CGEIT Certification Study Notes

Code: cgeit

IT Governance

Domain 1: Corporate IT Governance (26%)

IT Governance Framework

Strategic Alignment

Ensure IT risk management supports and enables enterprise strategy and objectives

Value Delivery

Optimize IT risk investments to deliver measurable business value

Risk Appetite

Define acceptable risk levels aligned with organizational tolerance and capacity

Resource Management

Allocate adequate resources for IT risk management activities

Performance Measurement

Monitor governance effectiveness through KPIs, KRIs, and KGIs

Line	Role	Responsibilities
First Line	Operational Management	Own and manage risks day-to-day, implement controls
Second Line	Risk & Compliance Functions	Oversee risk management, set policies, monitor compliance
Third Line	Internal Audit	Independent assurance, evaluate effectiveness of governance

Governance Roles

Role	Primary Responsibility	Accountability
Board of Directors	Risk oversight and governance direction	Ultimate accountability for risk
Risk Committee	Risk appetite and tolerance decisions	Strategic risk oversight
CRO / CISO	Risk program leadership and reporting	Program implementation
Risk Manager	Day-to-day risk operations	Tactical risk execution

Risk Culture & Policy

- Risk Culture: Shared values and behaviors that shape how risk is perceived and managed
- Risk Policy: Formal statement defining the organization's approach to IT risk management
- Risk Appetite Statement: Board-approved declaration of acceptable risk levels
- Risk Tolerance: Acceptable variation from risk appetite thresholds
- Regulatory Compliance: Alignment with industry regulations and legal requirements

Governance Maturity

Initial (Ad Hoc)

Risk management is reactive and unstructured

Repeatable

Basic risk processes exist but are not standardized

Defined

Risk management processes are documented and standardized

Managed

Risk metrics are used, processes are measured and controlled

Optimized

Continuous improvement, proactive risk management

Risk Assessment Process

- Asset Identification: Identify and classify IT and information assets by criticality
- Threat Assessment: Identify internal and external threats to IT infrastructure
- Vulnerability Assessment: Identify weaknesses in systems, processes, and controls
- Impact Analysis: Determine potential business impact of risk scenarios
- Likelihood Estimation: Assess probability of threat occurrence
- Risk Calculation: Analyze risk based on likelihood × impact to prioritize response

Risk Scenario Development

Threat Source

Internal, external, natural, or environmental threat actors

Threat Event

Specific action or occurrence exploiting a vulnerability

Vulnerability

Weakness in asset, control, or process that can be exploited

Asset at Risk

IT resource, data, or capability that could be impacted

Business Impact

Financial, operational, reputational, or regulatory consequence

Method	Description	When to Use
Quantitative	Uses numerical values: ALE = ARO × SLE	When monetary values are needed for decisions
Qualitative	Uses descriptive scales (High/Medium/Low)	Quick assessments, broad risk comparison
Semi-quantitative	Assigns numbers to qualitative ratings	Balances rigor with practicality
Bow-Tie Analysis	Visual diagram of causes and consequences	Complex risk scenario analysis

Key Risk Formulas

- **SLE** (Single Loss Expectancy) = Asset Value × Exposure Factor
- **ALE** (Annual Loss Expectancy) = SLE × ARO (Annual Rate of Occurrence)
- **Risk** = Threat × Vulnerability × Impact
- **Residual Risk** = Inherent Risk - Control Effectiveness
- **Risk Register**: Central repository documenting all identified risks

Emerging Risk Identification

- Technology risks: Cloud, IoT, AI, blockchain, quantum computing
- Threat intelligence: Monitoring evolving cyber threat landscape
- Regulatory changes: New compliance requirements (GDPR, CCPA, etc.)

