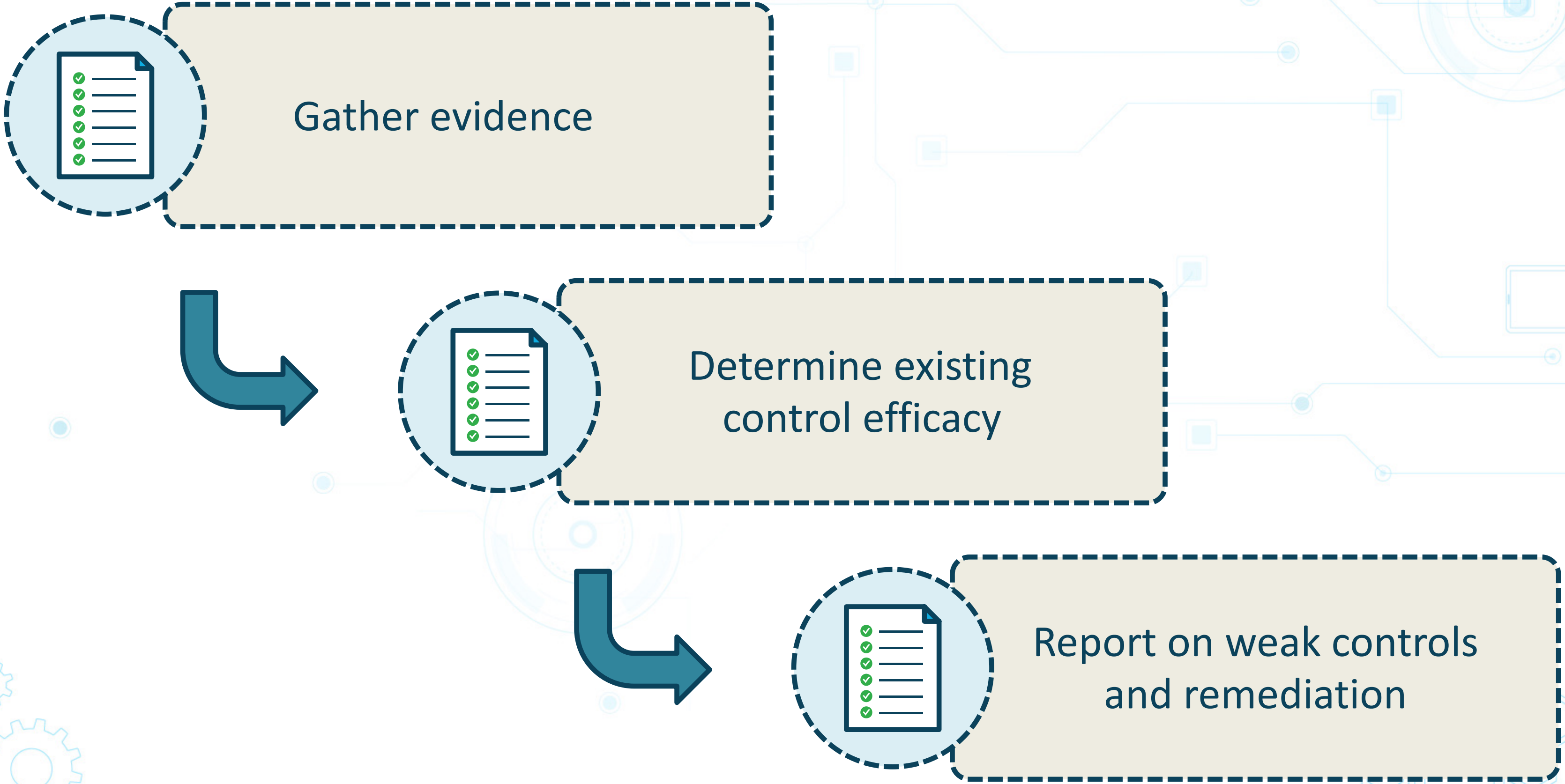
Information System Auditing

Investigate

Inform

The IS Auditing Process



Gather evidence

Determine existing control efficacy

Report on weak controls and remediation

IS Audit Planning

- Audit subject: location, business process
- Audit objective: payment processing and sensitive document retention
- Audit scope: what will be included in the audit?
- Audit pre-planning: risk assessment, compliance, and timeframe
- Audit procedure to be followed: create an audit program

