Risk Management Policy

|  |  |
| --- | --- |
| **Company** | Guatemaltek |
| **Version** | 1.0 |
| **Effective Date** | 2026-01-01 |
| **Review Schedule** | Annually |
| **Responsible Officer** | CISO |

# Purpose

Establishes systematic approach to identifying, assessing, treating, and monitoring information security risks.

# Scope

All Guatemaltek information assets, systems, processes, and business operations.

# Policy

## Risk Management Framework

* Annual comprehensive risk assessment
* Ongoing risk identification for new systems/processes
* Consider threats: cyber attacks, natural disasters, human error, system failures
* Consider vulnerabilities in people, processes, technology
* Likelihood: Rare, Unlikely, Possible, Likely, Almost Certain
* Impact: Negligible, Minor, Moderate, Major, Severe
* Risk Level = Likelihood × Impact

Impact → Negligible | Minor | Moderate | Major | Severe

Likelihood ↓

Almost Certain: Medium | High | High |Critical|Critical

Likely: Low | Medium| High | High |Critical

Possible: Low | Medium| Medium | High | High

Unlikely: Low | Low | Medium |Medium | High

Rare: Low | Low | Low |Medium |Medium

* Mitigate: Implement controls to reduce risk (preferred)
* Transfer: Insurance, outsourcing (for high-impact risks)
* Avoid: Eliminate the activity causing risk
* Accept: Document acceptance by executive management (rare)
* Monitor and review regularly
* Mitigate if cost-effective
* Accept with documentation
* Quarterly risk register review
* Annual comprehensive reassessment
* Continuous monitoring of control effectiveness
* Update after significant changes or incidents

## Risk Register

CISO maintains risk register containing:

* Risk description
* Likelihood and impact ratings
* Current controls
* Risk level (residual)
* Treatment plan
* Owner
* Review date

## Roles & Responsibilities

* Overall risk management program
* Facilitate risk assessments
* Maintain risk register
* Report to executive management
* Implement technical risk controls
* Monitor control effectiveness
* Report new risks
* Report potential risks
* Comply with risk controls
* Support risk assessments

## Risk Reporting

* Quarterly: Risk dashboard to executive management
* Annually: Comprehensive risk report to board
* Immediately: Critical/high risks to CISO

# Compliance

Approved: CISO | 2026-01-01 | Next Review: 2027-01-01