Audit and IT audits

SECURITY GOVERNANCE 2025-26

Intro

- We explore the fundamental principles of auditing and connect them to cybersecurity assurance, governance, and IT control frameworks
- We introduce core objectives, key methodologies, and the professional mindset required of auditors operating within complex digital ecosystems

Overview

- Auditing is the systematic and independent evaluation of processes, systems, and controls to ensure that objectives are achieved effectively and securely
- We bridge classical audit theory and contemporary cybersecurity practice, explaining risk-based approaches, evidence collection, and control verification as tools for organizational assurance

Outcomes

Ability to

- Define *audit* and *assurance* within a cybersecurity context
- Explain the principles of risk-based auditing
- Identify major control and governance
- Describe IT General Controls and their relevance to information integrity
- Apply audit reasoning to evaluate cybersecurity and compliance mechanisms

Motivation

- Digital trust depends on the demonstrable integrity of systems and data
- Auditing transforms technical compliance into credible assurance, enabling transparency, accountability, and stakeholder confidence in organization’s cybersecurity posture

Audit versus Inspection

- Auditing is an evidence-based, risk-focused process that evaluates the design and effectiveness of controls
- Unlike inspections (rule-based and punitive), audits aim to understand whether governance, risk management, and control mechanisms adequately support strategic objectives

Historical Evolution

- Auditing originated in financial accountability, ensuring that records accurately reflected transactions
- With the rise of information systems, the discipline evolved toward IT auditing, verifying data reliability, system integrity, and control adequacy
- Modern audit objectives extend to cybersecurity, privacy, and digital resilience

The Role of IT Auditors

- IT auditors assess system controls across access, change management, and operations
- Role is to verify that CIA triad is maintained and that governance structures effectively manage technological risk

Professional Context

- Professional certifications (CISA, ISO 27001 Lead Auditor, ISACA frameworks, etc.) define competence standards in auditing and cybersecurity assurance
- These credentials validate knowledge of audit processes, ethical codes, and regulatory requirements across industries

Definition of an Audit

- According to ISO 19011, **an audit is a systematic, independent, and documented process for obtaining evidence and evaluating it objectively against established criteria**
- The outcome provides assurance regarding compliance, performance, or governance effectiveness

Objectives of Auditing

- Audits aim to verify that policies, controls, and operations achieve their intended outcomes
- They provide confidence to management, regulators, and external stakeholders about the organization’s reliability, integrity, and security posture

Audit Types

Common methodology, different focus

- Financial Audit: validates the accuracy of financial statements
- Operational Audit: evaluates efficiency and effectiveness of processes
- Compliance Audit: tests adherence to laws, regulations, or standards
- Performance Audit: measures achievement of objectives
- IT Audit: examines technological infrastructure and control environment
- More…

Audit Principles

- Integrity and ethical conduct
- Independence and objectivity
- Due professional care and competence
- Evidence-based approach
- Confidentiality and discretion
- Professional skepticism and judgment

Assurance

Definition

- An independent and objective evaluation that provides confidence to stakeholders about the reliability, integrity, and effectiveness of an organization’s processes, controls, or information
- Assurance is both an engagement and its outcome: it results from audit or review activities that generate evidence-based conclusions

Key Features

- Independent: performed by parties not involved in operations (e.g., internal audit, external audit, certification bodies)
- Objective: evidence-based, free from bias or influence
- Evidence-driven: conclusions rely on verifiable data and documented testing
- Purpose: to enhance trust in management assertions and governance processes

Risk Management and Assurance: Two Complementary Perspectives

	Risk Management	Assurance (Internal Audit)
Objective	Identify, assess, and mitigate threats to achieving objectives	Provide independent evaluation of how risks and controls are managed
Responsibility	Management and operational staff	Internal audit and other assurance providers
Nature of Work	Proactive and continuous	Reactive and periodic (independent review)
Focus	Managing risk exposure and implementing controls	Testing, verifying, and reporting on control effectiveness
Output	Risk registers, mitigation plans, risk appetite statements	Audit reports, assurance opinions, recommendations
Time Horizon	Forward-looking	Retrospective and evaluative
Key Question	"Are we managing our risks effectively?"	"Is our risk management effective?"

