CISM Study Guide

Christian Reina, CISSP, CISA, CRISC

2010

An investment in knowledge pays the best interest.

Benjamin Franklin

Table of Contents

Information Security Governance

Overview

Significant benefits:

- Policy compliance
- Lowering risks
- Optimize resources
- Assurance on critical decisions
- Efficient and effective risk management
- Trust and reputation

Outcomes:

1. Strategic Alignment
    a. Security requirements driven by organizational objectives
    b. Security solutions fit for organizational processes
    c. Investments aligned with the organizational strategy
2. Risk Management
    a. Collective understanding
    b. Risks mitigation
3. Value delivery
    a. Standard set of security practices
    b. Prioritizing security objectives based on risk analysis
4. Resource management
    a. Knowledge is captured and available
    b. Efficient security architecture
5. Performance measurement
    a. Metrics
    b. External assessments and audits
6. Integration
    a. Relationships with assurance functions
    b. Roles and responsibilities between assurance functions should not overlap

Effective Governance

Business goals and objectives

- Security strategy linked with business objectives
- Policies address each aspect of strategy, controls, and regulation
- Standards for each policy
- Sufficient authority
- Metrics and monitoring

Roles and Responsibilities

Board of directors/senior management

- Validating and ratifying the key assets they want protected and the protection levels
- Penalties for non compliance must be communicated and enforced

Executive management

- Implement effective security governance
- Align information security activities in support of business objectives

Steering Committee

- Consensus on priorities and tradeoffs
- Ensuring the alignment of the security program with business objectives

CISO

- CISO, CSO, C-Level responsibility, authority, and required resources to improve the security posture

Governance, Risk and Compliance

Governance: senior executive management responsibility

Risk management: Risk tolerance, risk identification and impact, risk mitigation

Compliance: Records and monitors the policies, procedures, and controls needed to ensure that plicies and standards are adhered to.

Business Model for Information Security

1. Elements
    a. Organization design and strategy
    b. People
        i. Recruitment strategies
        ii. Employment issues
        iii. Termination
    c. Process
    d. Technology
2. Dynamic Interconnections
    a. Governance: Sets limits within which an enterprise operates and is implemented within processes to monitor performance
    b. Culture
    c. Enablement and support: Connects the technology element and the process element
    d. Emergence: Introduce feedback loops, alignment with process improvement,
    e. Human factors

f. Architecture

Information security manager

Obtaining senior management commitment

- Aligning security objectives with business objectives
- Identifying potential consequences
- Budget
- ROI
- Monitoring and auditing

Governance metrics

Effective security metrics

- Strong upper level management support
- Security policies and procedures
- Quantifiable performance metrics
- Periodic analysis of metrics data

Strategic alignment

From a business perspective, adequate and sufficient practices proportionate to the requirements are likely to be more cost effective than best practices.

Risk management

Reduce adverse impacts on the organization to an acceptable level

Value delivery

- Cost of security being proportional to the value of assets
- Well designed controls

Resource management

- Infrequent problem rediscovery
- Effective knowledge capture and dissemination

Performance measurement

- Time it takes to detect and report incidents
- Benchmarking comparable organizations
- Methods of tracking evolving risks

Assurance integration

- No gaps in information asset protection
- No security overlaps
- Well defined roles and responsibilities

Common pitfalls in developing a security strategy

- Overconfidence
- Optimism
- Anchoring
- Status quo bias
- Mental accounting
- Herding instinct
- False consensus

Strategic Objectives

The goal

1. Information is located and identified
2. Asset valuation
3. Level of sensitivity

Business case development

- Process
    - Introduce project considering value, risk, and relative priority
    - Value to the organization
    - Allow management to determine the value to the business relative to other alternatives
    - Enable management to objectively measure the benefits
- Business case format
    - Reference
    - Context
    - Value proposition: Important
    - Focus
    - Deliverables: important
    - Dependencies : critical success factors (CSF)
    - Project metrics: KGI, KPI
    - Workload
    - Resources
    - Commitments (Required)
- Objectives
    - Adaptable
    - Consistent
    - Business oriented
    - Comprehensive
    - Understandable
    - Measurable
    - Transparent
    - Accountable

The desired state

Complete snapshot of all relevant conditions at a particular point in the future.

