RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

IT ROLES

This module examines how various roles in the IT context interact with risk management and resilience

IT ROLES IN RISK MANAGEMENT

- Generally, risk management is holistic
  - It requires an overall cohesive strategy
  - Works best with continuous cross-disciplinary coordination between different functional areas
- For this to work
  - Each area of responsibility has its own unique set of targeted responsibilities
  - And must also collaborate with other roles involved in risk management, both IT and non-IT
- The roles discussed here are generic
  - They will map to a variety of specific roles in a specific organization

CONTROLS

- Each role owns controls
  - A control is a specific measure; whether a policy, process, practice, or technical mechanism, that is implemented to reduce risk to an acceptable level
  - Controls can be:
    - *Preventive*: stop a risk event from occurring (patching, input validation)
    - *Detective*: identify when a risk event is happening (monitoring, audits)
    - *Corrective*: restore systems and reduce impact after a risk event (backups, incident response)
- These are tied to policies, regulations, and frameworks
  - Examples:
    - *Sysadmin*: Patch management is a *preventive* control
    - *Developer*: Secure coding standards are *preventive* controls
    - *Tester*: Regression suites are *detective* controls for software defects
    - *Security analyst*: SIEM monitoring is a *detective* control
    - *DBA*: Backup and restore procedures are *corrective* controls

CREATE EVIDENCE

- Controls are only useful if
  - They can be shown to be in place and are effective at mitigating risk
  - *Evidence* is the documentation, reports, or logs that prove a control worked as intended
  - Evidence is the data that auditors, regulators, and risk managers depend on
  - Examples:
    - *Sysadmin*: Patch compliance reports, backup logs, configuration baselines
    - *Developer*: Code review records, dependency scanning reports
    - *Tester*: Test execution logs, defect reports, coverage metrics
    - *Security analyst*: Incident tickets, SIEM alerts, vulnerability scan results
    - *DBA*: Restore test results, access control reviews
  - Shows regulators, auditors, and executives that risks are managed
  - Without evidence, “we patched” or “we tested” can’t be trusted

INTRODUCES OR MITIGATES RISK

- Daily work in IT can either
  - Reduce risk when controls are applied correctly
  - Or introduce risk when shortcuts, errors, or omissions occur
  - Risk management is cumulative: every action shifts the organization's risk posture
- Examples
  - *Sysadmin*
    - Forgetting to apply a critical patch introduces risk
    - Consistently applying patches mitigates it
  - *Developer*
    - Writing insecure SQL queries introduces risk
    - Using parameterized queries mitigates it

INTRODUCES OR MITIGATES RISK

- Examples
  - *Tester*
    - Missing coverage for critical workflows introduces risk
    - Full testing mitigates it
  - *Security analyst*
    - Ignoring low-priority alerts that signal lateral movement introduces risk
    - Tuning SIEM rules mitigates the initial system attack
  - *DBA*
    - Not testing restores introduces risk
    - Scheduled restore tests mitigate it

ROLES

- The following discussion will deal with these generic roles
  - *System Administrator (Sysadmin)*
    - Manages servers, operating systems, and core infrastructure to ensure secure and stable IT operations
  - *Developer*
    - Designs, codes, and maintains software applications that support business functions
  - *Tester/QA Engineer*
    - Validates that software meets functional, quality, and security requirements before release
  - *Security Analyst*
    - Monitors, detects, and responds to threats across systems, networks, and application
  - *Database Administrator (DBA)*
    - Maintains and secures organizational data, ensuring availability, integrity, and recoverability

ROLES

- Generic roles (cont)
  - *Network Engineer*
    - Designs and manages network infrastructure to provide secure and reliable connectivity
  - *Cloud / DevOps Engineer*
    - Builds and operates cloud-native environments and CI/CD pipelines for scalable and compliant delivery
  - *Project Manager / Product Owner*
    - Coordinates projects, balancing scope, timelines, and risks while keeping stakeholders aligned
  - *Business Analyst*
    - Bridges business needs and technical requirements, ensuring systems support processes while meeting compliance and control expectations
  - *IT Auditor*
    - Evaluates IT controls, compliance, and governance to provide independent assurance that risks are effectively managed

