Your fastest way to learn. Why wait?

FIREBRAND

ISACA

CRISC Certification (Certified in Risk and Information Systems Control)

Courseware Version 4.1

KIT CODE: K-313-01

CRISC™

Certified in Risk and Information Systems Control™

Firebrand Custom Designed Courseware

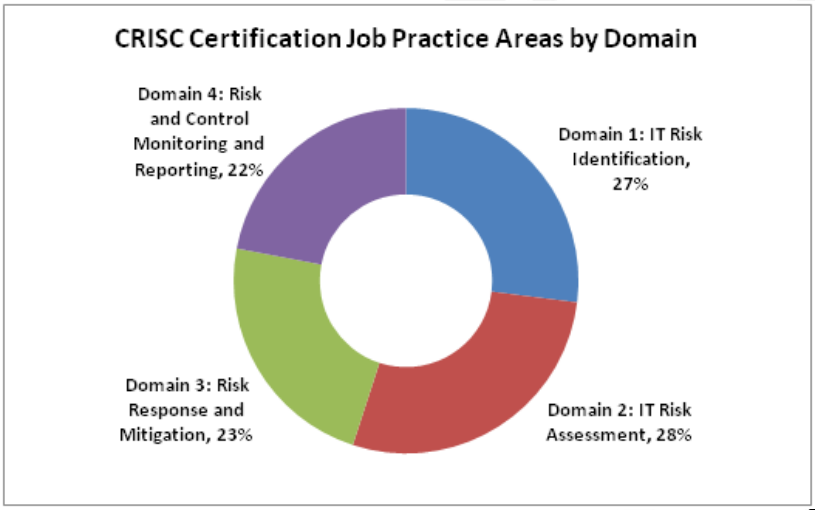
Logistics

- Start Time
- Breaks
- End Time
- Fire escapes
- Instructor
- Introductions

The Examination

- 150 multiple choice questions
- Four hours to complete
- Computer based
  - Various test centers
  - Exam window from:
    - May1 – June 30
    - Aug 1 – Sept 30
    - Nov 1 – Dec 31

Job Practice Areas



Introduction to Risk

Risk

- Risk is defined as the probability of an event and its consequence
  - Often seen as an adverse event
  - Impacts assets
  - Exploits vulnerabilities

Governance and Risk Management

- Governance is accountability for the protection of assets of the organisation.
  - Board of Directors
  - Senior Management

Governance in each Department

- Financial accountability
- Operational effectiveness
- Legal and human resources compliance
- Social responsibility
- Governance of IT investment, operations and control

Risk and Governance

- Risk management supports governance
- Management requires accurate information to:
  - Understand risk
  - Consider risk mitigation

Governance of IT

- Directs the current and future use of IT
  - Evaluation of IT
  - Direction of IT
  - Control of IT

Value Creation

- Ensure that IT creates value for the organisation
  - Resource optimisation
  - Benefits realisation
  - Risk optimisation

Four Questions of Governance

1. Are we doing the right things?
2. Are we doing them the right way?
3. Are we getting them done well?
4. Are we getting the benefits?

Risk Governance Objectives

1. Establish and maintain a common view of risk
2. Integrate risk management into the enterprise
3. Make risk-aware business decisions
4. Ensure that risk management controls are implemented and operating correctly

Enterprise Risk Management

- Risk must be managed in a consistent manner across the enterprise
- A risk in one area is a threat to all other areas of the enterprise

Risk Standards

- ISO/IEC 31000
- ISO/IEC 27005
  - "Information security risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation"

Risk Levels

- Affected by:
  - Intent and capability of a threat source
  - Value of an asset
  - Presence of a vulnerability
  - Reliance on supply chain or third party
  - Financing or debt
  - Partners

Forward Thinking

- Risk Management foresees challenges that could affect business objectives
  - Lowers the likelihood (chances)
  - Lowers the impact
  - Maximises opportunities

IT Risk Relevance

- First of all it must be remembered that IT risk is a subset of business risk. The impact of an IT incident is primarily measured by its impact on the business, not just by its impact on IT.

Risk Tiers

- Risk must be considered at all levels
  - Strategic risk – changes to market
  - Tactical risk – changes in business operations
  - Operational risk – challenges with IT systems

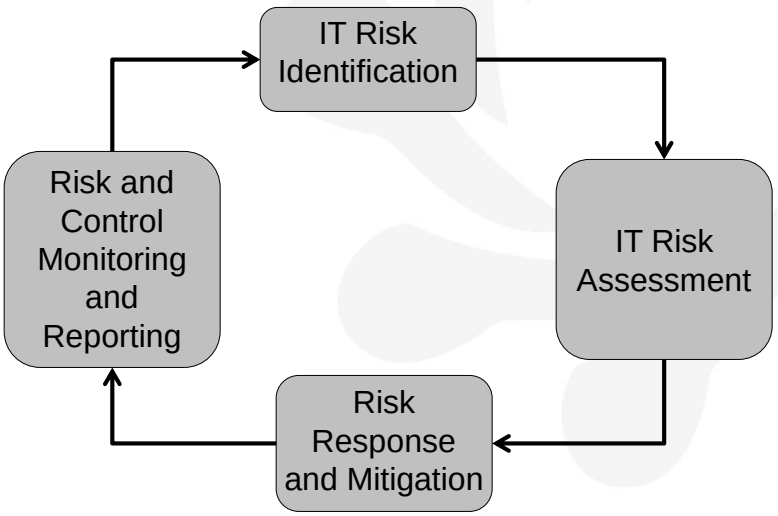
Context of Risk

- Factors that must be considered when evaluating risk:
  - Mission of the organisation
  - Regulations
  - Risk appetite of senior management
  - Budget

Other Risk Factors

- Changes in economic conditions
- Changes in market trends
- Emergence of new competition
- Impact of new legislation
- Natural disasters
- Legacy equipment
- Strained labour relations

Risk Management Lifecycle



Risk Practitioner (Agenda)

- The Risk Practitioner may examine areas such as:
  - Business continuity
  - Project risk
  - IT and IS controls
  - IS audit
  - Information security
  - Change management

Business Continuity

- Risk assessment supports business impact analysis (BIA) and the creation of a business continuity plan (BCP)
- BCP is concerned with the preservation of critical business functions in the event of an adverse event (risk)
- The risk practitioner evaluates the effectiveness of the BCP to recover from an incident

IT Risk and IS Audit

- Audit provides assurance to management on the effectiveness of IS controls
  - Adequate controls
  - Controls commensurate with risk
  - Objectivity and skill of audit personnel

IT Risk and Information Security

- Risk-based, cost-effective controls
- Incorrect risk assessment leads to controls that are:
  - Incorrectly designed
  - Poorly implemented
  - Improperly operated
- Controls are justified by risk and should be traceable back to the risk they are designed to mitigate