- Risk management creates confidence
- Assurance validates that confidence

From Audit to Assurance

- **Audit** is an independent evaluation of processes, controls, or information against defined criteria
- **Assurance** is the confidence or trust provided as a result of that evaluation
  - audit is the process; assurance is the outcome
- **Auditing** provides the evidence base that supports **assurance** about the reliability and effectiveness of an organization's controls and processes
- **Assurance** reflects an independent and objective assessment

Levels of Assurance

- Reasonable assurance: high but not absolute confidence, based on sampling and sufficient testing
- Limited assurance: moderate confidence, often in review engagements
- No assurance: purely descriptive or advisory observations

Negative Results Still Provide Assurance

- Assurance does not mean a positive result
- It represents confidence based on evidence, whether the findings are good or bad
- When an audit reveals weaknesses or non-compliance, it still provides assurance about the true state of controls
- Even a negative outcome gives assurance; it assures that controls do not meet the expected standards
- The value of assurance lies in transparency and reliability, not in favorable results

Independence and Objectivity

- Independence safeguards impartiality and credibility
- Auditors **must avoid conflicts of interest**, especially when auditing internal security functions
- Objectivity requires assessing evidence without bias, regardless of organizational pressures

Professional Skepticism

- A questioning attitude is essential to identify inconsistencies and potential misstatements
- Auditors critically evaluate evidence, seek corroboration from multiple sources, and avoid relying solely on management assertions

Materiality

Materiality defines the significance of an issue relative to the overall risk context

- *In cybersecurity, a single privileged account misconfiguration may be materially significant if it exposes sensitive data or critical infrastructure*

Audit Evidence

- Audit evidence must be sufficient (in quantity) and appropriate (in quality) to support conclusions
- Reliable evidence strengthens the credibility of the auditor’s opinion
- Key sources include
  - Documentation and records: policies, logs, reports, and configuration files
  - Observation of processes: direct review of control execution in real time
  - Interviews and inquiries: discussions with process owners to corroborate evidence
  - Analytical procedures: data comparisons, trend analysis, and correlation testing
  - Re-performance of controls: independent repetition of activities to confirm effectiveness
- Principle: credible, verifiable, and traceable evidence underpins every audit conclusion

The Audit Process

1. **Planning**: define objectives, scope, and criteria
2. **Understanding** the system: gather context and identify controls
3. **Risk assessment**: determine inherent and control risks (later)
4. **Designing tests**: establish audit procedures and sampling
5. **Collecting evidence**: execute fieldwork and document results
6. **Evaluating results**: compare evidence to criteria
7. **Reporting**: summarize findings, conclusions, and recommendations

Audit Documentation

- Workpapers record the procedures performed, evidence obtained, and reasoning applied
- They enable reproducibility, peer review, and traceability, ensuring that each audit conclusion is logically supported by documented evidence

Ethics & Quality Assurance

- Auditors must uphold ethical codes emphasizing confidentiality, objectivity, and competence
- Ethical lapses undermine trust, damage professional credibility, and may invalidate assurance engagements
- Quality assurance mechanisms (internal reviews, peer evaluations, and external assessments) ensure conformity with professional standards
- Continuous improvement reinforces the reliability and relevance of the audit function

Common Challenges

Modern auditing faces new complexities

- Massive data volumes and automation
- Evolving cybersecurity threats and cloud environments
- Integration of AI and analytics in control testing

The discipline adapts through continuous auditing, data-driven testing, and risk intelligence

From Theory to Application

- Auditing in cybersecurity translates traditional assurance principles to digital evidence
- Logs, configuration exports, access-control matrices, and forensic artifacts replace financial records as audit objects, maintaining the same rigor in evidence evaluation

Summary

- Auditing establishes trust through independent evaluation of governance and control mechanisms
- Understanding these foundations is essential before approaching risk-based auditing and framework-driven IT assurance

