RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

ISACA AND DRI FRAMEWORKS

The primary objective of this bootcamp is to prepare you for assuming risk and resilience job responsibilities
The secondary objective is to help prepare you for certification under either

- ISACA: International Systems Audit and Control Association
  - Provides risk management certification
- DRII: Disaster Recovery Institute International
  - Certifies resilience professionals

© 2025 Innovation In Software Corporation

ISACA FRAMEWORK

- For this course:
  - The main risk concepts presented align with the ISACA framework
  - Relevant risk and resilience issues beyond the scope of ISACA/DRII
  - The course material provides a larger context for the concepts
- Other standards
  - The ISACA is intended to align with other risk standards
    - ISO 31000 Risk Management
    - COSO Enterprise Risk Management
    - Other specific standards like NIST Cybersecurity and others
  - These will be supplied as references when possible

© 2025 Innovation In Software Corporation

ISACA FRAMEWORK

- The main areas covered by the Framework are
- Introducing the Risk IT Framework
  - The imperative for Risk IT
  - Definitions and terminology
  - Purpose of the Risk IT Framework
  - Target audience and stakeholders
- Risk IT Framework principles
  - Connect to enterprise business or mission
  - Align with enterprise risk management
  - Balance costs and benefits
  - Promote ethical and open communication
  - Establish tone at the top and accountability
  - Use a consistent approach aligned to strategy

© 2025 Innovation In Software Corporation

ISACA FRAMEWORK

- Framework components and alignment with COBIT
  - Components of the Risk IT Framework
  - Alignment of COBIT with the Risk IT Framework
  - Application of the Risk IT Framework independent of COBIT
- Essentials of risk governance
  - Risk appetite, tolerance and risk capacity
  - Stakeholders of IT risk management
  - Risk culture
- Essentials of risk management
  - Setting the context and scoping risk management
  - Understanding the risk management workflow

© 2025 Innovation In Software Corporation

ISACA FRAMEWORK

- Essentials of risk assessment
  - Risk identification
  - Risk analysis
  - Evaluating the business impact of identified risks
  - IT risk scenarios
- Risk awareness, reporting and communication
  - Benefits of risk awareness and communication
  - Risk reporting and communication
  - Key risk indicators

© 2025 Innovation In Software Corporation

ISACA FRAMEWORK

- Essentials of risk response
  - Risk avoidance
  - Risk mitigation
  - Risk sharing or transfer
  - Risk acceptance
  - Risk aggregation
  - Risk response selection and prioritization
- Relevant extracts of the framework are included in the readings folder

© 2025 Innovation In Software Corporation

DRI INTERNATIONAL BEST PRACTICES

- Publishes a lifecycle framework
  - Called the *Professional Practices for Business Continuity Management*
  - IBCM/resilience counterpart to ISACA's Risk IT
  - A structured body of knowledge used to build, run, test, and improve an enterprise resilience program
- What the DRI framework covers (the 10 Professional Practices)
- Program initiation & management
  - Establish the need for a business continuity program
  - Obtain support and funding for the business continuity program
  - Build the organizational framework to support the business continuity program
  - Introduce key concepts, such as program management, risk awareness, identification of critical functions/processes, recovery strategies, training and awareness, and exercising/testing

© 2025 Innovation In Software Corporation

DRI INTERNATIONAL BEST PRACTICES

- Risk assessment
  - Identify risks that can adversely affect an entity's resources or image
  - Assess risks to determine the potential impacts to the entity, enabling the entity to determine the most effective use of resources to reduce these potential impacts
- Business impact analysis
  - Identify and prioritize the entity's functions and processes in order to ascertain which ones will have the greatest impact should they not be available
  - Assess the resources required to support the business impact analysis process
  - Analyze the findings to ascertain any gaps between the entity's requirements and its ability to deliver those requirements

© 2025 Innovation In Software Corporation

DRI INTERNATIONAL BEST PRACTICES

- Business continuity strategies
  - Select cost-effective strategies to reduce deficiencies as identified during the risk assessment and business impact analysis processes
- Incident response
  - Develop and assist with the implementation of an incident management system that defines organizational roles, lines of authority and succession of authority
  - Define requirements to develop and implement the entity's incident response plan
  - Ensure that incident response is coordinated with outside organizations in a timely and effective manner when appropriate

© 2025 Innovation In Software Corporation

DRI INTERNATIONAL BEST PRACTICES

- Plan development and implementation
  - Document plans to be used during an incident that will enable the entity to continue to function
- Awareness and training programs
  - Establish and maintain training and awareness programs that result in personnel being able to respond to incidents in a calm and efficient manner
- Business continuity plan exercise, assessment, and maintenance
  - Establish an exercise, assessment and maintenance program to maintain a state of readiness