Control Risk

- Ineffective controls
- Wrong type of control
- Improper operation of control
- Lack of monitoring of control

Project Risk

- Project failure
  - Over budget
  - Late
  - Failure to meet customer needs
- Results in:
  - Loss of market
  - Failure to seize opportunities
  - Impact on customers, shareholders

Change Risk

- Changes may affect risk status:
  - Changes in technology
  - Patches
  - Changes in configuration
  - Changes in operational environment
- Manage change

Summary

- Governance
- Enterprise view
- Focus on business not just IT
- Add value

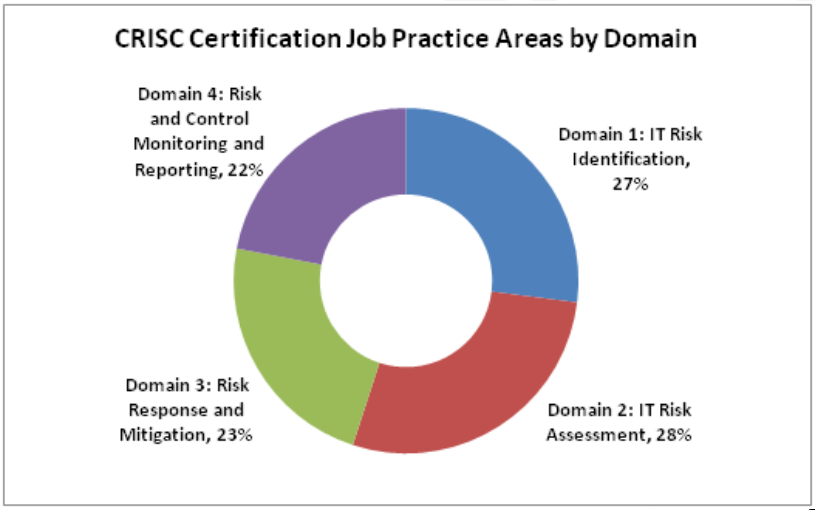
CRISC™

Certified in Risk and Information Systems Control™

Firebrand Custom Designed Courseware

IT Risk Identification

Job Practice Areas



IT Risk Identification Objective

- Identify the universe of IT risk to contribute to the execution of the IT risk management strategy in support of business objectives and in alignment with the enterprise risk management (ERM) strategy.

Key Topics

1.1 Collect and review information, including existing documentation, regarding the organisation's internal and external business and IT environments to identify potential or realised impacts of IT risk to the organisation's business objectives and operations.

1.2 Identify potential threats and vulnerabilities to the organisation's people, processes and technology to enable IT risk analysis.

1.3 Develop a comprehensive set of IT risk scenarios based on available information to determine the potential impact to business objectives and operations.

Key Topics (continued)

1.4 Identify key stakeholders for IT risk scenarios to help establish accountability.

1.5 Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into the enterprise-wide risk profile.

1.6 Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with business objectives.

1.7 Collaborate in the development of a risk awareness program, and conduct training to ensure that stakeholders understand risk and to promote a risk-aware culture.

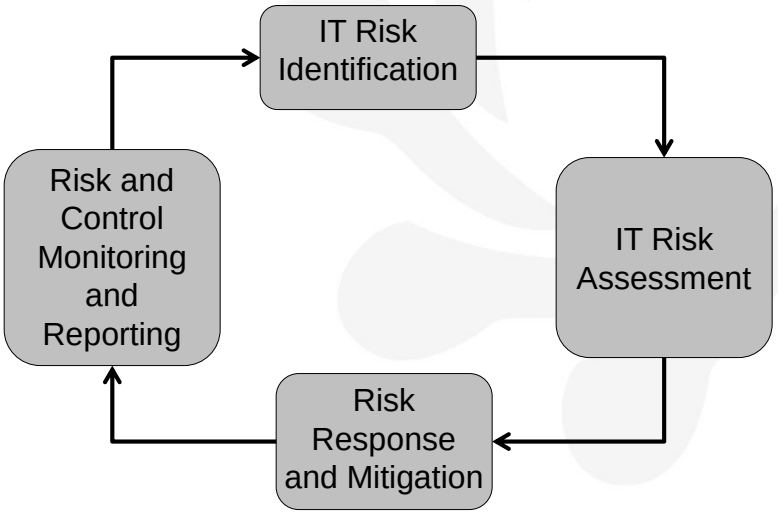
Learning Objectives

- Identify relevant frameworks, standards and practices
- Apply risk identification techniques
- Distinguish between threats and vulnerabilities
- Identify relevant stakeholders
- Discuss risk scenario development tools and techniques

Learning Objectives (continued)

- Explain the meaning of key risk management concepts, including risk appetite and risk tolerance
- Describe the key elements of a risk register
- Contribute to the creation of a risk awareness program

Risk Management Lifecycle



The Methodology of Risk Management

- Structured
- Enterprise-wide
- Consistent
- Continuously improving

Risk Practitioner Responsibilities

- Evaluate the effectiveness of the organisation's current risk management processes
- Based on acceptable and recognised good practices:
  - COBIT 5 for Risk
  - COSO
  - ISO 31000
  - NIST SP800-39
  - ISO 27005

Risk Identification

- To identify the risk is to:
  - Determine the value of the assets bring protected
  - Determine the threats to those assets
  - Identify the vulnerabilities those assets are subject to
  - Document controls currently in place
  - Understand the consequences of risk events

Risk Identification Output

- A list of incident scenarios with their consequences related to assets and business processes

Indicators of a Good IT Risk Management Program

- Comprehensive
- Complete
- Auditable
- Justifiable
- Legal
- Monitored
- Enforced
- Up-to-date
- Managed

Methods to Identify Risk

- Historical
  - What has happened previously
- Systematic
  - Expert opinion
  - Examine a business process to identify possible points of failure
- Inductive (Theoretical) analysis
  - New technology or process review to determine points of attack

Business-related IT Risk

- Investment – provide value for money
- Access and Security – loss of sensitive data
- Integrity – risk of inaccurate data
- Relevance – wrong information at wrong time
- Availability – loss of critical systems/data
- Infrastructure – legacy, inflexible
- Project ownership – lack of project support

Risk Register

- Document and track all identified risk in one place. Risk may have been identified in:
  - Audit reports
  - Incident management
  - Public media
  - Annual reports
  - Press releases
  - Vulnerability assessments and penetration tests
  - Business continuity and disaster recovery plans
  - Interviews and workshops
  - Threat intelligence services

Gathering Risk Data through Interviews

- Risk:
  - Inaccurate information
  - Exaggeration
- Good Practice:
  - Do research first
  - Time limits
  - Prepare questions in advance
  - Talk to all levels of staff