External audit

- Conducted by independent auditors or assurance firms, external to the organization
- Provides reasonable assurance on the accuracy, fairness, and reliability of financial statements or service organization controls
- Follows international standards such as
  - ISA (International Standards on Auditing)
  - ISAE 3402 and SSAE 18 for assurance engagements (later)
- Ensures credibility and transparency for investors, regulators, and other stakeholders
- Typically periodic, not continuous, and subject to formal reporting obligations
- Focus: external accountability, regulatory compliance, and public trust

Internal Audit

- Performed by an independent function within the organization, reporting to the board or audit committee
- Objective: evaluate and improve governance, risk management, and internal control effectiveness
- Based on frameworks like
  - COSO Internal Control
  - COBIT
  - ISO 9001 / ISO 27001
- Operates on a continuous and improvement-oriented basis
- Provides management with insights and recommendations to strengthen operations and reduce risks
- Focus: internal value creation, control maturity, and process improvement

Internal vs External Audit

Aspect	Internal Audit	External Audit
Position	Part of the organization	Independent from the organization
Objective	Improve processes, governance, and controls	Provide external assurance on statements or systems
Frequency	Continuous or periodic	Typically annual or engagement-based
Reporting line	Management / Audit Committee	Board, shareholders, regulators, clients
Primary standards	COSO, COBIT, ISO frameworks	ISAE 3000/3402, ISA, SSAE 18
Focus	Efficiency, risk, control effectiveness	Accuracy, compliance, reliability
Nature	Advisory and preventive	Certifying and evidential

Together, internal and external audits form a complete assurance ecosystem

Risk-Based Auditing and Frameworks

Section 2

Introduction to Risk-Based Auditing

- Risk-based auditing focuses audit efforts on areas where the probability and impact of failure are greatest
- By prioritizing high-risk domains, it ensures efficient resource allocation and enhances the relevance of findings
- This approach aligns audit scope with organizational objectives, emphasizing proactive assurance over reactive verification

The Audit Risk Model

- Audit Risk (AR) = Inherent Risk × Control Risk × Detection Risk
  - Inherent Risk: likelihood that an error or irregularity may occur in the absence of internal controls
  - Control Risk: likelihood that existing internal controls fail to prevent or detect such an error
  - Detection Risk: likelihood that audit procedures fail to identify the remaining error
- Managing audit risk involves balancing test depth, evidence sufficiency, and assurance confidence

Inherent and Control Risk

- Inherent Risk reflects the intrinsic vulnerability of a process or system
- Control Risk depends on the design and operational effectiveness of safeguards

An accurate understanding of both enables the auditor to design proportionate testing strategies and avoid redundant procedures

Detection Risk

- The likelihood that audit procedures fail to detect a material error or control weakness
- It depends on the nature, timing, and extent of audit testing, as well as on the effectiveness of procedures and auditor judgment
- Key aspects
  - Inversely related to the level of assurance: lower DR → higher confidence
  - Managed through increased sample size, test depth, and corroborating evidence
  - Influenced by auditor competence, automation tools, and time constraints
  - Balancing DR with inherent and control risks ensures the overall audit risk remains at an acceptable level
- Example: *if inherent and control risks are high, detection risk must be reduced by applying more extensive or rigorous audit procedures*

Materiality

- **Materiality is the threshold beyond which an error or control weakness becomes significant enough to influence decisions or audit conclusions**
- It guides the scope, depth, and prioritization of audit work
- Key aspects
  - Quantitative: measurable impact or size of error
  - Qualitative: sensitivity or nature of the issue
  - Contextual: depends on risk appetite and regulatory expectations
- In cybersecurity, even a single critical vulnerability can be material if it threatens core systems or sensitive data

Materiality and Risk

- Materiality thresholds define which control weaknesses or incidents are significant enough to influence the auditor’s conclusions or stakeholder decisions
- In a cybersecurity audit, even low-likelihood events (e.g., a privileged-access breach) may be material if their potential impact is critical
- Materiality interacts with the audit-risk model (AR = IR × CR × DR): higher inherent or control risk, or limited detection capability, requires a lower materiality threshold and expanded testing
- Together, risk and materiality guide audit judgment, sampling strategy, and evidence evaluation