© 2025 Innovation In Software Corporation

DRI INTERNATIONAL BEST PRACTICES

- Crisis communications
  - Provide a framework for developing a crisis communications plan
  - Ensure that the crisis communications plan will provide for timely, effective communication with internal and external parties
- Coordination with external agencies
  - Establish policies and procedures to coordinate incident response activities with public entities

© 2025 Innovation In Software Corporation

OVERLAP

- There are clearly some overlaps between the two frameworks
  - ISACA focuses on categorizing and governing IT risk end to end
    - Looks at benefit/value, program/project delivery, operations/security
    - Provides risk terminology and an oversight model
  - DRI focuses on continuity and resilience execution
    - Derives targets (via BIA/risk), chooses strategies, implements plans, trains, exercises, and keeps improving
- Integration
  - Use ISACA to frame and report risk (governance, appetite, domains).
  - Use DRI to operationalize resilience into actions
  - This pairing reflects how banks are examined today by regulators
  - Consistent with ISO's organizational-resilience guidance.

© 2025 Innovation In Software Corporation

INTEGRATION

ISACA Risk IT focus	What it means	DRI Professional Practice(s) that operationalize it	Tangible outputs/evidence
I&T governance & risk context (risk appetite, roles, oversight)	Set tone, accountability, and reporting for tech risk across the enterprise	**1. Program Initiation & Management**	Program charter/RACI, policy/standards, risk appetite statement, governance calendar
Benefit/value enablement risk	Tech may not deliver intended business value	**2. Risk Assessment**, **3. BIA**, **4. BC Strategies**	Risk register (missed-benefit scenarios), BIA impact curves, strategy options & cost/benefit
IT program & project delivery risk	Change initiatives miss scope/time/cost/quality	**6. Plan Development & Implementation**, **7. Awareness & Training**, **8. Tests & Exercises** (for new capabilities)	SDLC gates with continuity/security criteria, rollout plans, training records, pilot/exercise results
IT operations & service-delivery risk	Day-to-day outages, capacity shortfalls, control failures	**5. Incident Response**, **6. Plan Dev & Impl**, **8. Tests & Exercises**, **9. Maintenance & Improvement**	Runbooks, on-call playbooks, post-incident reports (PIR), exercise reports, corrective-action tracking
Cyber & information security risk	Threats to confidentiality, integrity, availability	**2. Risk Assessment**, **5. Incident Response**, **8. Tests & Exercises**	Threat/risk assessments, IR procedures, tabletop/technical drill artifacts, metrics (MTTD/MTTR)
Risk response & monitoring	Treat, accept, transfer, avoid; monitor KPIs/KRIs	**9. Program Maintenance & Improvement**	KRIs dashboards, lessons-learned → tickets → verified fixes, periodic program reviews
Ecosystem/third-party risk	Vendors/fintechs impact resilience & security	**10. Coordination with External Agencies** (plus 2/4/6/8 woven through vendor lifecycle)	Due diligence packs, contract RTO/RPO & test rights, joint exercises, incident notification evidence

© 2025 Innovation In Software Corporation

COBIT

- Referenced in the framework
  - COBIT (Control Objectives for Information and Related Technologies)
    - ISACA's framework for the governance and management of enterprise IT
    - Gives boards, executives, and technology leaders a common language, a set of objectives, and practical components to ensure IT creates value, manages risk, and achieves compliance
  - What COBIT is for
    - Governance: Set direction, evaluate options, and monitor results so that IT can support business goals
    - Management: Plan, build, run, and monitor IT services and change programs in a controlled way
    - Assurance & alignment: Map policies, controls, and metrics across other standards (NIST CSF, ISO/IEC 27001, ITIL, PCI DSS)

© 2025 Innovation In Software Corporation

COBIT STRUCTURE

- Principles: For governance systems
  - Tailored to enterprise needs and end-to-end coverage
- Objectives model
  - Governance objectives (EDM) – Evaluate, Direct, Monitor
- Management objectives grouped into domains:
  - APO: Align, Plan, Organize (strategy, risk, architecture, sourcing).
  - BAI: Build, Acquire, Implement (change, projects, configuration, release)
  - DSS: Deliver, Service, Support (operations, continuity, security ops, incident/problem)
  - MEA:Monitor, Evaluate, Assess (performance, compliance, internal control)

© 2025 Innovation In Software Corporation

COBIT STRUCTURE

- Components (“enablers”)
  - Processes, organizational structures
  - Policies & procedures
  - Information
  - Culture/behavior
  - People & skills
  - Services/infrastructure/applications