Risk Culture and Communication

- Do risk practices align with organisational culture?
- Is compliance enforced?
- Tendency to hide mistakes?
- Attitude/Appetite towards risk
  - Embrace risk
  - Discourage risk
  - Ignore risk

Communicating Risk

- Provides ability of management to provide governance and effective risk response
- Avoid a false sense of security
- Avoid inconsistent approach to risk management and acceptance
- Avoid accusations that the organisation is trying to hide something

Risk Communications

- Assists with:
  - Business continuity and disaster recovery
  - Compliance and policy reviews
  - Security awareness programs
  - Ensuring that risk management is built into all new business processes, applications and ventures

RACI Models

- Responsible – the individual responsible for managing the risk - getting the job done
- Accountable – the individual that ensures the job was done –oversight of responsible person
- Consulted – provides advice, feedback, input
- Informed – not directly responsible for the task but are informed of status and progress

Determination Of Risk Acceptance Levels

- A Senior Management decision
- What level of risk is management willing to 'live' with
  - Greater risk means greater reward
  - Less risk is more comfortable, stability
  - 'How fast would you drive on an icy road?'
    - A personal opinion
    - Opinions can change with age, experience

Effect of Culture on Risk

- Influences behaviours
  - Openness?
  - Fear?
  - Blame?
  - Ruthless?
  - Careless?

Ethics

- Personal beliefs of ‘right and wrong’
  - May not be the same as organisational ethics or as ethics stated in policy
- May lead to fraud
- Perception of being treated ‘fairly’ or ‘unfairly’

Compliance with Laws and Regulations

- Vary by country / jurisdiction / industry
- Know which laws that apply
- Liability if not compliant

Industry Standards

- Standards for industry sectors – not laws
  - PCI-DSS (payment card industry – data security standard)
    - Set of contractual obligations for protecting payment (i.e., credit card) card data
    - Failure to be compliant could lead to risk of financial penalties

Information Security

- Risks to Information are often described using:
  - Confidentiality
  - Integrity
  - Availability
  - Authentication

Risk Practitioner Concerns

- Protecting data, information systems and business processes requires:
  - Separation of duties
  - Least privilege / need to know
  - Job rotation
  - Mandatory vacations
  - Maintaining data in a secure condition

IAAA _ Identity Management

- Manage identities of personnel that have access to data, information systems, buildings, etc.,
- Identification
- Authentication
- Authorisation
- Accounting / Auditing

Asset Value

- Tangible assets
  - Cash, equipment, buildings
- Intangible assets
  - Reputation, brand, morale
- Value can change as assets increase/decrease in importance

Threat Identification

- Intentional
- Accidental
- Circumstantial
- Natural
- Utilities
- Equipment
- Man-made
- Internal
- External
- Supply chain
- Market conditions
- Financial conditions
- New technologies

Vulnerability Identification

- Weaknesses, gaps, missing or ineffective controls
- Network vulnerabilities
- Buildings
- Staff inexperience
- Culture
- Applications
- Inefficient processes

Vulnerability Assessments – Pen Tests

- Seek out potential points of failure
  - Compare against known problems
  - Try to ‘break-in’
  - Simulate the approach of an attacker
  - Test effectiveness of controls and response procedures

Risks Related to Business Processes

- People related risks
  - Staff
- Technology related risks
  - Acquisition, Maintenance,
- Operational risk
  - Fraud
- Protection of Intellectual Property
  - Fraud

Risk Scenario Development

- Scenarios are often used to understand and evaluate risk
- A risk scenario is a description of a possible event that, when occurring, will have an uncertain impact on the achievement of the enterprise's objectives. The impact could be positive or negative
  - Definition from COBIT 5 for Risk

Risk Scenarios

- Possible risk
  - Creative
  - Threat modeling
  - Realistic
  - Top-down approach – risk to business goals
  - Bottom-up approach – risk related to failure of a information system

Risk Ownership

- Management must accept ownership for risk
  - Responsible to ensure risk is acknowledged and managed properly
  - Update risk register

Management Responsibility

- Determine risk acceptance level
  - Risk tolerance (deviation from risk acceptance level)
- Ensure controls are adequate
  - Provide budget
  - Support
  - Enforcement

Risk Acceptance

- Risk Acceptance may be influenced by:
  - Regulations
  - Cost/benefit analysis
  - Availability of controls
  - Risk versus reward considerations

Risk Awareness

- Awareness affects:
  - Culture
  - Ethics
  - Direction and guidance

Risk Awareness Topics

- Ensure risk is understood and well-known
- IT risks are identified
- The enterprise recognises and manages risk
  - Risk factors
  - Risk impact
  - Risk controls

Summary

- The risk practitioner must ensure that is risk is identified in order to support the following steps of risk assessment and response
- Requires understanding business goals, management priorities and operational risks
- Creation of risk register

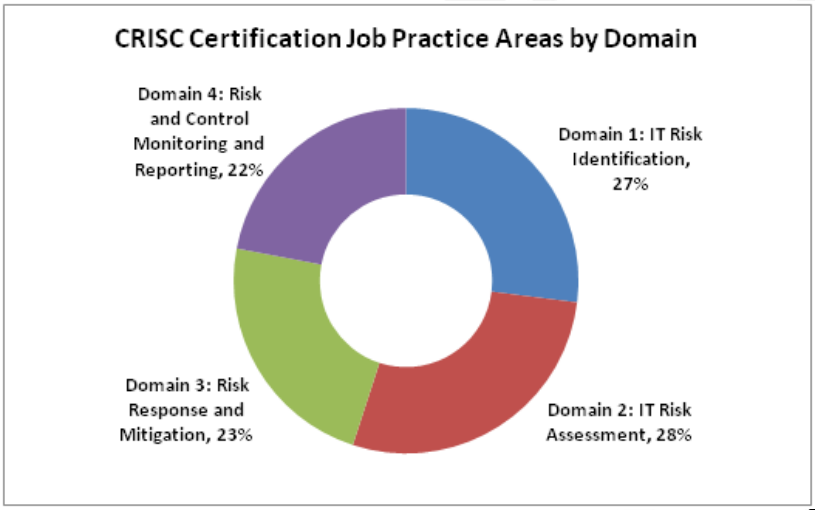
CRISC™

Certified in Risk and Information Systems Control™

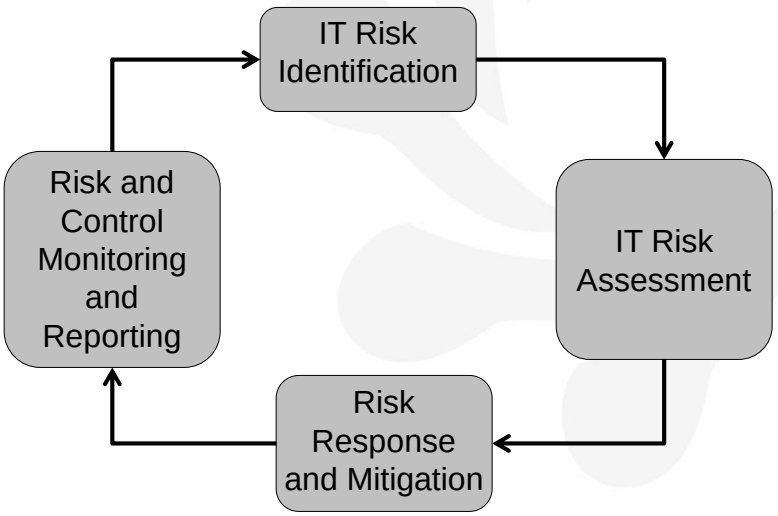
Firebrand Custom Designed Courseware

IT Risk Assessment

Job Practice Areas



Risk Management Lifecycle



IT Risk Assessment Objective

- Analyse and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based decision making