Approaches to get there:

COBIT:

- Plan and organize
- Acquire and implement
- Deliver and support
- Monitor and evaluate

CMM

- Nonexistent
- Ad hoc
- Defined process
- Managed
- Optimized

Balanced scorecard

- Learning and growth
- Business process
- Customer
- Financial

ISO 27001/27002

- Security policy
- Organizing information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations
- Access controls
- Infosec development and maintenance
- Infosec incident management
- BCP
- Compliance

Risk objectives

- Developing the right strategy objectives usually needs to be an iterative approach

- Process risks pose the greatest hazard and technical controls are unlikely to adequately compensate for poor management or faulty processes.

Information security strategy

The goal of security is business process assurance

Road map

- Consider the initial stages of developing a security architecture
- Break down complex projects into a series of shorter-term projects
- Shorter projects can serve as checkpoints and opportunities

Resources

- Policies, standards, procedures, and guidelines
- Architecture
- Controls
- Countermeasures
- Layered defenses
- Technologies
- Personnel security
- Organizational structure
- Roles and responsibilities
- Skills
- Training
- Awareness and education
- Audits
- Compliance enforcement
- Threat analysis
- Risk assessment
- BIA
- Resource dependency analysis
- Outsourced security providers
- Environmental security

Constraints

- Legal
- Physical
- Ethics
- Culture
- Costs
- Personnel
- Organizational structure
- Resources

- Capabilities
- Time
- Risk tolerance

Action Plan

- Gap analysis
    - Annually
    - Work backward from endpoint to the current state
    - Link business objectives with strategy
    - Appropriate authority
    - Appropriate security approvals
- Policy development
- Standards development
- Training and awareness
- Metrics
    - KGI:
        - Completing independent controls testing validation and attestation
        - Preparation of required statement of control effectiveness
    - CSF
        - Identification, categorization, and definition of controls
        - Defining appropriate test to determine effectiveness
    - KPI
        - Control effectiveness testing plans
        - Results of testing control effectiveness

Information Risk Management

Overview

The foundation for effective risk management is a comprehensive risk assessment. Although a computational approach may be used to arrive at various risk aspects, the approach is nevertheless qualitative and subjective to some extent.

Effectiveness is influenced by:

- Culture
- Mission and objectives
- Structure
- Products and services
- Processes
- Practices

- Regulatory conditions

Outcomes:

- Understanding of the organization's threat, vulnerability and risk profile
- Understanding risk exposure and potential consequences
- Awareness of risk management priorities
- Organizational risk mitigation strategy
- Organizational acceptance based on potential residual risk
- Cost effectiveness

Effective information risk management

Development

- Context and purpose: Defining the organization, process, project, scope, and establishing goals and objectives. Risk tolerance and appetite.
- Scope and charter
- Objectives: Based of risk analysis
- Methodologies
- Implementation team

Roles and Responsibilities

- Governing boards and senior management: Ultimate responsibility for mission accomplishment. Ensure adequate resources. Sign off acceptable risk levels.
- CIO: IT planning, budgeting, and performance.
- Information Security Manager: responsible for security program
- System and information owners: Ensuring proper controls are in place to address CIA.
- Business managers: Responsible for business operations

Implementing Risk Management

Process:

1. Establish scope and boundaries
2. Risk assessment
3. Risk treatment
4. Acceptance of residual risk
5. Risk communication and monitoring

Framework

Scope and framework are independent from the particular structure of the management process, methods, and tools to be used for implementation.

External and Internal environment

- External: Political, financial, local market, law, regulation, social and cultural.

- Internal: Key business drivers, Organization's SWOT, internal stakeholders, structure, culture, assets, goals and objectives

Risk management scope

- Must provide a balance between costs and benefits
- Duration
- Full scope of activities
- Roles and responsibilities
- Activities to be assessed

Risk Assessment

- Asset valuation
- Vulnerabilities
- Threat analysis
- Risk mitigation

NIST approach

1. System characterization
2. Threat identification
3. Vulnerability identification
4. Control analysis
5. Likelihood determination
6. Impact analysis
7. Risk determination
8. Control recommendations
9. Results documentation

Aggregated and cascading risk

- Aggregated: Minor vulnerabilities combined can have a significant impact.
- Cascading: Chain reaction as a result of one failure contribute to unacceptable impact.

Other

Factor Analysis of Information Risk (FAIR): Taxonomy, a method for measuring, a computational engine, simulation model

Probabilistic Risk Assessment (PRA): Systematic and comprehensive methodology to evaluate risk associated with a complex engineered technological entity. (Nuclear regulatory commission)

Identification of risks

- Brainstorming
- Flow charting
- What if

Threats
Natural, unintentional, intentional physical/nonphysical

Vulnerabilities
Poor network design, lack of redundancy, poor management communications, insufficient staff, lack of skills, defective software

Risks
Every organization has a level of risk to accept.