SYSTEM ADMINISTRATORS / PLATFORM OPERATIONS

- Responsible for the day-to-day management and upkeep of IT infrastructure
  - Includes servers, operating systems, storage, and supporting platforms
  - Ensures that IT services are available, secure, and reliable for the business
  - They are often the “front line” in keeping core systems running smoothly
- Typical responsibilities include
  - Installing, configuring, and maintaining servers, operating systems, and related tools
  - Monitoring performance and availability of systems
  - Managing system access and user accounts
  - Applying patches and upgrades to maintain security and stability
  - Backing up data and ensuring recovery processes work
  - Troubleshooting incidents and restoring service after disruptions

SYSTEM ADMINISTRATORS / PLATFORM OPERATIONS

- General risk-relevant activities
  - Maintain secure and stable infrastructure through baselines, patches, and hardening
  - Enforce configuration standards and ensure consistency across systems
  - Protect against unauthorized access by managing privileged accounts
  - Validate recovery capabilities so the business can bounce back from incidents
- Contribution to risk management
  - *Operational continuity*
    - Ensuring critical systems are patched, backed up, and available to reduce downtime risk
  - *Control ownership*
    - Directly operate preventive (patching), detective (monitoring), and corrective (restore) controls
  - *Evidence creation*
    - Logs, patch reports, baseline scans, and restore test results are evidence for auditors and risk teams
  - *Privilege management*
    - By managing “admin” access, they reduce insider threats and privilege creep

SYSTEM ADMINISTRATORS / PLATFORM OPERATIONS

- Typical risk management activities
  - *Patch management*
    - Regularly applying vendor and security patches to eliminate vulnerabilities
  - *Configuration management*
    - Using baselines (e.g., CIS benchmarks) and monitoring for drift from standards in performance and quality (KPIs and SLAs)
  - *Backups and restore testing*
    - Ensuring data and system recovery works through periodic restore exercises, often called disaster recovery drills
  - *Access reviews*
    - Auditing and limiting privileged accounts, enforcing least privilege
  - *Incident support*
    - Restoring services and providing logs during investigations

SYSTEM ADMINISTRATORS / PLATFORM OPERATIONS

- Common risks if not managed
  - *Unpatched vulnerabilities*
    - Exposed systems become easy targets for attackers
  - *Failed restores*
    - Backups that can’t be restored result in data loss or extended downtime
  - *Privilege creep*
    - Users accumulating unnecessary permissions over time, increasing insider risk
  - *Configuration drift*
    - Systems slowly deviating from secure standards, introducing hidden vulnerabilities
  - *Unauthorized changes*
    - Making system changes without following change control can introduce instability

DEVELOPERS

- Responsible for designing, coding, testing, and maintaining applications and services that support business operations
  - Ensures that software is not only functional but also secure, resilient, and maintainable
  - Translates business requirements into technology solutions
- Typical responsibilities include:
  - Writing and maintaining application code
  - Integrating with APIs, databases, and third-party components
  - Performing peer code reviews and unit testing
  - Managing source code repositories and version control
  - Fixing bugs and responding to security findings
  - Participating in the full Software Development Life Cycle (SDLC)

DEVELOPERS

- Role in risk management
  - Developers are the builders of digital products
  - Their choices directly affect confidentiality, integrity, and availability of systems
- Their risk contributions include
  - Embedding security by design into applications, not added on after the fact
  - Writing code that is defensive against potential misuse or deliberate attack
  - Follow secure coding guidelines and comply with SDLC controls
  - Ensure software can withstand real-world threats without introducing new vulnerabilities

DEVELOPERS

- SDLC controls
  - Policies, processes, and technical practices built into the SDLC
  - Ensures that applications are secure, reliable, and compliant from design through retirement
  - Checkpoints and safeguards applied throughout the development process, not just at the end
- Requirements phase
  - *Control*: Security and compliance requirements documented
    - Example: Application must comply with GDPR for data handling
- Design phase
  - *Control*: Threat modeling and secure design reviews
    - Example: Architecture reviewed against OWASP and internal standards

DEVELOPERS

- Development phase
  - *Control*: Secure coding standards and peer code reviews
    - Example: All code changes must be peer-reviewed before merge
- Testing phase
  - *Control*: Risk-based testing, security testing, automated unit and regression testing
    - Example: Static code analysis and penetration testing required before release
- Deployment phase
  - *Control*: Change management approvals and environment hardening
    - Example: No deployment to production without approval in change tracking system