Assertions

- Claims made by management regarding data, processes, or systems
- Common categories include
  - Existence: the item or control actually exists
  - Completeness: all relevant elements are included
  - Accuracy: information is recorded correctly
  - Authorization: actions are properly approved
  - Presentation: data are appropriately disclosed or formatted
- Auditors design tests to verify each assertion objectively

COSO

- Committee of Sponsoring Organizations of the Treadway Commission
- Private, U.S.-based initiative established in 1985 to improve the quality of financial reporting and **internal control**
- Created in response to corporate frauds of the early 1980s, following recommendations of the Treadway Commission on fraudulent financial reporting
- Sponsored by five professional associations: AICPA, IIA, FEI, IMA, and AAA
- In 1992, COSO released the Internal Control — Integrated Framework, later expanded to Enterprise Risk Management (ERM) (2004, 2017)
- COSO provides the global foundation for modern internal control and risk management frameworks

Internal Controls

- **Definition**: Processes, policies, and procedures established to ensure objectives are achieved effectively, efficiently, and ethically
- **Purpose**: Protect assets, ensure reliable reporting, and support legal and policy compliance
- COSO view (1992, 2013): *A process effected by the board, management, and staff to provide reasonable assurance on operations, reporting, and compliance*
- **Nature**: Ongoing, embedded in daily activities
- **Relevance**: The foundation of every audit, risk management, and governance system

The COSO Model

- The COSO Framework defines five interrelated components of internal control
  1. **Control Environment**: ethical tone, governance, and accountability
  2. **Risk Assessment**: identifying and evaluating risks to objectives
  3. **Control Activities**: policies and procedures mitigating those risks
  4. **Information & Communication**: ensuring reliable data flow
  5. **Monitoring**: evaluating control performance over time
- COSO remains a cornerstone for both financial and IT control systems.

Objectives of Internal Control

1. Operations: ensure effective and efficient use of resources to achieve organizational goals
2. Reporting: maintain reliable, timely, and transparent financial and non-financial reporting
3. Compliance: adhere to applicable laws, regulations, and internal policies

Control Types

- Classified by purpose and execution
  - **Preventive Controls**: stop errors or incidents before occurrence
    - access restrictions
  - **Detective Controls**: identify issues after occurrence
    - log monitoring
  - **Corrective Controls**: restore normal conditions
    - patch deployment
- Controls may also be manual or automated, each with distinct reliability profiles

Control Objectives

- To ensure the CIA triad within information systems
  - Access control to preserve confidentiality
  - Input validation to protect integrity
  - Redundancy and backups to guarantee availability
- Together, these objectives sustain operational resilience and trust in digital infrastructure

The Risk-Control-Test Relationship

- Each risk maps to one or more controls, and each control is verified through specific tests
- This matrix (Risk and Control Matrix, RCM) provides transparency and traceability
- It links audit scope, procedures, and evidence directly to organizational risk priorities

RCM Example

- 1-line RCM

Risk	Control	Test Procedure	Evidence
Unauthorized access	Enforcement of MFA	Review system configuration and test authentication	Screenshot of policy settings, audit logs

- This structure allows clear documentation and supports reproducibility of audit conclusions

Sampling in Auditing

- Testing every transaction is impractical, **sampling is done**
  - Statistical
  - Judgmental (non-statistical)
- Sampling must balance efficiency with assurance, ensuring that conclusions remain valid

Evidence Evaluation

- Evidence sufficiency and appropriateness depend on risk level and control criticality
- High-risk areas demand corroboration from multiple evidence types: documents, logs, interviews, and re-performance
- The auditor’s professional judgment determines when the evidence base justifies a conclusion

Control Framework Overview

- Control frameworks translate governance principles into structured control sets
- They promote consistency, comparability, and accountability across organizations
- Frameworks like COSO, COBIT, ISO 27001, and NIST CSF help auditors benchmark practices and align with regulatory expectations