Risk Analysis
- Examination of risk sources
- Consequences
- Likelihood
- Assessment of existing controls: Quantitative, Qualitative, Semiquantitative

Evaluation of risks
Risk evaluation may lead to a decision to undertake further analysis.

Risk treatment
- Terminate
- Transfer
- Mitigate
- Accept

Impact
The bottom line for risk management. A direct financial loss can include:

- Reputation
- Money
- Legal liability
- Business interruption
- Breach
- Noncompliance

Controls
- Deterrent controls reduce probability of threats
- Preventative controls reduce vulnerabilities
- Corrective controls reduce impact
- Compensatory controls compensate increased risk
- Detective controls discover attacks

Information Resource valuation
Valuation must be based on the total range of potential losses and impacts

Information Asset Classification

- Determine sensitivity and criticality
- Business dependency analysis can be used to provide a basis for protective activities if there are resource constraints or other reasons
- Locate and identify followed by appropriate level of sensitivity and criticality

Impact assessment and analysis

System mission, system/data criticality (system's value), system/personnel/data criticality (impact if disclosed) is required to conduct the analysis.

Integration with Life Cycle Processes

Risk management is paramount during SDLC phases for IT system development and during project management life cycles.

Risk monitoring and communication

- Monitoring: Key risk indicators (KRI) can be defined as measure that indicate when an enterprise is subject to risk that exceeds a defined risk level.
- Reporting: Reporting significant changes in risk is a primary responsibility of the information security manager.

Information Security Program Development

Overview

- Well developed information security strategy
- Cooperation and support from management and stakeholders

Outcomes

1. Strategic Alignment: change management practices that ensure business requirements drive security initiatives
2. Risk management: ongoing or continuous process of risk management
3. Value delivery: effective/efficient
4. Resource management: project planning, technology selection and skill acquisition
5. Assurance integration
6. Performance Measurement: progress and monitoring

Information Security Manager Responsibilities

1. Strategy: monitors and makes recommendations
2. Policy: writes and publishes

3. Awareness
4. Implementation: Contributes secure architecture, design, and engineering strategy.
5. Monitoring
6. Compliance

Scope and Charter development

- Integrated with corporate objectives
- Clearly defined
- End users are increasingly accountable
- Information security reporting
- Active monitoring
- Incidents are promptly addressed
- Threats and vulnerabilities analyzed
- Intrusion testing
- Continuous improvement

Challenges:

- Cost overruns
- New monitoring and metrics requirements
- New policies or standards

Pitfalls:

- Resistance
- Failure of strategy
- Increase security results in less job functionality
- Ineffective project management

Development Objectives

Defining objectives

- Develop the processes and projects that close the gap between the current state and those objectives.
- Develop KGI

Residual risks

A business case must address the fact that regardless of the level of control, residual risk will always remain and it must address the fact that it may aggregate into levels that are unacceptable

The Desired State

A state where defined objectives have corresponding KGIs, which in turn have corresponding control objectives. These control objectives should be supported by a control activity which is managed and measurable.

Defining a program development road map

Review Security Level:

- Objective
- Scope
- Constraint
- Approach
- Result

Program Resources

- Documentation: Policies, standards, procedures
- Security Architecture: Conceptual layer integrates with business requirements.
- Controls
    - Logical access: MAC, DAC
    - Secure failure: affects availability
    - Principle of least privilege
    - Compartmentalize to minimize damage
    - Segregation of duties
    - Transparency
    - Trust
    - Trust no one
- Countermeasures
- Technologies
    - ACLS
    - Choke routers
    - Content filtering
    - DBMS
    - Encryption
    - Hashing
    - PKI
    - Route filtering
    - Traffic/packet filtering
- Skill, roles and responsibilities
- Awareness
- Formal audits
- Compliance enforcement
- Project risk analysis: Possible threats include the following
    - Unclear objectives
    - Carelessness
    - Mistakes

    - Deficient strategy
    - Poor planning
    - Inadequate resources
    - Incorrect specifications
    - Faulty execution
    - Sabotage
- Vulnerability analysis
- BIA
- Resource dependency analysis

Implementing an Information security program

- Objectives have been defined
- Resources are available
- Control objectives have been defined
- Security reviews and audits are available
- Management support
- Integration into life cycle processes