DEVELOPERS

- Maintenance phase
  - *Control*: Patch management and continuous monitoring
    - Example: Third-party dependency updates must be reviewed within 30 days of release
- Decommissioning - retirement phase
  - *Control*: Secure data disposal and documentation of system shutdown
    - Example: All sensitive data must be deleted or anonymized

DEVELOPERS

- Contribution to risk management
  - *Preventing vulnerabilities*
    - Secure coding and dependency checks reduce exploitable flaws
  - *Control ownership*
    - Implement preventive controls (input validation, encryption) and support detective controls (logging, error handling)
  - *Evidence creation*
    - Code reviews, automated test results, dependency scan reports, and design documentation provide risk evidence
  - *Resilience*
    - Building applications that degrade gracefully, recover quickly, and log effectively in order to support both risk and resilience objectives

DEVELOPERS

- Typical risk management activities
  - *Secure coding practices*
    - Using defensive programming techniques (e.g., input sanitization, parameterized queries)
  - *Peer reviews*
    - Reviewing code for quality, maintainability, and adherence to security standards
  - *Threat modeling*
    - Identifying possible attack vectors and mitigating them at the design stage
  - *Dependency scanning*
    - Checking third-party libraries and frameworks for vulnerabilities
  - *Unit and integration testing*
    - Ensuring code works as intended, with tests to validate security-critical functions

DEVELOPERS

- Common risks if not managed
  - *Injection flaws*
    - For example: SQL Injection, XSS, etc
    - Occur if user input isn't validated
  - *Insecure dependencies*
    - Using outdated or unvetted open-source libraries introduces vulnerabilities
  - *Logic errors*
    - Mistakes in business logic can create exploitable loopholes
  - *Poor documentation*
    - Incomplete or unclear documentation increases maintenance and handover risks
  - *Hardcoded secrets*
    - Embedding credentials in code creates serious exposure
  - *Insecure error handling*
    - Revealing system details in error messages can aid attackers

TESTERS/QA ENGINEERS

- Responsible for evaluating software and systems
  - Ensure they function correctly, meet requirements, and are free from critical defects
  - Confirm that applications are not only functional but also secure, reliable, and usable before reaching production
  - A key line of defence against introducing risks into the operational environment
- Typical responsibilities include
  - Designing and executing test cases
  - Running regression and integration tests after code changes
  - Performing risk-based and security-focused testing, including exploratory testing
  - Supporting the use of automated testing tools and frameworks
  - Documenting test results and tracking defects
  - Collaborating with developers to resolve issues before release

TESTERS/QA ENGINEERS

- Role in risk management
  - Ensure that quality and security requirements are validated before release
- Directly reduces operational, compliance, and reputation risks by:
  - Detecting defects that could lead to failures, outages, or vulnerabilities
  - Providing assurance evidence that controls are effective
  - Applying risk-based testing to focus on the most critical functionality and threats
  - Providing feedback to other roles on potential risk issues

TESTERS/QA ENGINEERS

- Contribution to risk management
  - *Risk detection*
    - Identify vulnerabilities, defects, and weak points before release
  - C*ontrol validation*
    - Confirm that preventive and detective controls (e.g., input validation, error handling) actually work
  - *Evidence creation*
    - Provide logs, defect reports, test coverage reports, and pass/fail results for auditors and risk managers
  - *Risk communication*
    - Translate technical defects into business impact (e.g., “This flaw could expose customer data”)
- Security testing
  - The area of security testing has evolved a number of specific methods to deal with adversarial attack risks
  - For example, red team testing where external testers take on the role of an adversary and attempt to breach the organization’s security measures

TESTERS/QA ENGINEERS

- Typical risk management activities
  - *Functional testing*
    - Ensuring systems perform as intended under expected conditions
  - *Regression testing*
    - Verifying that new changes don’t break existing functionality
  - *Security testing*
    - Checking for vulnerabilities such as weak authentication, injection flaws, and misconfigurations
  - *Risk-based testing*
    - Prioritizing testing on the highest-risk features (e.g., payments, authentication, data access)
  - *Defect tracking and reporting*
    - Documenting issues and following up on remediation before going live in production
  - *Exploratory testing*
    - Looking for “what if?” scenarios that have been overlooked
  - *Live testing*
    - Running operational tests in the production environment to detect any signs of drift or potential breaches