© 2025 Innovation In Software Corporation

COBIT STRUCTURE

- Performance management
  - Maturity/capability levels and metrics to track whether objectives are being met.
- Design factors
  - Enterprise strategy
  - Risk profile
  - Regulatory requirements
  - Sourcing model
  - Technology adoption

© 2025 Innovation In Software Corporation

COBIT

- Risk and resilience teams use COBIT to support
  - Clear ownership
    - Ties controls to specific enterprise objectives
  - Evidence-ready:
    - Points to artifacts examiners expect
    - Risk registers
    - BIA/RTO-RPO
    - Change tickets
    - Restoration tests
    - Key Risk Indicators (KRIs)
    - Compliance reports

© 2025 Innovation In Software Corporation

ISACA FRAMEWORK

- Principles are in the readings section

© 2025 Innovation In Software Corporation

ISACA DEFINITIONS

- To be consistent with ISACA, we will use their definitions
  - Enterprise
    - A group of individuals working together for a common purpose, typically within the context of a business organization, such as a corporation, partnership, limited liability company, government or public agency, charity, nonprofit or trust
  - Organization
    - The structure or arrangement of interrelated components of an enterprise, defined by a particular scope
  - Business or mission
    - The strategic purpose for which the organization exists
    - In the scope of risk IT, an enterprise typically sets strategic objectives, such as delivering a product or service, meeting sales targets and generating revenue.
    - The purpose of a mission-driven organization may be similar to a business enterprise, but often operates to meet a mission, or nonprofit objectives.

© 2025 Innovation In Software Corporation

ISACA DEFINITIONS

- Governance: The framework and system ensuring that:
  - Stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives
  - Strategic direction is set, and goals are prioritized and supported through appropriate, timely decision making
- Risk
  - The combination of the likelihood of an event and its impact
- Information security
  - The enterprise discipline that protects information against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-availability when required (availability)

© 2025 Innovation In Software Corporation

DRI STATEMENTS

- The DRI has similar statements and definitions
- These are in the supplied documents in the repository
  - The Professional Practices for Business Continuity Management
  - International glossary for Resilience

© 2025 Innovation In Software Corporation

DRI STATEMENTS

- Program Management
  - Establish the need for a business continuity program
  - Introduce key concepts, such as
    - Program management
    - Risk awareness
    - Impact to critical functions/processes
    - Recovery strategies
    - Training and awareness
    - Exercising/testing
- Risk Assessment
  - Identify risks that could impact an entity's resources, processes or reputation
  - Assess risks to determine the potential impacts to the entity, enabling the entity to determine the most effective means of reducing them

© 2025 Innovation In Software Corporation

DRI STATEMENTS

- Business Impact Analysis
  - Identify and prioritize all of the entity's functions, processes, and dependencies in order to determine the greatest impact upon the entity should the functions not be available
  - This analysis should be retained and available to assist the entity in understanding incidents and/or the resulting consequences
    - Quantify the impact on the entity, its services, and the affected parties
  - Analyze, document, and communicate the findings to highlight all gaps between the entity's requirements and its current capabilities
- Business Continuity Strategies
  - Select strategies to reduce gaps as identified during the risk assessment and business impact analysis
  - Identify the major functions of the entity, including potential third-party service providers, with the support of the responsible party for the business impact analysis

© 2025 Innovation In Software Corporation

DRI STATEMENTS

- Incident Preparedness and Response
  - Understand the types of incidents that could threaten life, property, operations, or the environment and their potential impacts
  - Establish and maintain capabilities to protect life, property, operations, and the environment from potential incidents through the implementation of an incident management system to command, control, and coordinate response, continuity, and recovery activities with internal and external resources
- Plan Development and Implementation
  - Document plans to be used during an incident that will enable the entity to continue to function
  - Define the exercise/testing criteria to validate that the plans will accomplish the desired goal

© 2025 Innovation In Software Corporation

DRI STATEMENTS

- Awareness and Training Programs
  - Establish and maintain training and awareness programs that result in personnel being able to respond to disruptive incidents in a calm and efficient manner
- Business Continuity Plan Exercise/Test, Assessment, and Maintenance
  - Establish a business continuity plan exercise/test, assessment and maintenance program to maintain a state of readiness of the entity
- Crisis Communications
  - Create and maintain a crisis communications plan
  - Ensure that the crisis communications plan will provide for timely, effective communication with internal and external parties
- Coordination with External Agencies and Resources
  - Establish policies and procedures to coordinate response activities with applicable public entities and private resources in accordance with *Incident Preparedness and Response*

© 2025 Innovation In Software Corporation

FRAMEWORK INTEGRATION VIEW

- Purpose of Integration
  - The two domains complement each other by providing a more complete solution to managing, controlling and responding to potential risk and risk related events
    - ISACA = governance lens: defines IT risk terminology, appetite, tolerance, and alignment with business strategy
    - DRI = execution lens: operationalizes resilience with lifecycle practices (assessment, BIA, incident response, testing, improvement)
  - ISACA focuses on categorizing and governing IT risk end-to-end (value delivery, project delivery, operations, security)
  - DRI focuses on continuity and resilience execution: identify risks, perform BIAs, select strategies, develop and exercise plans, communicate, and coordinate externally
    - ISACA tells you what needs to be governed and reported.
    - DRI tells you how to operationalize resilience actions.