Key Topics

2.1 Analyse risk scenarios based on organisational criteria (e.g. organisational structure, policies, standards, technology, architecture, controls) to determine the likelihood and impact of an identified risk.

2.2 Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.

2.3 Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment.

Key Topics (continued)

2.4 Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability.

2.5 Communicate the results of risk assessments to senior management and appropriate stakeholders to enable risk-based decision making.

2.6 Update the risk register with the results of the risk assessment.

Learning Objectives

- Identify and assess risk assessment techniques
- Analyse risk scenarios
- Identify current state of controls
- Assess gaps between current and desired state of the IT risk environment
- Communicate IT risk assessment results to relevant stakeholders

The Objective

- Based on the results of the Risk Identification step, the IT Risk Assessment step calculates the level of risk that the organisation faces, to be used in the next step - Risk Response and Mitigation

Risk Identification vs. Risk Assessment

Risk Identification

- Recognition of threats, vulnerabilities, assets and controls
- Documenting risk

Risk Assessment

- Evaluates potential effect of risk
- Evaluates probabilities of an adverse event
- Documents critical business operations

Risk Assessment Techniques

- Bayesian Analysis
- Bow Tie Analysis
- Brainstorming/ Structured Interview
- Business Impact Analysis
- Cause and Consequence Analysis
- Cause-and-effect Analysis
- Checklists
- Delphi Method
- Event Tree Analysis
- Fault Tree Analysis
- Hazard Analysis and Critical Control Points

Risk Assessment Techniques (continued)

- Hazard and Operational Studies
- Human Reliability Analysis
- Layers of Protection Analysis
- Market Analysis
- Preliminary Hazard Analysis
- Reliability-centered Maintenance
- Root cause Analysis
- Scenario Analysis
- Sneak Circuit Analysis
- Structured “What if” Technique (SWIFT)

Analysing Risk Scenarios

- Risk scenarios used in Risk Identification are sometimes inaccurate due to:
  - Difficulty in calculating impact
    - Impact may be affected by:
      - Response time
      - Skill of staff
      - Maturity of response process
      - Effectiveness of controls
  - Organisational culture

Effect of Organisational Culture on Risk

- Mature Organisational processes
  - Presence of policies and procedures
  - Relationship between management and employees
  - Relationship between organisation and community
  - Effectiveness of monitoring
  - Proactive, preventative procedures

Blame Culture

- Is the first approach of management to hide events or seek to allocate blame?
  - Discourages openness and truthfulness about incidents
  - Prohibits honest feedback and continuous improvement
  - Poor communication between stakeholders
  - Loss of trust

Policies

- Policies are the foundation of the organisation.
- Declare managements' priorities and support
- Outline boundaries of behaviour and compliance
- Are interpreted through:
  - Standards, procedures, baselines, guidelines

Hierarchy of Policy

- High level policy
  - Non technical
  - Changes rarely
- Functional policies
  - Technical (remote access, wireless, BYOD, etc.,)
  - May change frequently
  - Interpret intent of high level policy

Impact of Architecture on Risk

- Single Points of Failure
- Missing controls – gaps
- Redundant controls
- Bottlenecks and resource constraints
- Conflicting controls

Controls

- The risk practitioner must assess the effectiveness of controls;
  - Misconfigured controls
  - Lack of monitoring
  - Wrong control
  - Ability to bypass a control
  - Lack of documentation

Types of Controls

- Managerial / Administrative
- Technical / Logical
- Physical / Operational

- Effective controls are a combination of all three types

Control Gap

- Compensating controls
  - Address a gap or weakness in the controls
  - May be caused by an inability to enact a more desirable control
    - i.e. additional monitoring, dual control

Evaluating Controls

- Audits
- Penetration Tests, vulnerability assessments
- Observation
- Incident reports
- User feedback
- Logs
- Vendor reports

Audit

- Audit may identify a risk due to missing, ineffective or improperly managed controls
- The risk practitioner may be required to assess the level of risk associated with the audit recommendation

Testing Controls

- Ensure that controls were installed/implemented as designed
- Ensure that the controls are working correctly
- Ensure that the controls are producing the desired result
  - Mitigating risk

Testing Controls

- Test both the technical and non-technical aspects of the control
  - Configuration
  - Documentation
  - Monitoring
  - Staff training
  - Architecture placement

Third Party Assurance

- SSAE 16 (formerly SAS 70)
  - SOC 1 - financial reviews
  - SOC 2 – non-financial reviews – detailed internal report
  - SOC 3 – like a SOC2 but used for external distribution
- ISAE 3402 – International standard

Vulnerability Assessments

- Examples of vulnerabilities
  - Insecure physical access
  - Application vulnerabilities
  - Unpatched systems
  - Exposed cabling
  - Unprotected sensitive data
  - Open ports or services

Current vs. Desired State of Risk

- Desired state is reflective of:
  - Management's risk appetite
  - International standards of good practice

Determining Risk

- Dependent on quality of data received for assessment
  - Complete
  - Accurate
  - Biased
  - Format
  - Relevant

Identifying Risk Trends

- Emerging risk
- Changes in risk
  - New threats
  - Newly discovered vulnerabilities
  - Bypass of controls
  - Erosion of control effectiveness
- Likelihood of risk levels exceeding KPIs

Gap Assessment

- Threat modeling
  - Discover the severity of the risk
- Root cause analysis
  - The true, underlying cause for the risk
- Gap Analysis
  - Delta between desired and current state

Measuring Risk Levels

- Key Performance Indicators (KPIs)
- Key Risk Indicators (KRIs)
- Key Goal Indicators (KGIs)
- Measuring risk and providing comparable reports to indicate trends, levels of compliance, etc.

