COBIT for Information Security Governance Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The digital age demands an integrated, enterprise-wide approach to managing information and technology (I&T) risks, making Information Security Governance a paramount business requirement, not merely a technical concern. Organizations are increasingly threatened by sophisticated cyberattacks, stringent regulatory compliance mandates like GDPR and HIPAA, and the accelerating pace of Digital Transformation. Relying on disparate security controls is no longer sufficient; a robust, cohesive governance framework is essential to ensure I&T investments create business value while effectively managing the evolving threat landscape. This challenge is precisely what the COBIT 2019 framework is designed to address, providing a comprehensive, globally accepted standard for the Governance of Enterprise IT (GEIT). COBIT for Information Security Governance Training Course moves beyond foundational concepts, demonstrating how to leverage COBIT?ÇÖs Goals Cascade and Design Factors to architect a dynamic governance system that positions information security as a strategic enabler of business objectives.

This intensive course on COBIT 2019 for Information Security Governance is the definitive guide for integrating security practices directly into your organization?ÇÖs core business strategy and operational processes. We will focus on key governance and management objectives relevant to security, such as Managed Security Services (DSS05), Managed Risk (APO12), and Governed Information Security (EDM03), ensuring graduates can translate stakeholder needs into measurable I&T goals. Participants will master the art of tailoring the framework using a holistic approach, covering everything from organizational structures and policies to culture, ethics, and behavior. By applying real-world case studies and a practical implementation roadmap, this training will equip you with the expertise to lead strategic security initiatives, achieve regulatory alignment, optimize resource utilization, and drive superior organizational performance in an era of constant cyber risk.

Programme Curriculum

COBIT for Information Security Governance Training Course

Introduction

The digital age demands an integrated, enterprise-wide approach to managing information and technology (I&T) risks, making Information Security Governance a paramount business requirement, not merely a technical concern. Organizations are increasingly threatened by sophisticated cyberattacks, stringent regulatory compliance mandates like GDPR and HIPAA, and the accelerating pace of Digital Transformation. Relying on disparate security controls is no longer sufficient; a robust, cohesive governance framework is essential to ensure I&T investments create business value while effectively managing the evolving threat landscape. This challenge is precisely what the COBIT 2019 framework is designed to address, providing a comprehensive, globally accepted standard for the Governance of Enterprise IT (GEIT). COBIT for Information Security Governance Training Course moves beyond foundational concepts, demonstrating how to leverage COBIT?ÇÖs Goals Cascade and Design Factors to architect a dynamic governance system that positions information security as a strategic enabler of business objectives.

This intensive course on COBIT 2019 for Information Security Governance is the definitive guide for integrating security practices directly into your organization?ÇÖs core business strategy and operational processes. We will focus on key governance and management objectives relevant to security, such as Managed Security Services (DSS05), Managed Risk (APO12), and Governed Information Security (EDM03), ensuring graduates can translate stakeholder needs into measurable I&T goals. Participants will master the art of tailoring the framework using a holistic approach, covering everything from organizational structures and policies to culture, ethics, and behavior. By applying real-world case studies and a practical implementation roadmap, this training will equip you with the expertise to lead strategic security initiatives, achieve regulatory alignment, optimize resource utilization, and drive superior organizational performance in an era of constant cyber risk.

Course Duration

5 days

Course Objectives

1. Strategically Align I&T Security goals with Enterprise Objectives using the COBIT 2019 Goals Cascade.
2. Design a Tailored Governance System for Information Security by applying COBIT's Design Factors.
3. Implement and monitor key COBIT processes for security, specifically Managed Security Services (DSS05) and Managed Risk (APO12).
4. Establish a clear separation between Governance (EDM) and Management functions within the security domain.
5. Develop an effective Risk Management Framework for I&T that integrates with enterprise risk management (ERM).
6. Drive Digital Trust and ensure Cyber Resilience across the enterprise by adopting a Holistic Approach to security.
7. Assess and improve the Process Capability and Focus Area Maturity of the organization?ÇÖs information security function using the COBIT Performance Management model.
8. Ensure Regulatory Compliance and Global Standards Alignment (e.g., ISO 27001, NIST CSF, GDPR) using COBIT as the overarching governance layer.
9. Master the principles of Dynamic Governance to enable agility and responsiveness to emerging AI-driven threats and rapid technology changes.
10. Integrate Culture, Ethics, and Behavior as a critical component of the security governance system to foster a strong Risk Culture.

11. Construct a compelling Business Case for security investments, focusing on Value Creation and Resource Optimization.
12. Facilitate the seven-phase Implementation and continual improvement of the COBIT-based Information Security Governance system.
13. Apply COBIT principles to govern emerging technology domains like Cloud Security and Third-Party Risk Management (TPRM).