TESTERS/QA ENGINEERS

- Common risks if not managed
  - *Incomplete test coverage*
    - Leaving critical areas untested exposes the system to undetected failures
  - *Missed critical flaws*
    - Security or functional defects that escape testing can lead to breaches or outages
  - *Ineffective test evidence*
    - Poorly documented test results weaken compliance and audit readiness
  - *Over-reliance on automation*
    - Automated tests may miss context-specific issues if not complemented with exploratory testing
  - *Late testing*
    - Defects found too late in the SDLC increase cost, delay, and risk
  - *System drift*
    - Failure to detect changes in the functioning of the operational system that may introduce risk

SECURITY ANALYSTS

- Responsible for monitoring, detecting, analyzing, and responding to security threats
  - Ensures that suspicious activities are identified quickly
  - Ensures incidents are contained before they escalate
  - Serve as the eyes and ears of cybersecurity, constantly watching for signals of compromise or attack
- Typical responsibilities include
  - Monitoring logs and alerts from SIEM systems and other security tools
  - Investigating suspicious activity and escalating incidents when needed
  - Performing vulnerability scans and analyzing the results
  - Responding to and documenting security incidents
  - Coordinating with IT and risk teams to remediate threats
  - Supporting compliance and audit requests with monitoring evidence

SECURITY ANALYSTS

- Role in risk management is to ensure
  - Incidents are identified quickly before they cause significant damage
  - Vulnerabilities are surfaced and remediated before attackers can exploit them
  - Responses are coordinated to minimize the impact of threats
  - Monitoring evidence is available to support audits, governance, and regulatory obligations
  - Works with testers to actively probe system defences

SECURITY ANALYSTS

- Contribution to risk management
  - *Detective controls*
    - Identify abnormal or malicious activity (e.g., SIEM alerts, anomaly detection)
  - *Corrective controls*
    - Trigger incident response procedures and containment actions
  - *Evidence creation*
    - Generate incident tickets, SIEM logs, vulnerability reports, and response timelines
  - *Risk reduction*
    - Shorten the “dwell time” of attackers and reduce potential impact by ensuring fast detection and response

SECURITY ANALYSTS

- Typical risk management activities
  - *SIEM monitoring*
    - Reviewing real-time alerts for signs of intrusion, misuse, or anomalies
  - *Incident response*
    - Containing and eradicating threats, restoring services, and conducting post-incident reviews
  - *Vulnerability scanning*
    - Running scans to identify system weaknesses and prioritizing remediation
  - *Threat intelligence review*
    - Tracking new and emerging threats relevant to the enterprise
  - *Reporting and documentation*
    - Maintaining evidence for audits and supporting governance reporting

SECURITY ANALYSTS

- Common risks if not managed
  - *Alert fatigue*
    - Too many alerts can overwhelm analysts, leading to missed true positives
  - *Missed indicators*
    - Subtle signs of intrusion (e.g., lateral movement, unusual logins) may go unnoticed
  - *Delayed response*
    - Slow containment allows attackers to escalate and cause more damage
  - *Over-reliance on tools*
    - Assuming automated tools catch everything, without human analysis
  - *Poor documentation*
    - Weak or missing incident records reduce accountability and hinder compliance

DATABASE ADMINISTRATORS (DBAS)

- Responsible for the design, implementation, maintenance, and security of databases that store critical business data
  - Ensure that data remains confidential, accurate, and available to authorized users while preventing loss, corruption, or unauthorized access
- Typical responsibilities include
  - Installing, configuring, and upgrading database systems
  - Managing user accounts, permissions, and access rights
  - Performing backups and validating restore procedures
  - Monitoring performance, tuning queries, and optimizing storage
  - Implementing encryption and other data protection controls
  - Responding to incidents such as outages or data corruption

DATABASE ADMINISTRATORS (DBAS)

- DBAs are central to protecting the confidentiality, integrity, and availability (CIA) of organizational data.
  - Directly influence whether sensitive data remains secure
  - Ensure systems can recover from failure
  - Ensure compliance requirements (e.g., GDPR, HIPAA, SOX) are met