Audit Procedures

Activity	Example
Obtain documentation	Security policies, departmental policies, process procedures, and workflows

Audit Procedures

Activity	Example
Obtain documentation	Security policies, departmental policies, process procedures, and workflows
Regulatory compliance	Retention of specific documents, logs, and transactions for a specific period of time

Audit Procedures

Activity	Example
Obtain documentation	Security policies, departmental policies, process procedures, and workflows
Regulatory compliance	Retention of specific documents, logs, and transactions for a specific period of time
Audit tools	Web application fuzzer, host vulnerability scanner

ISACA Code of Conduct

- Information Systems Audit and Control Association (ISACA)
- International association with a goal of proper IT governance
- Certified Information System Auditor (CISA)
  - Assurance that business processes and supporting IT solutions are secure

ISACA Code of Conduct

Support the implementation of, and encourage compliance with, appropriate standards, procedures, and controls for information systems.

Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.

ISACA Code of Conduct

Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.

Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.

ISACA Code of Conduct

Maintain competency in their respective fields and agree to undertake only those activities, which they can reasonably expect to complete with professional competence.

Inform appropriate parties of the results of work performed; revealing all significant facts known to them.

ISACA Code of Conduct

Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

ISACA Auditing Standards

- Information Technology Assurance Framework (ITAF)
- Risk-based approach
- Adherence to the ISA Code of Conduct
- Guidelines for IS auditing
- Audit efficiency
- Audit report effectiveness

ISACA Auditing Standards

Standard	Summary
1001 Audit Charter	Audit purpose, scope, and access to resources
1002, 1003 Organisational and Professional Independence	Objectivity and no interference in all audit phases
1004 Reasonable Expectation	Audit execution as per IS audit assurance standards in a timely fashion
1005 Due Professional Care	Audit activity execution with integrity, care, and communication

ISACA Auditing Standards

Standard	Summary
1006 Proficiency	Skills competency, continuing education, and subcontracting
1007 Assertions	Verify internal and third party control assertion validity
1008 Criteria	Criteria against which controls are compared
1201 Engagement Planning	Audit objective, scope, and timeline

ISACA Auditing Standards

Standard	Summary
1202 Risk Assessment in Planning	Risk-based approach used for the audit plan
1203 Performance and Supervision	Ensure audit objective completion in accordance with laws, regulations, and audit milestone schedules
1204 Materiality	Weak or absent controls result in a failure to meet control objectives
1205 Evidence	Audit conclusions are objective and based solely on evidence

ISACA Auditing Standards

Standard	Summary
1206 Using the Work of Other Experts	Verify professional qualifications and determine if conclusions are in a separate audit report
1207 Irregularity and Illegal Acts	Assume that some form of fraud might be encountered
1401 Reporting	Communicate audit findings, conclusions, and recommendations only to authorized parties
1402 Follow-up Activities	Revisit recommendations to ensure timely action

Organizational Documentation

- Audit information gathering
- Ensure documents fall within audit scope
- Ensure documents are up-to-date

Organizational Documentation

Organizational chart

- Employee hierarchy
- Job role relationships
- Overlapping roles
- Conflict of interest

Business processes

- How processes achieve organizational objectives
- Process efficiency
- Instruction manuals
- Underlying technology
- Existing security controls

Organizational Documentation

Network diagram

- Falls within audit scope
- Hosts
- Infrastructure devices
- Security control placement
- Common traffic flows

Risk assessment

- Prioritized list of assets and threats
- Existing security controls

Organizational Documentation

Products and services

- Know the business purpose of the client you are auditing
- Understand how products and services are made available, sold, and supported

Past audit reports

- Were recommendations acted upon?
- Business and technological changes since last report