PDCA Methodology

1. Plan: Design, plan, initiate. Create strategy, policies, goals, objectives
2. Do: Execute and control including integration into organizational practices
3. Check: semiannual audits
4. Act: Continuous improvement

Information Infrastructure and Architecture

Objectives

- Defined
- Precise
- Tested
- Monitored
- Measured

Business View: Business risk model	Contextual
Architect's View: Control objectives	Conceptual
Designer's View: Security Policies	Logical
Builder's View: security rules, procedures	Physical
Tradesman's View: Security standards	Component
Facilities Manager's View: Operational risk management	Operational

Development Metrics

- Security is certainly comprised of technical controls, processes, and people issues, called security program
- Measurement is a fundamental requirement for security program success

Levels

- Strategic: security program on track, on target, and on budget
- Management/tactical: policy standards compliance, incident management effectiveness
- Operational: Technical metrics

Attributes

- Manageable
- Meaningful
- Actionable
- Unambiguous
- Reliable
- Timely
- Predictable

Goals

1. Strategic Alignment:
    a. Portfolio of projects
    b. Committee charters include data protection
    c. Regulatory audit
2. Risk management
    a. Design risk
    b. Project risk
    c. Program development
    d. Risk management at the steering committee
3. Value delivery
    a. Expected value
    b. Cost of work performed
    c. Cost variance
    d. Cost of internal services
4. Resource management
    a. Deficiencies detected and corrected
    b. Resource utilization
    c. Functions have a backup
5. Assurance integration
    a. Assurance providers participating in development, planning, oversight
6. Performance metrics: Metrics on metrics

Information Security Program Management

Overview

- Ongoing, largely administrative function
- Involves addressing incidents, conducting investigations, protect management, consulting, educating, budgeting, recruiting, business case development.

Outcomes

1. Strategic alignment:
    a. Enumeration of risks, selection of controls, agreement on risk tolerance
    b. Consideration of security solutions taking into account enterprise processes as well as culture, cost, governance, and existing technology.
2. Risk management:
    a. Develop a comprehensive understanding of threats the organization faces.
3. Value delivery:
    a. Security solutions be institutionalized as normal and expected practices
4. Resource management
    a. Knowledge is captured and made available to those who need it
5. Performance measurement
    a. Good metrics design and implementation
6. Business process assurance

Roles and responsibilities

Information security manager

- Alignment to business objectives
- Consistent strategy
- Corporate culture values security
- Interaction with business process owners
- Established metrics
- Risk management
    - Methods for assessing
    - Ability to analyze
    - Knowledge of risk analysis
    - Impact analysis
    - Methods of tracking
- Technology competencies
- Administrative
    - Project management
    - Service delivery
    - Budgeting

- SDLC

Board of directors

- Direction, oversight, and requirements for appropriate metrics

Executive management

- Sets tone for information security

Steering committee

- Communications channel and provides ongoing basis for the alignment of the security program with business objectives
- Information security manager should clearly define the roles, responsibilities, and scope of the information security steering committee

IT

- Configuring security within the actual technical environment

Business unit managers

- Ensuring business operations meet security requirements
- Identify and escalate security incidents

Management Framework

Conceptual representation of an information security management structure

Technical

1. Native controls
2. Supplemental controls
3. Management controls

Control Analysis

- Placement
- Effectiveness
- Efficiency
- Policy
- Implementation

Operational

- Ongoing management activities
  - Procedures
  - Security practices
  - Maintenance
  - IAM
  - Change control
  - Security metrics collection

    - Incident response, investigation, and resolution

Management

- Strategic
    - Policy review
    - Standards implementation
    - Threat, risk, analysis

Administrative

- Financial: TCO, ROI
- HR: job description, organizational planning, recruitment, hiring, payroll, termination

Educational

- Employee quiz scores
- Avg time since last employee training

Assurance integration

- Assurance functions provide input, requirements, and feedback

Measuring Performance

- Objectives
    - Minimize risk
    - Support business
    - Support compliance
    - Maximize productivity
    - Maximize cost effectiveness
    - Security awareness
    - Measure and manage performance

Risk and Loss

- Technical vulnerability management
- Risk management
- Loss prevention

Support of business objectives

- Completed objectives that support the business

Compliance

- Internal and external audits

Operational productivity

- Logs analyzed
- Personnel cost savings

Cost effectiveness

- Accurate cost forecasting
- Total cost of keeping up security program

Organizational awareness

- Tracking awareness success
- Employee testing

Technical security architecture

- Intrusions detected
- Blocked attacks

Effectiveness of management framework and resources

- Frequency issue occurrence
- Infosec requirements in every project plan

Operational performance

- Time between vulnerability detection and resolution
- Time to detect, escalate, isolate, and contain incidents