DATABASE ADMINISTRATORS (DBAS)

- Contribution to risk management
  - *Data protection*
    - Enforce encryption, access controls, and least privilege for sensitive data
  - *Availability and resilience*
    - Ensure backups and recovery plans are tested and reliable
  - *Control ownership*
    - Operate preventive controls (encryption, permissions)
    - Operate detective controls (monitoring logs, anomaly detection)
    - Operate corrective controls (restore after failure)
  - *Evidence creation*
    - Backup and restore logs, access control reviews, and encryption status reports serve as audit evidences

DATABASE ADMINISTRATORS (DBAS)

- Typical risk management activities
  - *Backup and restore validation*
    - Running regular restore tests to ensure data can be recovered after an incident
  - *Access management*
    - Defining and reviewing database user roles and privileges to enforce least privilege
  - *Performance monitoring*
    - Tracking database health to prevent outages or bottlenecks that affect critical services
  - *Encryption and data security*
    - Applying encryption at rest and in transit, masking sensitive data, and ensuring compliance
  - *Audit logging*
    - Enabling database logs to detect unauthorized or suspicious activity

DATABASE ADMINISTRATORS (DBAS)

- Common risks if not managed
  - *Data loss*
    - Backups that fail or untested restores that don’t work when needed
  - *Unauthorized access*
    - Weak privilege management leading to insider threats or external breaches
  - *Weak recovery*
    - Lack of tested recovery plans causing extended downtime
  - *Unencrypted sensitive data*
    - Exposure of personal or financial data leading to regulatory fines and reputational damage
  - *Performance failures*
    - Poorly tuned systems causing outages or degraded business operations

NETWORK ENGINEERS

- Responsible for designing, implementing, and maintaining the organization's network infrastructure
  - Including routers, switches, firewalls, VPNs, and wireless systems
  - Ensure that communication across the enterprise is secure, reliable, and efficient.
- Typical responsibilities include
  - Designing network architectures to support business needs
  - Configuring firewalls, intrusion detection/prevention systems, and segmentation
  - Monitoring network performance and troubleshooting connectivity issues
  - Managing VPNs and remote access solutions
  - Ensuring redundancy and failover mechanisms are in place
  - Documenting network diagrams and maintaining configuration baselines

NETWORK ENGINEERS

- Common risks if not managed
  - *Misconfigurations*
    - Incorrect firewall or routing rules creating vulnerabilities
  - *Single points of failure*
    - Lack of redundancy causing major outages
  - *Shadow networks*
    - Unauthorized or undocumented devices introducing unmanaged risk
  - *Data exfiltration*
    - Attackers may use the network to exfiltrate sensitive data undetected
  - *Weak remote access control*
    - Poorly secured VPNs or remote connections enabling intrusions

CLOUD / DEVOPS ENGINEERS

- Responsible for building, automating, and maintaining IT services in cloud environments and continuous delivery pipelines
  - Ensures that infrastructure and applications are scalable, resilient, and compliant while supporting rapid software delivery
  - Instead of hardware, they use systems defined with infrastructure as code tools
- Typical responsibilities include
  - Designing and provisioning cloud resources (compute, storage, networking)
  - Writing and maintaining Infrastructure as Code (IaC) templates
  - Automating deployments via CI/CD pipelines
  - Monitoring performance, reliability, and security in cloud environments
  - Managing identity, access, and permissions for cloud services
  - Ensuring compliance with cloud security frameworks and organizational policies

CLOUD / DEVOPS ENGINEERS

- Cloud environments are highly dynamic environments where risks can escalate quickly if left unchecked
- Their role in risk management includes
  - Preventing misconfigurations
    - For example: public storage buckets, over-permissive IAM roles
  - Embedding controls directly into automated pipelines (“security as code”)
  - Ensuring cloud systems are resilient, redundant, and recoverable
  - Supporting compliance by mapping infrastructure to regulatory standards (e.g., ISO 27001, SOC 2, NIST CSF)