Risk Assessment Methodologies

- Quantitative Risk
  - Monetary value of risk
- Qualitative Risk
  - Scenario-based
  - Range of risk levels
    - Very Low, Low, moderate, High, Very High

Quantitative Risk

- Cost of single risk event
- Frequency of risk events (usually calculated annually)
- Cost of risk averaged per year
- Justifies cost of controls

Qualitative Risk

- Non-monetary elements of risk
- Morale, reputation, customer confidence
- Risk levels by comparing likelihood with impact
- Semi-Quantitative Risk Assessment
  - Combination of Quantitative and Qualitative risk methods – associates money with range of risk levels

OCTAVE

- Operationally Critical Threat and Vulnerability Evaluation
- Explores risk relationship between IT and operation processes
- Evaluates:
  - Organisation
  - Technology
  - Strategy and plan development

Measuring Risk Management Capabilities

- Measure maturity of risk management function
  - Reflects managements' priorities
  - Proactive
  - Aligned with risk appetite
  - Policies, standards and procedures

Key Elements to Measure Risk Management

- Management support
- Communication
- Current BIA
- Logging and Monitoring
- Scheduled risk assessments
- Testing of BCP/DRP
- Staff training
- Involvement of risk in IT projects
- Feedback from users
- Time to detect incidents

Validate Risk Appetite

- As part of the Risk Assessment, the Risk Practitioner should validate the risk appetite of management to ensure that:
  - Management understands the significance of accepting risk
  - Documentation of risk acceptance level
  - Sign off by management
  - Alignment with laws and international standards

Risk Assessment and Incident Response

- The way an organisation handles incidents is a clear indicator of the maturity of their risk management program
  - Prepared
  - Prevention
  - Rapid Detection
  - Effective Response
  - Containment
  - Recovery/restoration
  - Feedback

Risks Related to IT Management

- Hardware
- Software
  - Operating Systems
  - Utilities, Drivers, APIs (application Program Interfaces)
  - Applications
- Database

Network Based Risk

- Network architecture
  - LAN, WAN, DMZ
  - Bus, Ring, Star, Tree, Mesh
- Network devices
  - Repeaters, switches, firewalls, routers, proxy, gateways
  - Domain name system (DNS)
  - Wireless

Virtual Private Networks (VPNs)

- Secure communications
  - Confidentiality
  - Integrity
  - Authentication
- Transport Layer Security (TLS/SSL)
- IPSEC

SDLC

- Software Development Lifecycle
  - Methodology for systems and software development
  - Project management
  - Security must be integrated into each phase:
    - Initiation, Development/Acquisition, Implementation, Operation and Maintenance, Disposal

Risk Assessment Report

- The final result of risk assessment is to prepare a risk assessment report for management
  - Documents risk and risk levels
  - Recommends risk response

Risk Ownership

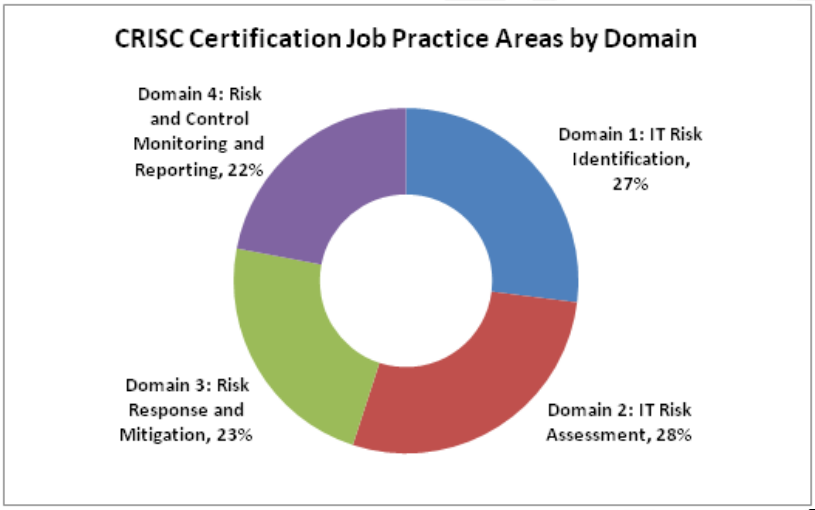
- Management owns the risk
- The Risk Practitioner must advise management of risk levels
- Update the risk register with the results of the risk assessment

Summary

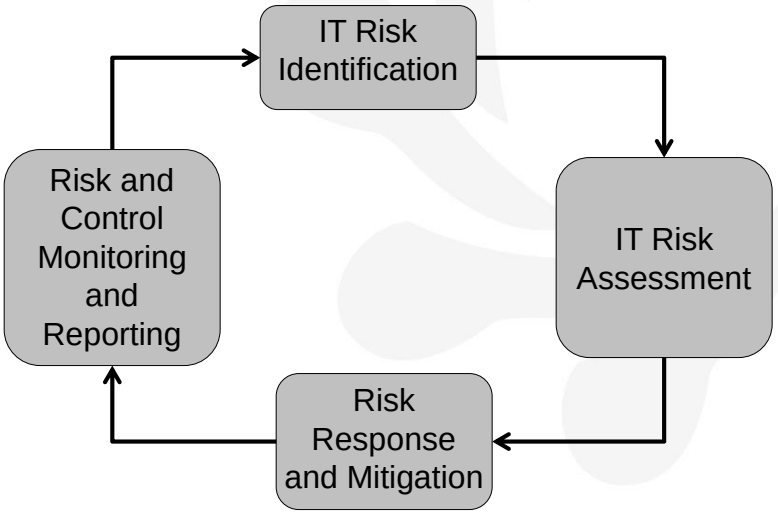
- The risk practitioner must assess and determine the severity of each risk facing the organisation
- All risk must be identified, assessed and reported to senior management

Risk Response and Mitigation

Job Practice Areas



Risk Management Lifecycle



Risk Response and Mitigation Objective

- Document risk response options and evaluate their efficiency and effectiveness to manage risk in alignment with business objectives

Learning Objectives

- List the different risk response options
- Define various parameters for risk response selection
- Explain how residual risk relates to inherent risk, risk appetite and risk tolerance
- Discuss the need for performing a cost-benefit analysis when determining a risk response
- Develop a risk action plan

Learning Objectives (continued)

- Explain the principles of risk ownership
- Leverage understanding of the systems development life cycle (SDLC) process to implement IS controls efficiently and effectively
- Understand the need for control maintenance

Overview

- The risk response process requires management to make the decisions regarding the correct way to respond to, and address risk
  - Based on the information provided in risk identification and risk assessment

Overview (continued)

- Management must be prepared to justify its risk response decision
- Provide a roadmap to implementing the required changes on a reasonable schedule
- Risk response must strike a balance between protecting business operations, but not unduly impeding operations

Alignment of Risk Response with Business

- Risk response is based on the risk documented and in the risk register and prioritized in the risk assessment report (RAR)
- Management considers the recommendations from the RAR
  - Determines best response
  - Develops action plan
  - Meet compliance requirements and business goals