Management challenges

- Inadequate management support
- Inadequate funding
- Inadequate staffing

Determine the State of Information Security

- Evaluate program objectives
    - Goals alignment
    - Objectives alignment
    - Collaboration
- Evaluate compliance requirement
    - Compliance in policies
    - Recent audit results
- Evaluate program management
    - Documentation
    - Roles and responsibilities
    - Approved polices
    - Program accountability
- Evaluate security operations
    - Standard Operating Procedures (SOP)
    - Separation of duties
    - Effective operational metrics
- Evaluate technical security management

    - Technical security standards
    - Technical standards uniformly implemented
- Evaluate resource levels
    - Financial: budget
    - HR: skilled people
    - Technical: capacity of supporting technologies

Information Security Management Resources

- Policies, standards, and procedures
- Controls
- Countermeasures
- Technologies
- Skills
- Awareness and education
- Audits
- Compliance enforcement
- Threat analysis: at least annually by evaluating changes in the technical and operating environments of the organization, particularly where external entities are granted access to organizational resources.
- Vulnerability analysis
- Incremental risk assessments
- Resource dependency analysis

Implementing Management

- Review Policies and Standards
- Security metrics and monitoring
    - Must be implemented to determine the ongoing effectiveness
    - Monitoring with risk assessments
    - Determine success of information security investments
- Control testing and modification: Under change control management
- Monitoring and communication: SIEM
- Documentation
- Assurance integration
    - Steering committees
    - Policies and standards
- Acceptable use policies
- Change management
- Vulnerability assessments
    - There must be a threat to exploit a vulnerability that must cause an impact.
- Due dillegence
    - Senior management support

    - Appropriate security education, training, awareness
    - Comprehensive policies
    - Risk assessments
    - Backup recovery
    - Compliance efforts
- SDLC
    - Establishing requirements
    - Feasibility
    - Architecture and design
    - Proof of concept
    - Full development
    - Integration testing
    - Quality and acceptance testing
    - Deployment
    - Maintenance
    - System end of life

Outsourcing

- Contracts
    - Right to audit
    - Notification procedures
    - Investigation process
    - SLA
    - Indemnity clauses to mitigate impacts caused by the service provider
    - Data protection
    - Privacy laws

Incident Management and Response

Overview

Incident management and response is part of business continuity. It may be less costly to maintain an effective incident management capability than to try to prevent most incidents. It is critical to achieve stakeholder consensus and senior management support.

Response activities:

1. Detect incidents quickly
2. Diagnose incidents accurately

3. Manage them properly
4. Contain and minimize damage
5. Restore affected services
6. Determine root causes
7. Implement improvements to prevent reoccurrence

Incident management and response

Incident Management Planning (IRP) focuses on security breaches. Defining requirements and expectations is primarily the responsibility of business owners. BCP, DR, and IRP must be consistent but not necessarily integrated.

Decisions to be made:

- Detection
- Severity level: triggers response
- Assessment and triage: Effectively manage limited resources during incident
- Declaration criteria
- Scope of incident management
- Response capabilities

Incident handling process

Detection and reporting

Receive and review event information

Triage

Categorize, prioritize, and assign events and incidents

Analysis

Determine what happened

Incident response

Actions taken to resolve or mitigate and incident

Information security manager responsibilities

- Developing plan
- Handling and coordinating
- Validating, verifying, and reporting

Metrics and Indicators

Strategic alignment

- Constituency: who are the stakeholders
- Mission
- Services: manage stakeholders expectations

- Organizational structure: Provide business with the maximum availability of IMT services on the most cost-effective basis.
- Resources: staffing
- Funding
- Management buy-in

Risk management
Any risk that materializes becomes an incident

Assurance process integration
Involvement from other business units

Value delivery
- Integrate with business processes
- Provide assurance to stakeholders
- Integrate with BCP
- Part of overall strategy

Resource management
Optimal effectiveness

Performance Measurement
Successful handling of incidents

Plan of action
1. Prepare/improve/sustain (Prepare)
2. Protect infrastructure (Protect)
3. Detect events (Detect)
4. Triage events (Triage)
    a. Tactical: based on set criteria
    b. Strategic: based on the impact of business
5. Respond
    a. Technical
    b. Management
    c. Legal

Challenges
- Lack of business buy in
- Mismatch to organizational goals and structure
- IMT member turnover
- Lack of communication process
- Complex and wide plan