CLOUD / DEVOPS ENGINEERS

- Contribution to risk management
  - *Control ownership*
    - Preventive controls: IaC templates, hardened images, least-privilege IAM roles
    - Detective controls: Continuous monitoring, automated compliance scans
    - Corrective controls: Auto-scaling, automated rollbacks in CI/CD
  - *Evidence creation*
    - Pipeline audit logs, compliance scan results, cloud provider configuration reports, IaC version control history
  - *Risk reduction*
    - Automation reduces human error, enforces consistency, and makes security repeatable at scale
  - *Resilience*
    - Auto-healing and redundant cloud architectures minimize downtime

CLOUD / DEVOPS ENGINEERS

- Typical risk management activities
  - I*aC compliance and drift detection*
    - Validating deployed infrastructure matches approved configurations
  - *CI/CD security*
    - Integrating static analysis, dependency scanning, and secret detection into pipelines
  - *Access and identity management*
    - Enforcing least privilege through IAM or equivalent roles and periodic reviews
  - *Cloud monitoring and logging*
    - Using tools like AWS CloudWatch, Azure Monitor, or GCP Stackdriver for anomaly detection
  - *Disaster recovery planning*
    - Leveraging multi-region replication, snapshots, and automated failover

CLOUD / DEVOPS ENGINEERS

- Common risks if not managed
  - *Misconfigured cloud resources*
    - Publicly exposed databases or storage buckets
  - *Excessive permissions*
    - Overly broad IAM roles leading to privilege abuse
  - *Pipeline vulnerabilities*
    - Compromised CI/CD pipelines allowing malicious code injection
  - *Uncontrolled shadow IT*
    - Teams spinning up cloud resources without governance
  - *Failed auto-recovery*
    - Automation scripts misfiring during outages, making problems worse

PROJECT MANAGERS / PRODUCT OWNERS

- Role in risk management
  - PMs and POs are risk integrators
  - Ensure risks are captured, tracked, and mitigated at the project or product level
    - Their decisions influence whether risks are properly addressed or overlooked
- Contribution to risk management
  - *Risk awareness*
    - Ensure that project plans include risk identification and mitigation
  - *Control alignment*
    - Verify that controls are scheduled and completed
  - *Evidence creation*
    - Maintain risk registers, project reports, and change logs as audit artifacts
  - *Risk communication*
    - Translate technical risks into business terms for stakeholders
  - *Governance support*
    - Enforce adherence to risk frameworks

PROJECT MANAGERS / PRODUCT OWNERS

- Responsible for planning, coordinating, and delivering IT projects and products
  - Ensure conformance with scope, budget, timelines, and stakeholder expectations
  - Ensure that quality and compliance requirements are met
  - Also focus on governance, prioritization, and risk visibility across the lifecycle of a project or product
- Typical responsibilities include
  - Defining project scope, objectives, and deliverables
  - Tracking timelines, budgets, and resource allocations
  - Maintaining communication with business stakeholders and technical teams
  - Managing risks, issues, and dependencies through registers and reviews
  - Prioritizing features and backlog items to align with business value
  - Coordinating testing, release planning, and post-release reviews

PROJECT MANAGERS / PRODUCT OWNERS

- Typical risk management activities
  - *Risk register maintenance*
    - Recording identified risks, their owners, likelihood, and impact
  - *Dependency tracking*
    - Monitoring interdependent systems or deliverables that could create cascading failures
  - *Change and release management*
    - Ensuring proper approvals and testing before go-live
  - *Status and risk reporting*
    - Providing regular updates to leadership on open risks and mitigation progress
  - *Prioritization with risk lens*
    - Balancing business features with technical debt and security backlog

PROJECT MANAGERS / PRODUCT OWNERS

- Common risks if not managed
  - *Ignored technical debt*
    - Security and stability issues accumulate if schedules prioritize only new features
  - *Poor prioritization*
    - Focusing on low-value features while leaving critical vulnerabilities unresolved
  - *Lack of risk transparency*
    - Failure to communicate risks upward can leave executives blindsided
  - *Scope creep*
    - Expanding requirements without addressing capacity or risk implications
  - *Compliance gaps*
    - Missing required controls or documentation due to poor planning

BUSINESS ANALYSTS (BAS)