Goal of Risk Response

- Ensure all risk is at an acceptable level according to risk appetite
  - If not acceptable, then mitigate (reduce) the risk
    - May require the implementation of multiple controls to reduce the risk sufficiently
      - Controls may be Technical, Managerial or Operational
  - Risk response is not a one time effort, it is a part of the risk management process cycle

Scheduling Control Implementation

- Based on:
  - Business impact
  - Cost
  - Dependencies
  - Other ongoing projects
  - Regulations
  - Operational workload

Risk Response Options

- Risk Acceptance
- Risk Mitigation (reduction)
- Risk Avoidance
- Risk Sharing/Transfer

Risk Acceptance

- To knowingly acknowledge and accept the risk – taking no action to reduce the risk
- Management decision
  - Risk acceptance level
  - Risk tolerance (used by some risk management practices as the allowable deviation from acceptance)
  - Residual risk – risk that remains after the implementation of controls

Risk Acceptance (continued)

- Management (risk owner) decision to absorb or assume the risk
  - Self-insurance
- Must be careful that data used in risk acceptance determination is accurate

Risk Mitigation

- The decision to mitigate or reduce the risk through the implementation of new controls or the improvement of existing controls
  - Managerial controls (policy/practices)
  - Technical controls (firewall)
  - Physical controls (locks, screen filters)
  - Compensating controls
- May require several controls before the risk is reduced to an acceptable level

Risk Avoidance

- The decision by management to cease the risk-laden activity
  - Close down an office in a hazardous region
  - Replace old equipment that is likely to fail
  - Stop production of an unsafe product
- Applies when the risk is too large to accept and there are no cost-effective controls available

Risk Sharing/Transfer

- The reduction of overall risk to the organization by diluting/sharing/transferring the risk to/with other parties.
  - Insurance
  - Joint ventures

Selecting a Risk Response - Analysis

- The selection of the appropriate response is based on several factors such as:
  - Priority of risk
  - Availability of recommended controls
  - Cost
    - Training
    - Implementation
    - Operational costs/maintenance/licensing
    - Impact on business operations/productivity

Selecting a Risk Response – Analysis (continued)

- The 'best' response may be based on:
  - Compatibility with other projects, equipment, business partners
  - Legal requirements
  - Time, resources and budget available

Cost-benefit Analysis

- Compare the cost of a control against the benefit (reduction in risk) that the control would provide
- Must consider the entire cost
  - Throughout the lifecycle
    - Acquisition, installation, maintenance, operation, licensing, training, operational impact, decommissioning

Cost-benefit Analysis (continued)

- Calculating benefit
  - Reduced insurance premiums
  - Reduced liability
  - Customer confidence/perception
  - Faster recovery
  - Reduced cost of risk event

Return on Investment (ROI)

- Time before a new product will pay for itself
  - Savings due to:
    - Increased efficiency
    - Lower operational costs
    - Reduced liability
    - Reduced likelihood or impact of an incident
- May also see ROSI used – return on security investment

Introduction of New Vulnerabilities

- A new control may introduce new vulnerabilities
  - A new lock may keep authorized people out
  - A new control may fail resulting in denial of service
  - A new control may present a new attack surface that could be exploited
  - An unreasonable control may frustrate users and cause them to bypass the control

Risk Action Plan

- Management should decide on an risk action plan – a strategy and timeframe to address risk
- Risk practitioner may play a consulting role is advising management
- Project management
- Schedule and budget for control implementation
- Oversight of project – ensure it delivers on time
- Ensure that the risk mitigation is effective

Business Process Review

- Document current business process
- Identify potential changes/areas of improvement
- Schedule and implement changes
- Feedback and evaluation

Control Design and Implementation

- The risk practitioner will provide advice on the selection, design, implementation, testing and operation of the controls
  - Countermeasures
  - Proactive
  - Reactive
  - Enhancement of existing controls
  - Compensating controls

Control Design and Implementation

- Select controls
  - Managerial
  - Technical
  - Physical
- Develop procedures to support technical controls
  - Determine ownership for the controls
  - Set up monitoring and reporting schedule
- A technical control requires managerial and operational controls to work effectively

Control Frameworks

- Selection of the “right” control – implemented in the “right” way
  - May be justified through compliance with a standard framework
  - PCI-DSS
  - NIST SP800-53
  - ISO/IEC 27001

Control Monitoring and Effectiveness

- Ensure that the risk response is achieving the desired result
  - Continuous monitoring
  - Security Information and Event Management Systems (SIEM)
- Examined in more detail in the next chapter

Inherent Risk

- Areas of the business that have a higher level of risk due to the nature of their operations.
  - A area with flammable liquids has a higher inherent risk of fire than other areas
- Areas with higher levels of inherent risk may require additional controls

Residual Risk

- The level of risk that remains following the implementation of a control(s)
- The goal is that Residual Risk must be less than or equal to Acceptable Risk
  - Having a residual of less than acceptable is OK, having a residual risk greater than acceptable risk would indicate a requirement for additional controls

Information Security

- Risk management controls should protect the;
  - Confidentiality
  - Integrity
  - Availability

Of Information and of Information Systems

Information Security

- Risk response ensures that technology is adequately protected, secure and reliable
- New technology undergoes a proactive risk assessment
  - Training, policies, procedures, BCP. etc.
- Legacy systems may not be securable due to cost or complexity
  - Implement compensating controls

Change Control

- The risk practitioner must be aware of the risk associated with changes to:
  - Hardware
  - Software
  - Network configuration
  - Projects, etc.,
- A change to any of these may affect the security and risk of the organization

Change Control

- Communication between business and IT
- Change control board for oversight
- Change requests are reviewed to ensure:
  - The change does not unknowingly affect risk or security
  - The change is formally requested, approved and documented
  - The change is scheduled at a time convenient for the business
  - All affected stakeholders are advised

Certification and Accreditation

- Often called 'Systems Authorization'
- The process of formal review and approval for any new information system or change to an existing system.
- Approval is granted by an independent third party – not by the system owner
- Part of Enterprise Risk Management
  - Intended to ensure that no system can be implemented that does not meet organizational standard and could therefore pose a risk to the rest of the organization

Certification and Accreditation (continued)

- Certification is the formal review of the system throughout all phases of development to ensure that adequate security is integrated into the system
- Accreditation is the formal approval by management for the implementation of the system for operation
  - The accreditor accepts the risk associated with system operations on behalf of the organization

Asset Inventory

- When technical controls are added, they need to be added to the CMDB (configuration management database) to ensure that they are:
  - Monitored
  - Tracked
  - Operated correctly

Configuration Management

- Ensure the correct configuration of equipment according to security baselines.
  - Hardening systems
  - Control over firewall rules and access permissions
  - Secure architecture