Organizational Documentation

- Organizational security policies
  - VPN
  - E-mail
  - Social media
  - Mobile device usage
  - Document sharing and destruction
  - Clean desk policy

Stakeholder Needs

- Know your client
  - History
  - Products and services
  - Processes
  - Outsourcing dependencies
  - Previous audit reports
  - Questionnaires

Stakeholder Needs

Assets

Threats

Stakeholder Needs - Compliance

- Standards such as PCI DSS
- Regulations
- Contractual obligations
- Laws

Stakeholder Needs

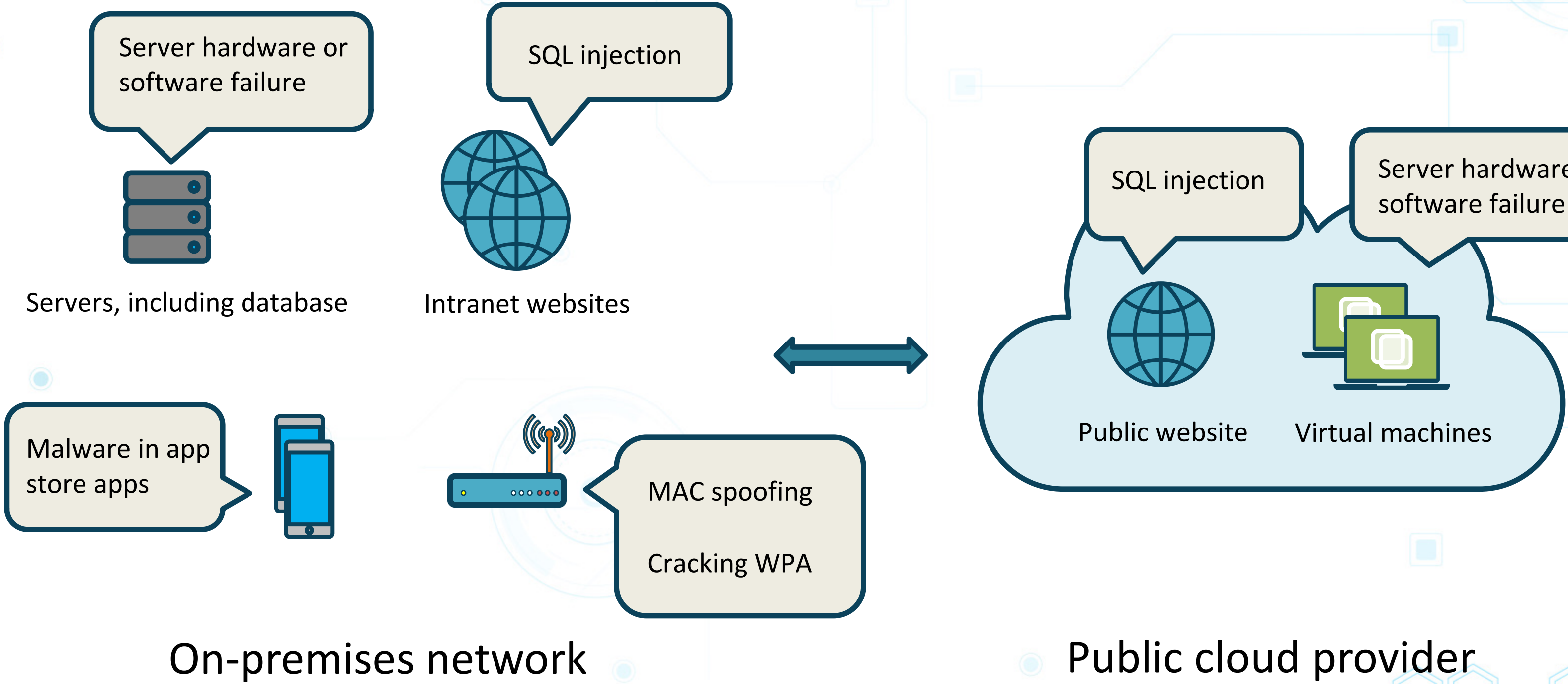
Audit scope

- Department
- Specific business process
- Network(s)
- Host(s)
- Database(s)

IS Auditing and Network Diagrams

- Understand the technology supporting business processes that serve business objectives
- Identify
  - Risks
  - Weaknesses
  - Control testing details
- Does the network comply with security requirements?