- Act as bridges between business stakeholders and technical teams.
  - Responsible for gathering, analyzing, and documenting business requirements and ensuring that technology solutions align with business goals, compliance needs, and risk considerations
  - Their role helps prevent misalignment between what is built and what the business (and regulators) actually require
- Typical responsibilities include
  - Gathering and documenting business and functional requirements
  - Translating business needs into technical specifications
  - Modeling business processes and identifying bottlenecks or control gaps
  - Supporting solution design and testing by validating requirements
  - Ensuring compliance and governance needs are captured in requirements
  - Facilitating communication between non-technical and technical stakeholders

BUSINESS ANALYSTS (BAS)

- Ensures risks are considered early in requirements and process design
  - If risks are not identified up front, they propagate into design, development, and operations
- Contribution to risk management
  - *Risk identification*
    - Spot business process weaknesses that could introduce operational or compliance risks
  - *Control definition*
    - Capture requirements for controls
    - For example: “all sensitive data must be encrypted” or “two-person approval required for payments”
  - *Evidence creation*
    - Provide requirement documents, process models, and traceability matrices as proof of risk-aware design
  - *Communication*
    - Ensure stakeholders understand risk of business and technical decisions
  - *Governance alignment*
    - Map requirements to frameworks and standards
    - For example:, PCI DSS for payments, GDPR for data protection

BUSINESS ANALYSTS (BAS)

- Typical risk management activities
  - *Business process modeling*
    - Creating models to reveal single points of failure, manual dependencies, or role confusion
  - *Requirements validation*
    - Checking that risk, compliance, and resilience needs are included in solution requirements
  - *Traceability*
    - Linking business requirements to test cases and controls, ensuring nothing is missed
  - *Stakeholder analysis*
    - Identifying Responsible, Accountable, Consulted, Informed (RACI) roles to clarify accountability
  - *Risk-based prioritization*
    - Helping prioritize requirements that reduce critical risks

IT AUDITORS

- Provide independent assurance that IT systems, processes, and controls are designed and operating effectively to manage risk
  - Review evidence from across IT roles, evaluate compliance with frameworks and regulations, and report findings to leadership
  - Auditors do not build or run systems, they assess and validate how others manage risk
- Typical responsibilities include
  - Planning and conducting IT audits based on regulatory or organizational requirements
  - Reviewing logs, reports, and controls operated by IT staff
  - Testing the effectiveness of preventive, detective, and corrective measures
  - Identifying gaps, weaknesses, and non-compliance issues
  - Writing audit reports with findings and recommendations
  - Following up on remediation efforts and control improvements

IT AUDITORS

- Provid an independent “second line of risk defence”
  - Ensures that controls owned by others are in place, effective, and aligned with policies, standards, and regulations
- Contribution to risk management
  - *Independent assurance*
    - Validate that risks are being managed as claimed
  - *Control effectiveness testing*
    - Assess whether controls work as intended (e.g., restore tests, access reviews)
  - *Evidence review*
    - Examine patch reports, logs, test cases, and other artifacts for sufficiency and reliability
  - *Risk communication*
    - Escalate findings to management and boards in business-relevant language
  - *Governance support*
    - Ensure alignment with ISACA, COBIT, NIST, ISO, and regulatory frameworks

IT AUDITORS

- Typical risk management activities
  - *Audit planning and scoping*
    - Identifying high-risk areas to focus on
  - *Control testing*
    - Re-performing or reviewing key controls such as backups, access reviews, and monitoring
  - *Sampling and evidence review*
    - Checking a representative set of logs, reports, or system outputs
  - *Reporting*
    - Documenting gaps, deficiencies, and strengths in control environments
  - *Follow-up and verification*
    - Ensuring remediation actions are completed and effective

IT AUDITORS

- Common risks if not managed
  - *Undetected control failures*
    - If audits are weak or infrequent, broken controls may persist
  - *Regulatory penalties*
    - Missing or incomplete audits can lead to fines or sanctions
  - *Management blind spots*
    - Without independent assurance, executives may think risks are covered when they are not
  - *Inconsistent assurance*
    - Poor audit methodologies or incomplete evidence review undermine reliability
  - *Over-reliance on self-reporting*
    - Accepting control owners' claims without evidence verification increases residual risk

CROSS-ROLE COORDINATION

- These roles do not operate in isolation
- They need to collaborate and communicate in order to implement an overall risk management program
- We will explore this aspect of risk management in another module

Q&A AND OPEN DISCUSSION