Third Party Management

- When services are provided by a third party the liability and responsibility for ensuring data protection remains with the organization that is doing the outsourcing
- Must ensure that security requirements are documented in contracts
  - Service Level Agreements (SLAs)
  - Reporting

Data Protection

- Protect data in all forms in all locations:
  - Paper
  - Electronic
  - In transit
  - In storage
  - When displayed
  - When discarded

Protect Data Integrity

- Size checks (buffer overflows)
- Format checks (mm/dd/yyyy)
- Range checks – allowable values
- Special character checks (disallow script or injection attacks)
- Canonicalization – different ways to represent the same values
- Protection from improper changes to data

Encryption

- Protect Data using encryption
  - Confidentiality
    - Symmetric encryption
  - Integrity
    - Hash functions
- Secure communications
  - Public Key Infrastructure (PKI)
  - Non-repudiation, access control, authentication

Risk Associated with Cryptography

- Key management
  - Key generation
  - Key length
  - Key storage
  - Key distribution
  - Key expiry

Digital Signatures

- Authenticate the sender of the message and authenticate that the message was not altered either accidentally (noise) or intentionally in transit
- Not the same as a digitized signature
- Created by encrypting a hash (digest) of a message with the private key (asymmetric) of the sender

Certificates

- A certificate validates that a public key belongs to the entity (person, organization, process, server, etc.,) identified on the certificate
- Issued by a Certificate Authority
- Risk is associated with:
  - Certification path
  - Trust in the certificate authority
  - Class of certificate

Risk Associated with Projects

- Project monitoring and reporting:
  - Scope creep
  - Lack of management support
  - Lack of skilled resources
  - Changing requirements
  - Unproven technology
  - Project cancellation

Risk Associated with the SDLC

- Incomplete or changing requirements
- Lack of standards
- Failure to follow selected methodology
- Failure to integrate security requirements into each phase of the project
- Lack of oversight/accountability

Risks Associated with BCP/DRP

- Unproven, untested plans
- Unrealistic timeframes
- Incorrect prioritization
- Lack of management commitment
- Outdated BIA
- Out-of-date plans

Risk Associated with IT Operations

- Failure to monitor systems
- Disabled logs
- Not reviewing logs
- Misconfiguration of equipment
- Lack of training
- Incompatible equipment
- Outdated systems – lack of vendor support
- Incomplete backups

Risk Associated with Backups

- Loss of data integrity
- Loss of encryption keys
- Incomplete backups
- Age and number of uses of backup media
- Ensuring all files are backed up
- Ensuring backups can be reloaded to meet Recovery Time Objectives and Recovery Point Objectives

Risk Associate with IT Architectures

- Ability to bypass controls
  - Backdoors
- Failure to separate sensitive data and applications
  - Flaws in code
- Misconfiguration of equipment

Risk Associated with Operating Systems and Applications

- Unpatched systems
- Lack of hardening
- Software Piracy
- Disclosure of sensitive data
- Incorrect access controls

Risks Associated with Networks

- Misconfiguration
- Open ports and services
- Failure to segregate systems
- Lack of training
- Lack of architecture/planning
- Undocumented networks
- Unknown equipment on a network
- Lack of encryption

Testing Applications

- Unit testing
- Code review
- Integration/System Testing
- Version control
- Regression testing
- Test data – disclosure of sensitive information
- Fuzzing

Risk Associated with Application Testing

- Using production data in testing
  - Disclosure of sensitive data
  - Corruption of production data
- Lack of Quality Assurance/Standards
- Lack of separation of development and production environments
- Lack of Rollback plans in case of implementation failure

Implementation Challenges

- Data migration
  - Loss of data integrity
  - Operational failure
- Parallel changeover
- Phased changeover
- Abrupt changeover

Risk of Emerging Technologies

- Unproven operations
- Undiscovered vulnerabilities
- New threat vectors
- Lack of skills and training
- Business interruption

Ownership of Risk and Controls

- Ownership of controls
- Ownership of risk response
- Ownership of risk response plans
- Ownership of reporting and compliance

Summary

- Be aware of risk
- Be aware of changes to risk
  - New threats
  - New vulnerabilities
  - Environmental changes
  - Changes in asset value
  - Changes in control effectiveness

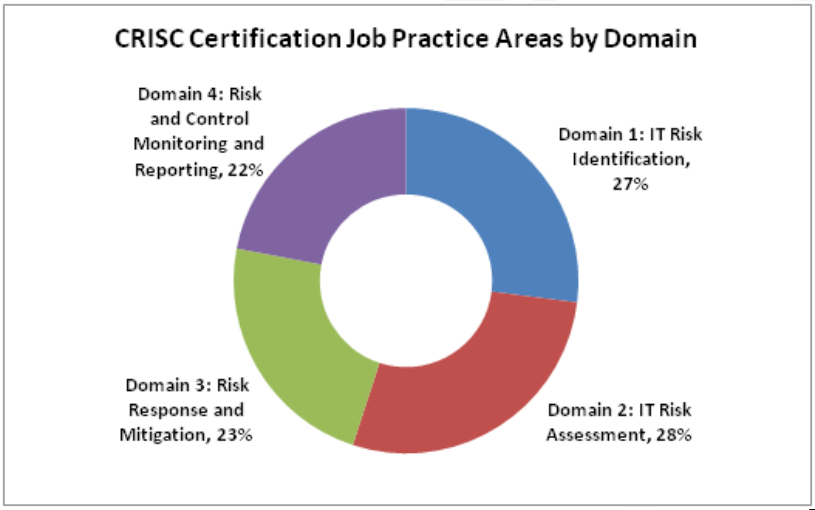
CRISC™

Certified in Risk and Information Systems Control™

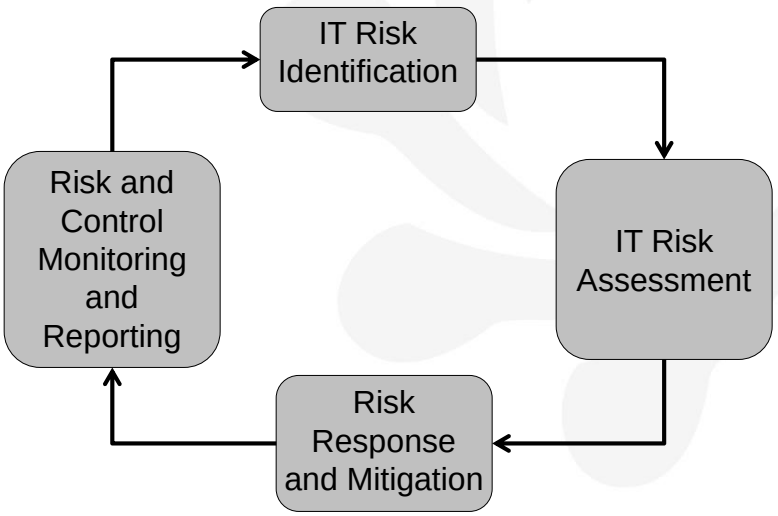
Firebrand Custom Designed Courseware

Risk and Control Monitoring and Reporting

Job Practice Areas



Risk Management Lifecycle



Risk and Control Monitoring and Reporting Objective

- Continuously monitor and report on IT risk and controls to relevant stakeholders to ensure the continued efficiency and effectiveness of the IT risk management strategy and its alignment to business objectives.