Resources

- Policies and standards
- Technologies
- Personnel
    - Central IRT
    - Distributed IRT: geographically dispersed
    - Coordinating IRT
    - Outsourced IRT
- Roles and responsibilities
- Personal Skills
    - Communication
    - Presentation skills
    - Ability to follow policies and procedures
    - Team skills
    - Integrity
    - Self understanding
    - Coping with stress
    - Problem solving
    - Time management
- Technical skills: foundation and handling skills
- Awareness and education
- Audits
- BIA

BIA

Vulnerability analysis is often part of the BIA process. The first step in the incident response management process is to consider the potential impact of each type of incident that may occur. A BIA must establish the escalation of loss over time, identify the minimum resources needed for recovery, and prioritize the recovery of processes and supporting systems.

Goals

1. Criticality prioritization
2. Downtime estimation
3. Resource requirement

Activities

- Gathering assessment material
- Vulnerability assessment
- Analyzing information
- Documenting results

Current state of incident response capability

What's already in place.

- History of incidents
- Threats: environmental, technical, man-made
- Vulnerabilities
- Risks
- Risk tolerance
- Business & incident response integration
- RPO/RTO/SDO/MTO (Maximum tolerable outage) integration

Developing an incident response plan

Elements

1. Preparation
2. Identification: chain of custody, ownership of an incident, determining severity
3. Containment: activating the incident management, notifying, controlling
4. Eradication: locating recent backups, improving defenses
5. Recovery: restoring, validating actions taken
6. Lessons learned

Gap analysis

Processes that need to be improved and resources needed to achieve the objectives

Response and recovery plans

Threat mitigation

- Eliminate or neutralize a threat
- Minimize the likelihood of a threat's occurrence (The best option)
- Minimize the effects of a threat if an incident occurs

Recovery sites

- Hot sites
- Warm sites
- Cold sites
- Mobile sites
- Duplicate information processing facilities
- Mirror sites

Basis for recovery

- Interruption window: total time the organization can wait from the point of failure to the restoration of critical services/applications
- RTO: Recovery Time Objective

- RPO: Recovery Point Objective
- SDO: Service Delivery Objective. Level of service to be supported
- MTO: Maximum Tolerable Outage. Maximum time the organization can support processing in alternate mode.

Incident management teams

- Emergency action team: fire wardens
- Damage assessment team
- Emergency management team: Coordinating the activities of all other recovery teams and handling key decision making
- Relocation team
- Security team

Continuity of network services

- Redundancy
- Alternate routing: Using alternate medium such as fiber optics
- Diverse routing: duplicate cable facilities
- Long haul network diversity
- Last mile circuit protection
- Voice recovery

Insurance

- IT equipment and facilities
- Media reconstruction
- Extra expense
- Business interruption
- Valuable papers
- Error and omissions
- Fidelity coverage: Loss from dishonest or fraudulent acts by employees
- Media transportation

Testing

- Identifying gaps
- Verifying assumptions
- Testing time lines
- Effectiveness of strategies
- Performance of personnel
- Accuracy and currency of plan information

Types of tests

- Checklist review
- Structured walkthrough

- Simulation test: role play
- Parallel test
- Full implementation test

Other tests

- Table-top walk-through of plans
- Table-top walk-through with mock disaster scenarios
- Testing infrastructure
- Full restoration and recovery with some personnel unfamiliar with systems
- Surprise test

Test Results

- Verify completeness
- Evaluate personnel performance
- Level of training and awareness
- Evaluate coordination
- Retrieval capability

Executing Response and Recovery Plans

It is virtually guaranteed that untested plans will not work.

Ensuring Execution as required

- Facilitator or director to direct the tasks within the plans
- Independent observer to record progress and document any exceptions
- Change management is paramount
- Maintenance activities
    - Periodic review
    - Calling for revisions
    - Coordinating scheduled and unscheduled tests to evaluate adequacy
    - Participating in scheduled plan test
    - Training personnel
    - Maintaining records

Forensic Evidence

- Requirements
    - Disconnect the power to maximize the preservation of evidence on the hard disk is not universally accepted as the best solution, and the information security manager will need to establish the most appropriate approach.
    - Trained personnel must use forensic tools to create a bit by bit copy of any evidence on hard drives
    - Original media must remain unchanged
- Legal aspects

- Chain of custody
- Checklists for acquiring technicians
- Detailed activity log
- Signed non-disclosure/confidentiality forms for all technicians involved in recovering evidence