© 2025 Innovation In Software Corporation

ORGANIZATIONAL CULTURE

- Why culture matters in resilience and risk management
  - Resilience and risk management are not just technical, they are organizational
  - Systems and plans only work if the people in the enterprise value risk awareness, act responsibly, and follow through in a crisis
  - Risk assessments are useful only when they are acted on
  - Culture influences how risks are identified, reported, and addressed before they escalate
-

© 2025 Innovation In Software Corporation

TONE AT THE TOP

- Tone at the Top
  - Defined as the attitude and actions of senior leadership toward governance, ethics, and risk management
  - Sets the standard for acceptable behavior across the organization
  - When executives model accountability and openness, employees are more likely to report issues and follow established controls
  - When leadership ignores or downplays risks, resilience suffers; incidents are hidden, controls bypassed, and recovery delayed

© 2025 Innovation In Software Corporation

TONE AT THE TOP

- Tone at the Top
  - Elements of risk-aware and resilient culture
    - *Risk Awareness:* employees understand how their role affects risk and recovery
    - *Accountability*: clear ownership of controls, incidents, and recovery actions
    - *Open Communication:* safe channels to escalate problems without fear
    - *Continuous Learning:* post-incident reviews are used to improve, not blame
    - *Ethics and Trust:* trust in leadership decisions builds collective commitment to recovery
  - Organizations with a strong resilience culture recover faster because employees already know:
    - What matters, who decides, and how to act under stress

© 2025 Innovation In Software Corporation

IT RISK AND I&T RISK

- Why ISACA moved to I&T risk
  - Information itself is a critical asset
    - Its quality, availability, confidentiality, and integrity are sources of business risk
  - Technology now extends beyond traditional IT
    - Now includes cloud, IoT, AI, robotics, and fintech ecosystems
  - Digital business models blur the line between IT and business
    - Risk must be managed across both domains, not in silos
  - Resilience depends on enterprise-wide coordination, not only IT controls
  - I&T risk is a broader, business-centric lens for risk and resilience management

© 2025 Innovation In Software Corporation

DIFFERENCE EXAMPLES

Scenario	Treated as IT Risk	Treated as I&T Risk
Server outage	System downtime affecting availability; resolved by IT ops.	Considered as part of enterprise resilience — customer impact, reputational harm, regulatory breach if SLAs are missed.
Data breach	Breach of IT systems / cybersecurity failure.	Broader concern for data governance, privacy compliance, cross-border data flow, legal & reputational impacts.
AI decision bias	(Not covered under traditional IT risk.)	An *I&T risk*: misuse of information (data bias) and technology (AI model) affecting business ethics, regulation, trust.
Cloud vendor failure	Technical vendor risk.	An *I&T risk*: third-party dependency affecting strategic digital service delivery, contractual compliance, and resilience posture.
Inaccurate analytics	Data quality issue (if seen by IT).	Information risk: poor data accuracy affects strategic decisions, financial reporting, and risk appetite metrics.

© 2025 Innovation In Software Corporation

IT RISK AND I&T RISK

- The distinction means:
  - When you assess “IT risk,” you are examining technical failure modes
  - When you assess “I&T risk,” you are assessing business risk arising from the enterprise’s entire digital environment
    - Including data misuse, algorithmic decisions, cloud dependence, or third-party integration.
- In governance terms:
  - IT Risk: managed operationally by IT chief risk officer
  - I&T Risk: governed strategically by the enterprise risk committee
    - IT risk is a subset

© 2025 Innovation In Software Corporation

IT RISK AND I&T RISK

Aspect	IT Risk	I&T Risk
Scope	IT infrastructure & systems	Enterprise-wide information & technology ecosystem
Focus	Technical failures & vulnerabilities	Business risks arising from digital transformation & data use
Responsibility	IT & security functions	Enterprise leadership, risk & compliance, business lines
Governance model	IT governance / operational risk	Enterprise governance of I&T (COBIT 2019 EGIT)
Relationship to resilience	Disaster recovery, incident response	End-to-end resilience: information, people, processes, partners

© 2025 Innovation In Software Corporation

Q&A AND OPEN DISCUSSION

© 2025 Innovation In Software Corporation