Key Topics

4.1 Define and establish key risk indicators (KRIs) and thresholds based on available data, to enable monitoring of changes in risk.

4.2 Monitor and analyse key risk indicators (KRIs) to identify changes or trends in the IT risk profile.

4.3 Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making.

4.4 Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance

Key Topics (continued)

4.5 Monitor and analyse key performance indicators (KPIs) to identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls.

4.6 Review the results of control assessments to determine the effectiveness of the control environment.

4.7 Report on the performance of, changes to, or trends in the overall risk profile and control environment to relevant stakeholders to enable decision making.

Learning Objectives

- Differentiate between key risk indicators (KRIs) and key performance indicators (KPIs)
- Describe data extraction, aggregation and analysis tools and techniques
- Compare different monitoring tools and techniques
- Describe various testing and assessment tools and techniques

The Objective

- A risk response is designed and implemented based on a risk assessment that was conducted at a single point in time;
- Risk changes; controls can become less effective, the operational environment may change, and new threats, technologies and vulnerabilities may emerge. Because of the changing nature of risk and associated controls, ongoing monitoring is an essential step of the risk management life cycle.

Measuring Effectiveness

- The effect of risk response and selected controls must be measureable
  - Management overview
  - Management support
  - Due care and due diligence
  - Compliance with regulations

Impacts of Changes on Risk

- Changes to the business, technology, projects can affect the risk profile
- Risk practitioner reviews proposed changes to determine the impact of the changes on risk
- Monitor trends
- Compare results with performance and risk objectives

Key Risk Indicators

- Measure the level of risk
- Compare to risk thresholds
- Alert to risk reaching or approaching an unacceptable level of risk
- Tracking mechanism

KRI Selection

- Select a meaningful set of controls to monitor
  - Consistent areas to measure
  - Good indicators of health of risk management program
  - Areas that can be influenced by management

SMART Metrics

- Specific – based on a clearly understood goal
- Measureable – Able to be measured
- Attainable – Realistic, based on important goals and values
- Relevant – Directly related to a specific activity or goal
- Timely – Grounded in a specific time frame

Sample of Possible KRIs

- Number of unauthorised devices discovered on a network
- Breaches of Service Level Agreements (SLAs)
- Time to deploy new patches
- Number of misconfigured systems

KRI Effectiveness

- Measure areas of higher risk
- Measure areas that are relatively easy to measure
- Reliability – a good predictor of risk level
- Sensitivity – accurately reflect changes in risk
- Repeatable – consistent measurement to detect trends and patterns

KRI Optimisation

1. Collect and report on the correct data
2. Set KRI thresholds correctly

Data must be reliable, monitored and reported to management in a timely manner – so that action can be taken expeditiously

Changing KRIs

- Changes in the risk appetite of management
- Changes in goals and the processes related to attaining goals
- Whether the activities are associated with reaching goals

Key Performance Indicators (KPIs)

- Determines how well a process is performing in enabling a goal to be reached
- Indicated likelihood of reaching a goal
- Threshold that indicates unacceptable results
- Sets benchmarks
- Quantitative measurement

Comparing KRIs and KPIs

- KPIs indicate the threshold of unacceptable results
- KRIs are a ‘tripwire’ that indicates a measure is in danger of exceeding a KPI.
  - A KRI is an early warning signal to allow action to be taken before a KPI is exceeded

Sample KPIs

- Network or system availability
- Customer satisfaction levels
- Number of complaints resolved on first contact
- Response to for data retrieval
- Number of employees that have attended annual awareness sessions

Data Collection Sources

- Audit reports
- Incident reports
- User feedback
- Observation
- Interviews
- Security reports
- Logs

Logs

- Capture and store data fro analysis
- Must be protected from alteration
  - May be needed for investigative processes
  - May contain sensitive data
- Retained for a suitable length of time
- Capture data in a timely way, close to the source of the incident to enable analysis

Log Analysis

- Identify violations
- Identify trends or developing attacks
- Identify the source of an attack

Require time synchronisation in order to facilitate and comparison between logs

Goals of Monitoring

- Create a culture of risk management
- Encourage continuous monitoring instead of periodic monitoring
- Provide feedback to improve risk response
- Verify that controls are working correctly and mitigating risk

Types of Monitoring

- Self-assessment
- Automated assessment
- Third party audits
  - Internal
  - External

Effectiveness of Assessments

- Depends on:
  - Having complete and accurate data
  - Skill of analyst
  - Management support and response
  - Continuous scheduled reviews not ad-hoc

IS Audits

- Provide an objective review of the efficiency of IT operations
  - Acquisition (the right product)
  - Implementation
  - Maintenance
  - Disposal
- Audit both technical and non-technical aspects of the operations of Information Systems

Vulnerability Assessments

- Discover any potential vulnerabilities that could be exploited by an attacker
- Report to management
  - False positives
  - False negatives
- Tries to find a vulnerability but does not try to exploit a vulnerability

Vulnerability Assessments and Penetration Tests

- May be conducted by internal or external teams
- Try to simulate the methods used by attackers
- May be both technical and non-technical
  - Physical security
  - Social engineering

Penetration Tests

- Try to exploit a perceived vulnerability
- Often based on the results of a vulnerability assessment
- May test:
  - Applications
  - Networks
  - Physical
  - People
  - Incident management processes

Results of Penetration Tests

- Report provided to management
  - Identify test procedures
  - Identify any areas of concern
  - Provide recommendations for improvement
  - Prioritise risk according to severity

Third Party Assurance

- Provide assurance to clients and partners of:
  - Compliance with best practice
  - Standards
  - Maturity of risk management program
  - Information Security
- SSAE 16
- ISAE 3402

Maturity of Risk Management Process

- Continuous improvement
- Optimisation
- Quantitatively managed
- Defined reliable processes
- Proactive management of risk

Monitoring Change

- The risk practitioner must always be alert to changes that could affect the risk profile of the organisation and the ability of the organisation to reach its goals
- Annual review of monitoring an reporting program

Summary

- Proper and effective management of risk is essential to protecting the assets of the organisation.
- Risk management is a never-ending process.
- IT risk and controls should be monitored continuously to ensure that they are adequate and effective