Risk Response

Domain 3: Risk Response and Reporting (23%)

Risk Response Options

Option	Description	When to Use
Mitigate	Implement controls to reduce risk to acceptable level	When cost-effective controls are available
Transfer	Shift risk to a third party (insurance, outsourcing)	When risk exceeds internal capacity
Avoid	Eliminate the activity causing the risk	When risk greatly exceeds acceptable levels
Accept	Acknowledge and monitor the risk	When risk is within appetite and tolerance

Control Design & Implementation

Preventive Controls

Stop incidents before they occur (access controls, encryption)

Detective Controls

Identify incidents when they happen (monitoring, logging, IDS)

Corrective Controls

Restore operations after incidents (backups, patches, DR)

Compensating Controls

Alternative controls when primary ones aren't feasible

Key Risk Indicators (KRIs)

- Leading indicators: Predict future risk levels before they materialize
- Lagging indicators: Measure risk impact after events have occurred
- Thresholds: Define green/yellow/red levels for KRI monitoring
- Escalation: Automated alerts when KRI thresholds are breached
- Reporting cadence: Regular KRI dashboard updates for stakeholders

Risk Reporting & Communication

Audience	Report Type	Frequency
Board/Risk Committee	Executive risk dashboard, risk heat maps	Quarterly

Audience	Report Type	Frequency
External Stakeholders	Compliance reports, audit findings	As required

Risk Acceptance Best Practices

- Document risk acceptance with clear business justification
- Ensure appropriate authority level approves risk acceptance
- Set expiration date for risk acceptance decisions
- Monitor accepted risks for changes in threat landscape
- Review and re-validate risk acceptances periodically

IT Security

Domain 4: Information Technology and Security (24%)

Security Architecture

Defense in Depth

Multiple layers of security controls to protect IT assets

Zero Trust

Never trust, always verify — regardless of network location

Least Privilege

Separation of Duties

Identity & Access Management

- Authentication: Verify user identity (MFA, biometrics, certificates)
- Authorization: Grant appropriate access based on role and need
- Accounting: Log and monitor all access activities
- Provisioning: Automate user account lifecycle management
- Privileged Access Management: Control and monitor admin accounts

Cloud Security

Model	Customer Responsibility	Provider Responsibility
IaaS	OS, middleware, apps, data	Hardware, networking, hypervisor
PaaS	Applications, data, user access	OS, middleware, runtime, infrastructure
SaaS	Data, user access, configuration	Everything else — full stack

Business Continuity & DR

BIA

RTO

Recovery Point Objective — maximum acceptable data loss

Maximum Tolerable Period of Disruption before severe harm

⚠ Vulnerability & Incident Management

- Vulnerability scanning: Regular assessment of systems for weaknesses
- Patch management: Timely application of security updates
- Penetration testing: Simulated attacks to validate control effectiveness
- Incident response: Preparation, detection, containment, eradication, recovery
- Digital forensics: Evidence collection and chain of custody

Exam Tips

CGEIT Exam Preparation Tips

⚠ Exam Focus Areas

- Focus on risk management perspective — CGEIT is about identifying and managing IT risk, not technical implementation
- Understand the relationship between business objectives and IT risk strategy
- Know the difference between risk appetite, risk tolerance, and risk capacity
- Study all four risk response options and when each is appropriate

Domain Weights

Domain	Weight	Focus Areas
Domain 1: Corporate IT Governance	26%	Governance, risk appetite, three lines of defense
Domain 2: IT Risk Assessment	27%	Risk scenarios, analysis methods, risk register
Domain 3: Risk Response & Reporting	23%	Controls, KRIs, risk dashboards
Domain 4: IT & Security	24%	Architecture, IAM, cloud, BCP/DRP

Key Exam Strategies

- **Think like a risk manager:** Focus on governance and risk-based decisions
- **Business alignment:** IT risk management must support business objectives
- **Risk-based approach:** Decisions should be proportional to risk levels
- **Cost-benefit:** Consider ROI of controls and risk responses
- **Stakeholder communication:** Know who needs what risk information

Brakto