COSO again

- COSO integrates objectives, components, and principles to support reliable internal control systems
- Its structure (**objectives**, slide 39, and **components**, slide 38) creates a holistic approach adaptable to both financial and IT domains
- It provides a conceptual foundation for subsequent frameworks like COBIT

COBIT 2019

governance

- COBIT = Control Objectives for Information and Related Technologies
  - from ISACA (Information Systems Audit and Control Association)
- Defines governance and management objectives across domains
  - Evaluate, Direct, Monitor (EDM) – strategic oversight and governance
  - Align, Plan, Organize (APO) – policy, strategy, and planning
  - Build, Acquire, Implement (BAI) – system development and integration
  - Deliver, Service, Support (DSS) – operations and service delivery
  - Monitor, Evaluate, Assess (MEA) – performance and compliance
- COBIT aligns IT governance with business strategy and stakeholder value

management

ISO/IEC 27001 and Annex A

- ISO/IEC 27001 establishes an Information Security Management System (ISMS), ensuring continuous protection of information assets
- Annex A enumerates 93 controls across four themes: organizational, people, physical, and technological
- These controls operationalize the ISMS and support certification-based assurance

NIST CSF

- The NIST CSF organizes cybersecurity activities into five core functions
  1. Identify – Understand assets, risks, and organizational context
  2. Protect – Implement safeguards to ensure data and service security
  3. Detect – Identify and analyze cybersecurity events
  4. Respond – Contain and mitigate incidents
  5. Recover – Restore capabilities and services after disruption
- CSF 2.0 extends the framework to include governance and supply chain risk management, linking cybersecurity directly to business outcomes

NIST SP 800-53

- NIST Special Publication 800-53 offers a detailed control catalog widely used by U.S. federal agencies
- It defines 20 control families, including Access Control, Audit and Accountability, System and Communications Protection, and Security Assessment and Authorization
- Its rigor makes it a global reference for control design and testing in critical infrastructures

ISAE

- International Standard on Assurance Engagements
- It’s a category of professional standards issued by the International Auditing and Assurance Standards Board (IAASB) — part of the International Federation of Accountants (IFAC)
- Several documents on assurance

ISAE 3402	Assurance Reports on Controls at a Service Organization	Controls at third-party providers relevant to financial reporting

ISAE 3402: Overview

ISAE 3402: Assurance for Service Organizations

- ISAE 3402 (Assurance Reports on Controls at a Service Organization) is an international standard issued by the IAASB (technical board of IFAC)
- It defines how an independent auditor evaluates and reports on the design and operating effectiveness of controls at a service organization
- Purpose: to provide assurance to user entities and their auditors that outsourced processes are reliable and well-controlled
- Applies to services that impact financial reporting, such as payroll, accounting, or data-hosting for ERP systems
- Scope: controls at third-party providers relevant to financial reporting

Service Organizations and User Entities

Term	Meaning
Service Organization	A third-party provider that performs functions for another entity which affect its financial reporting (e.g., payroll processor, data center)
User Entity	The company that outsources part of its operations and relies on the service organization's controls
User Auditor	The external auditor of the user entity who relies on the ISAE 3402 / SOC 1 report

Example

A bank uses an external cloud provider to host its loan accounting platform: the provider is the service organization, and its controls are relevant to the bank's financial statements

ISAE 3402 Report Types

Type	Description	Period Covered	Usefulness
Type I	Design and implementation of controls at a specific point in time	One date	Verifies control design
Type II	Design and operating effectiveness of controls over a period (6–12 months)	Time period	Tests control performance

Key point: Type II reports provide stronger assurance because they test whether controls operated effectively over time

Relationship with SOC Reports (AICPA)

- The AICPA (U.S.) developed the SOC reporting framework under SSAE 18, which mirrors ISAE 3402 principles
- Both standards describe the same engagement type: assurance on controls at service organizations
- SOC 1 reports = U.S. equivalent of ISAE 3402
- SOC reports expand beyond financial reporting through SOC 2 and SOC 3
- *ISAE 3402: international standard*
- *SOC 1: U.S. implementation of the same concept*