Target Audience

1. Chief Information Security Officers (CISOs) and Security Directors.
2. IT Governance, Risk, and Compliance (GRC) Professionals.
3. IT Auditors.
4. Chief Information Officers (CIOs) and IT Executive Management.
5. Senior Business Managers responsible for technology strategy.
6. Enterprise Architects and Process Owners for I&T.
7. Risk Management Professionals and Chief Risk Officers (CROs).
8. IT Consultants and Advisors specializing in Security and Governance.

Course Modules

Module 1: Introduction to COBIT 2019 and Security Strategy Alignment

- COBIT 2019 Core Concepts and Architectural Components.
- The 6 Principles of the Governance System and Governance Framework.
- Mapping Stakeholder Needs to Enterprise Goals and I&T-Related Goals.
- Defining the strategic role of Information Security in achieving Business Value.
- Documenting initial organizational Enterprise Goals and relevant I&T Goals.
- Case Study: Analyzing a financial institution?ÇÖs strategy to use COBIT?ÇÖs Goals Cascade to justify a $5M security technology upgrade.

Module 2: The Security Governance Design Factors

- Understanding the 11 COBIT Design Factors and their critical impact on security.
- Deep dive into the Risk Profile and Threat Landscape Design Factors for tailoring the system.
- Selecting appropriate Focus Areas and applying them to the security model.
- Assessing the current Compliance Requirements and Technology Adaptation Strategy.
- Completing a Design Factor analysis to determine the optimal COBIT governance system for a high-risk manufacturing company.
- Case Study: Tailoring the COBIT security processes for a healthcare provider operating under strict HIPAA and GDPR regulations.

Module 3: Governing Information Security (EDM Domain Focus)

- Evaluate, Direct, and Monitor (EDM) domain.
- Detailed walkthrough of EDM03.
- Defining roles and responsibilities for the Governing Body in security oversight.
- Establishing security monitoring metrics and Key Risk Indicators.
- Developing a concise Governing Body Security Dashboard based on EDM03 metrics.
- Case Study: Examining a data breach scenario and how a lack of proper EDM03 oversight contributed to the failure.

Module 4: Security Risk Management and Planning

- The role of the Align, Plan, and Organize domain in security strategy.
- Managed Risk the comprehensive approach to risk identification, analysis, and response.
- Developing an I&T Security Strategy aligned with enterprise objectives.
- Integrating the COBIT risk process with a standard Enterprise Risk Management framework.
- Creating a high-level Risk Register for a new digital service based on APO12 practices.
- Case Study: Applying APO12 to manage the risks associated with a major Cloud Migration project.

Module 5: Security Implementation and Control Building (BAI Domain)

- The Build, Acquire, and Implement domain's role in establishing controls.
- Managed Changes to ensure security is integrated into all change management processes.
- Integrating security practices into the DevOps/Agile lifecycle.
- Implementing Identity and Access Management and Segregation of Duties controls.
- Designing a security-focused change enablement process using BAI06 control objectives.
- Case Study: Evaluating a software development firm's use of BAI to embed security testing into their continuous integration/continuous delivery pipeline.

Module 6: Operational Security and Service Delivery (DSS Domain)

- The Deliver, Service, and Support domain.
- Managed Security Services the operational backbone of information protection.
- Managing security incidents and continuity effectively.
- Control implementation for physical security and environmental protection.
- Drafting a framework for a Security Incident Response Plan based on DSS002 activities.
- Case Study: Simulating an advanced persistent threat (APT) and tracking the response using DSS02 and DSS05 controls.

Module 7: Performance Management and Continual Improvement

- Understanding the COBIT Performance Management model.
- Assessing the Process Capability of key security processes using the CMMI-based approach.
- Monitoring and reporting on Conformance and Performance using the MEA domain.
- Implementing the Continual Improvement lifecycle for the security governance system.
- Performing a quick self-assessment of the organization's current security capability level.
- Case Study: Developing a 12-month Security Improvement Roadmap based on a COBIT capability assessment gap analysis.

Module 8: Implementation Roadmap and Next Steps

- The 7-Phase COBIT Implementation Guide for the security focus area.
- Building the Business Case for the security governance program.
- Addressing Change Enablement and embedding a positive Security Culture throughout the organization.
- Integrating COBIT with other frameworks like NIST CSF, ISO 27001, and ITIL.
- Creating a phased, high-level COBIT 2019 Security Implementation Plan.
- Case Study: Reviewing the successful enterprise-wide implementation of COBIT for security at a major utility company.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com