business owners
* Chief information officers
* Chief information security officers
  + Information system owners
  + Common control providers
  + Enterprise architects
  + Information security architects

## Board of Directors

The board will actively manage and assess major risks for the organization, including cybersecurity risks and any risks that have been escalated by the risk executive. In addition, the board will delegate responsibility to management to complete strategic risk actions based on the established risk tolerance level.

The board of directors will be responsible for:

* Reviewing findings from the risk executive regarding information security risk.
* Determining strategic risk mitigation actions to be completed, as appropriate.
* Delegating responsibilities to management to complete certain goals and/or actions.
* Determining the risk tolerance in conjunction with the risk executive.
* Acting as the highest authority when it comes to risk management decisions.

The board will meet quarterly [update frequency to your preference] to manage these risks.

[Include or delete the following statement based on organizational ability:] When assembling the board, include one member who has some background in information security and can bring that expertise to the organization.

The members of the board of directors are:

* CEO
* [Insert other names/positions]
* [Insert other names/positions]
* [Insert other names/positions]
* [Insert other names/positions]

## IT Security Team

The IT security team will actively monitor and identify risks. This group will remediate most low-level risks and will escalate higher-level risks to the risk executive and/or board of directors. In addition, the IT security team will act as the internal subject matter experts on cybersecurity when discussing information security risks.

The IT security team will be responsible for:

* Monitoring security technologies for potential incidents, vulnerabilities, and other risks on a daily basis.
* Escalating identified security risks to the risk executive.
* Mitigating against security risks based on the decisions made by the risk executive and/or board of directors.
* Acting as a knowledgebase to communicate security risks to non-technical personnel, including those within the risk executive and/or board of directors.

The IT security team will meet weekly [update frequency to your preference] to identify risks and determine which will need to be escalated.

The IT security team members include:

* CISO
* [Insert other names/positions of IT and/or IT security staff]
* [Insert other names/positions of IT and/or IT security staff]
* [Insert other names/positions of IT and/or IT security staff]
* [Insert other names/positions of IT and/or IT security staff]
* [Insert other names/positions of IT and/or IT security staff]

## Escalation of risks

Larger and more impactful risks will have to be escalated to higher-level groups for guidance. The process will be as follows:

* The IT security team regularly monitors for most risks through the use of security technologies, threat intelligence feeds, and other relevant sources.
* The IT security team will escalate risks to the risk executive if the risk is perceived to be larger than the established threshold.
* The risk executive will evaluate the risk and make the appropriate risk decision.
* The risk executive will escalate risks to the board of directors if the risk is perceived to be larger than the established threshold.
* The board of directors will have the final decision-making responsibility on major risks to the organization.

The thresholds to escalate risks are described in the table below:

[Customize the below table with the thresholds specific to your risk governance structure.]

|  |  |
| --- | --- |
| **Risk Governance Group** | **Threshold** |
| IT Security Group | All risks will be evaluated. |
| Risk Executive | All risks with a moderate impact (one of functional, informational, or recoverability) will be evaluated. |
| Board of Directors | All risks with a high impact (one of functional, information, or recoverability) will be evaluated. |

## RACI Chart

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Board of Directors** | **CEO** | **CFO** | **VP, IT** | **Information Owners (Business Directors/VP)** | **CISO** | **Manager, Security & Compliance** | **IT Security Team** | **All Employees & Contractors** |
| Define the risk tolerance level | A | R | C | C | C | R | C | C | I |
| Identify and monitor for risks | I | I | - | C | I | A | R | R | I |
| Perform comprehensive system-wide risk assessments | A | C | - | C | - | R | R | C | - |
| Perform per-project or initiative-based risk assessments | I | I | - | C | C | A | I | C | - |
| Evaluate and identify risk actions | I | I | I | C | C | A | I | R | - |
| Approve and fund risk actions | C | A | R | I | I | C | - | - | - |
| Accept risk | A | R | C | C | I | C | I | I | I |
| Manage and maintain risk register/inventory | I | I | I | I | I | A | R | C | - |

Legend:

A – Accountable

R – Responsible

C – Consulted

I – Informed

# Risk Tolerance Impact and Frequency Thresholds

Document any frequency or impact thresholds for your organization. These are specific characteristics that would trigger you to take action (or not) regardless of any other risk factors.

**Upper Frequency Threshold:**

* In the event that a risk scenario results in a high-enough frequency, [Insert Company’s Name] will choose to always mitigate that risk regardless of the potential impact.
* Any risk scenario calculated to have a higher frequency than [Insert Company’s frequency thresholds, e.g. weekly] will always be mitigated.

**Lower Frequency Threshold:**

* In the event that a risk scenario results in a low-enough frequency, [Insert Company’s Name] will choose to never mitigate that risk regardless of the potential impact.
* Any risk scenario calculated to have a lower frequency than [Insert Company’s frequency thresholds, e.g. never] will never be mitigated.

**Upper Impact Threshold:**

* In the event that a risk scenario results in a high-enough impact, [Insert Company’s Name] will choose to always mitigate that risk regardless of the frequency of that risk occurring.
* Any risk scenario calculated to have a higher impact than [insert Company’s impact thresholds, e.g. high functional impact] will always be mitigated.

**Lower Impact Threshold:**

* In the event that a risk scenario results in a low-enough impact, [Insert Company’s Name] will choose to never mitigate that risk regardless of the frequency of that risk occurring.
* Any risk scenario calculated to have a lower impact than [insert Company’s impact thresholds, e.g. low functional, information and recoverable impact] will never be mitigated.

# Risk Tolerance Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.