SOC Report Types — AICPA Framework

Report	Standard	Focus	Audience
SOC 1	SSAE 18 / AT-C 320	Controls relevant to financial reporting	User auditors, CFOs
SOC 2	SSAE 18 / AT-C 205	Controls on security, CIA, and privacy	Clients, regulators, partners
SOC 3	SSAE 18 / AT-C 205	Public, summarized version of SOC 2 (no sensitive details)	General public, marketing

- SOC 1 ↔ ISAE 3402 (financial focus)
- SOC 2 & 3 ↔ broader assurance on IT and data governance

Why ISAE 3402 and SOC Reports Matter

Assurance and Trust in Outsourced Environments

- Organizations increasingly rely on third-party providers for critical processes
- ISAE 3402 and SOC reports give confidence that these providers
  - Have documented and effective controls
  - Maintain integrity, confidentiality, and availability of data
  - Support financial reporting reliability and regulatory compliance
- User entities can leverage these reports instead of duplicating control testing on suppliers
- *Outcome: transparency, reduced audit duplication, and trusted outsourcing*

ISAE 3402 vs SOC Reports (Summary)

Aspect	ISAE 3402	SOC Reports
Issuer	IAASB / IFAC	AICPA (U.S.)
Standard	ISAE 3402	SSAE 18
Scope	Service organization controls relevant to financial reporting	SOC 1: financial; SOC 2/3: broader IT & privacy
Report Type	Type I / Type II	Same structure: Type I / Type II
Recognition	International	U.S. and global recognition
Relationship	Conceptual standard	Practical reporting framework

Different origins — same assurance goal: trust in third-party control environments

GDPR and Data Protection Audits

- Under the General Data Protection Regulation (GDPR), audits assess compliance with data protection principles such as lawfulness, fairness, purpose limitation, minimization, and integrity
- Auditors verify the existence of technical and organizational measures (TOMs) and evaluate accountability documentation and breach-handling procedures

Technical and Organizational Measures (TOM)

- Controls ensuring data protection, risk mitigation, and compliance (e.g., GDPR, ISO 27001, SOC 2)
- Technical measures
  - Encryption, Access control, Backup, Monitoring
- Organizational measures
  - Policies, Training, Incident response, Vendor management
- TOMs are the practical safeguards supporting security and compliance frameworks

Continuous Auditing

- Continuous auditing integrates automation and analytics to perform control testing in near real time
- It supports early detection of control breakdowns, fraud, or misconfigurations, bridging traditional periodic audits with continuous assurance models
- Mainly internal

Mapping Frameworks

- Auditors often cross-reference controls between frameworks
  - e.g., mapping NIST CSF to ISO 27001 Annex A or COBIT
- These mappings ensure comprehensive coverage, reduce redundancy, and enhance interoperability across compliance regimes

The Auditor’s Toolbox

- Modern auditors employ a diverse toolkit, including
  - Policy and documentation review
  - Walkthroughs and interviews
  - Sampling and re-performance
  - Configuration inspection
  - Data analytics and automated queries
  - Observation of control operation
- Integration of technical and analytical methods strengthens audit reliability

Risk-Based Audit Process Flow

A structured workflow ensures audit consistency

1. Plan – define objectives and scope
2. Assess Risk – identify and rank critical areas
3. Design Tests – develop tailored procedures
4. Execute – collect and analyze evidence
5. Evaluate – compare results to criteria
6. Report – communicate findings and recommendations
7. Follow-Up – verify remediation and continuous improvement

Section Summary

- Risk-based auditing aligns assurance activities with organizational priorities and risk exposure
- By integrating control frameworks such as COSO, COBIT, ISO 27001, and NIST, auditors establish a structured foundation for IT-specific auditing (later)

IT Audit Domains and Cases

Section 3

Introduction to IT Audit

- IT auditing evaluates the governance, infrastructure, and operational controls of information systems
- Its purpose is to verify that technology supports organizational objectives securely, efficiently, and reliably
- Through a structured approach, IT audit bridges the gap between management assurance and technical validation

IT General Controls (ITGCs)

- ITGCs form the foundation of system reliability and automated controls
- They are typically grouped into three domains
  1. Access Management – ensuring authorized and traceable system access
  2. Change Management – maintaining controlled system modifications
  3. IT Operations – sustaining consistent, secure, and recoverable system functioning
- Strong ITGCs underpin every layer of audit assurance

Access Management Controls

Effective access control frameworks include

- Joiner–Mover–Leaver procedures for user lifecycle management
- Role-Based Access Control (RBAC) to enforce least privilege
- Segregation of Duties (SoD) to prevent conflicts and fraud
- Privileged account monitoring for administrative actions
- Multi-Factor Authentication (MFA) to strengthen authentication resilience

Auditors assess both configuration and operational enforcement

Change Management Controls

Change management ensures that system modifications are authorized, tested, and traceable

Auditors examine

- Version control systems (e.g., Git) for tracking code changes
- Testing and approval workflows validating reliability
- Release documentation and rollback plans confirming reversibility

Weak change management is a frequent source of security incidents and operational failures

IT Operations Controls

IT operations provide stability and continuity to digital systems.

Key control areas include

- Backup and recovery validation
- Patch and vulnerability management
- Incident and problem management with root-cause tracking
- Job scheduling and monitoring for automated processes
- Capacity management and business continuity planning

These controls ensure service resilience and data protection

Application Controls

Application controls operate within specific software environments, ensuring processing accuracy and completeness

Examples include

- Input validation to prevent data corruption
- Processing checks to confirm integrity
- Output reconciliation for accuracy and completeness
- Interface controls guaranteeing data exchange integrity

When automated, they significantly reduce operational risk

Testing Automated Controls

- Auditors assess automated controls by inspecting configuration parameters, logic rules, and exception handling mechanisms
- Typical evidence includes screenshots, configuration exports, and system logs
- Automated controls offer higher reliability, but only if systems are properly configured, maintained, and protected from unauthorized change

CAATs (Computer-Assisted Audit Techniques)

- CAATs integrate technology into the audit process
- Common tools and languages (e.g., SQL, Python, ACL, IDEA) enable
  - Full-population data analysis
  - Detection of anomalies, duplicates, or exceptions
  - Cross-validation of transactional integrity
- CAATs enhance efficiency, accuracy, and reproducibility of audit testing

Example of Data Analytics in Audit

Data analytics can identify systemic issues, such as

- Duplicate payments or inconsistent transactions
- Orphan records violating referential integrity
- Unauthorized access attempts detected in system logs

Automated queries allow auditors to validate control performance across large datasets

Audit of Logical Security

- Logical security audits verify that information access and protection mechanisms are effective
- Key focus areas include
  - Identity and Access Management (IAM) systems
  - Password policies and encryption standards
  - Network segmentation and access control lists (ACLs)
  - Logging, monitoring, and alerting mechanisms
- Auditors assess compliance with ISO 27002 (*Information Security, Cybersecurity and Privacy Protection — Information Security Controls*) and related best practices

Infrastructure and Network Audit

- Infrastructure audits assess the integrity and resilience of physical and virtual components
- Typical procedures include
  - Reviewing firewall and router configurations
  - Checking patch levels and system hardening
  - Verifying vulnerability management processes
  - Ensuring asset inventories are accurate and complete
- Strong network governance supports reliable cybersecurity assurance

Cloud Auditing

- Cloud environments introduce shared-responsibility models between provider and customer
- Auditors must
  - Distinguish between provider and client control domains
  - Review SOC 2 reports and certifications for provider assurance
  - Evaluate IAM roles, encryption, and data segregation
  - Verify contractual SLAs and data residency obligations
- Cloud audits require understanding of both regulatory compliance and technical configuration

Vendor and Third-Party Audits

- Organizations increasingly rely on external service providers
- Auditors evaluate
  - Contractual controls and SLAs
  - Monitoring mechanisms for vendor performance
  - Third-party assurance reports (e.g., SOC 2, ISO 27001)
  - Incident response coordination and data protection clauses
- Robust third-party auditing mitigates supply-chain and outsourcing risks

DevOps and Continuous Delivery

- DevOps environments combine speed with automation, creating new audit challenges
- Auditors examine
  - Change pipelines for evidence of testing, approval, and segregation
  - Peer-review documentation and automated deployment logs
  - Rollback and version control mechanisms
- Effective auditing balances agility with control discipline, ensuring traceability in fast-paced delivery cycles

Privacy Audits

- Privacy audits ensure compliance with GDPR and other data protection laws
- They assess
  - Lawfulness and consent management
  - Data minimization and purpose limitation
  - Retention policies and secure deletion
  - Encryption and pseudonymization measures
  - Data subject rights management (access, rectification, erasure)
- Privacy audits bridge legal compliance with technical enforcement

AI and Machine Learning Audit

- Auditing AI systems involves evaluating both model governance and ethical implications
- Key dimensions include
  - Data lineage and quality of training datasets
  - Fairness, bias, and explainability of model outputs
  - Monitoring and drift detection to maintain reliability
  - Accountability frameworks defining human oversight
- Auditors assess whether AI systems align with transparency, accountability, and non-discrimination principles

Evidence in IT Audits

- In IT audits, evidence includes digital artifacts such as system logs, configuration files, access reviews, screenshots, and automated reports
- The authenticity, integrity, and traceability of evidence determine its reliability
- Auditors document the source and context of each artifact to maintain a defensible audit trail

Common IT Audit Findings

- Frequent findings include
  - Weak or inconsistent access provisioning
  - Missing change authorizations or documentation
  - Incomplete or untested backups
  - Insufficient monitoring or alerting mechanisms
  - Outdated or misaligned security policies
- Each finding must be supported by evidence, evaluated by risk, and accompanied by remediation recommendations

Reporting IT Audit Results

- Audit reports synthesize evidence into actionable insights
- Standard structure: Criterion → Condition → Cause → Effect → Recommendation
- Each issue includes a risk rating and a management response, ensuring traceability and accountability
- Effective reporting communicates both technical depth and strategic relevance

Case Study 1: Identity and Access Management

- Scenario: A SaaS platform manages thousands of users with evolving roles
- Risks: Excessive privileges, dormant accounts, and lack of periodic review
- Controls: Automated provisioning, periodic access recertification, and prompt deactivation of inactive accounts
- Audit focus: Verify enforcement of RBAC and review frequency to ensure least-privilege compliance

Case Study 2: Change Management

- Scenario: Continuous integration and delivery (CI/CD) pipelines push frequent updates
- Audit procedures
  - Verify authorization of code changes
  - Review test and approval evidence
  - Confirm rollback and versioning capabilities
- Objective: Ensure rapid delivery without compromising control and traceability

Case Study 3: Data Analytics Audit

- Scenario: Security event logs are analyzed for anomalies
- Method: Use CAATs to detect outliers, unauthorized access, or unmonitored assets
- Audit value: Demonstrate control coverage and identify areas for continuous monitoring improvement

Quiz Slide

Question 1: What is the primary purpose of IT General Controls (ITGCs)?

A. Ensure data confidentiality only
B. Provide foundational reliability for automated controls
C. Detect malware
D. Replace application testing

Quiz Slide

Question 2: Which control type prevents errors?

A. Detective
B. Preventive
C. Corrective
D. Responsive

Quiz Slide

Question 3: Which framework defines Identify – Protect – Detect – Respond – Recover?

A. ISO 27001
B. COBIT 2019
C. NIST CSF
D. ISAE 3402

References and Further Reading

- ISO 19011:2018 – Guidelines for Auditing Management Systems
- COBIT 2019 – Framework for Governance and Management of Enterprise IT (ISACA)
- ISO/IEC 27001:2022 – Information Security Management Systems
- NIST Cybersecurity Framework 2.0 – Risk Management Guidance
- NIST SP 800-53 Rev. 5 – Security and Privacy Controls for Information Systems
- ISAE 3402 / SOC 2 – Assurance Reports on Controls at a Service Organization
- ISACA, IT Audit Fundamentals (3rd ed., 2023)
- GDPR Regulation (EU) 2016/679
- INTOSAI GOV 9140 – Internal Control Standards for the Public Sector