IS Auditing and Network Diagrams



Security Controls

Risk mitigation

Map to control objectives

Security Controls

Preventive

- Employee background checks
- User training
- Data backups
- Firewall access control lists (ACLs)
- Job rotation
- Door locks
- Security guards

Detective

- Log file review
- Intrusion Detection System (IDS)
- Alarm systems
- Job rotation
- Security guards

Security Controls

Corrective/recovery

- Restore a system or data to a functional state
- Data restoration
- Reimaging a failed server
- Patching a vulnerable host

Deterrent

- Perimeter fencing
- Lighting
- Signage
- Video surveillance cameras
- Security guards

Security Controls

- Compensating
  - Alternative or second choice to a primary control
  - Primary control
    - Cost prohibitive
    - Complexity
  - Examples
    - Segregation of duties
    - Network isolation for legacy devices that may not support password complexity requirements

Security Controls

- Approach existing controls with professional scepticism
  - What was once secure may no longer be effective

Control Objectives and Controls

- Maps specific audit objectives to how controls are tested
- Multiple controls can be used to satisfy a single control objective
- Control objectives can be influenced by
  - Laws and regulations
  - Contractual obligations

Control Objectives

Represent a desired state

Data availability

Financial transaction integrity

Data confidentiality

Control Objectives and Controls

Control Objective	Control(s)
No more than 2 hours of data may be lost	Back up data every 1.5 hours

Control Objectives and Controls

Control Objective	Control(s)
No more than 2 hours of data may be lost	Backup data every 1.5 hours
User awareness of latest social engineering threats	Monthly or quarterly lunch and learn sessions

Control Objectives and Controls

Control Objective	Control(s)
No more than 2 hours of data may be lost	Backup data every 1.5 hours
User awareness of latest social engineering threats	Monthly or quarterly lunch and learn sessions
Financial spreadsheet user accountability	Separate user accounts Audit file system access to spreadsheet files

Control Objectives and Controls

Control Objective	Control(s)
No more than 2 hours of data may be lost	Backup data every 1.5 hours
User awareness of latest social engineering threats	Monthly or quarterly lunch and learn sessions
Financial spreadsheet user accountability	Separate user accounts Audit file system access to spreadsheet files
Encryption of personally identifiable information (PII)	Force PII storage on Windows BitLocker disk volumes

Control Objectives and Controls

Control Objective	Control(s)
No more than 2 hours of data may be lost	Backup data every 1.5 hours
User awareness of latest social engineering threats	Monthly or quarterly lunch and learn sessions
Financial spreadsheet user accountability	Separate user accounts Audit file system access to spreadsheet files
Encryption of personally identifiable information (PII)	Force PII storage on Windows BitLocker disk volumes
High importance e-mail messages are authentic	E-mail digital signatures

Control Objectives and Controls

Control Objective	Control(s)
No more than 2 hours of data may be lost	Backup data every 1.5 hours
User awareness of latest social engineering threats	Monthly or quarterly lunch and learn sessions
Financial spreadsheet user accountability	Separate user accounts Audit file system access to spreadsheet files
Encryption of personally identifiable information (PII)	Force PII storage on Windows BitLocker disk volumes
High importance e-mail messages are authentic	E-mail digital signatures
Accurate migration of data between systems	XML file format

Audit Resource Planning

- Internal and external audits
- Team members
- Tools
- Budget

Audit Resource Planning

- External audit teams
  - Meetings and correspondence
  - May not be familiar with the client organization
  - Unaware of internal control changes since the last audit
  - Must be informed of audit objective and scope

Audit Resource Planning

Skillsets and tools

- Outsourcing of specialized skills such as auditing a Storage Area Network (SAN)
- Hardware and software tools used to conduct the audit

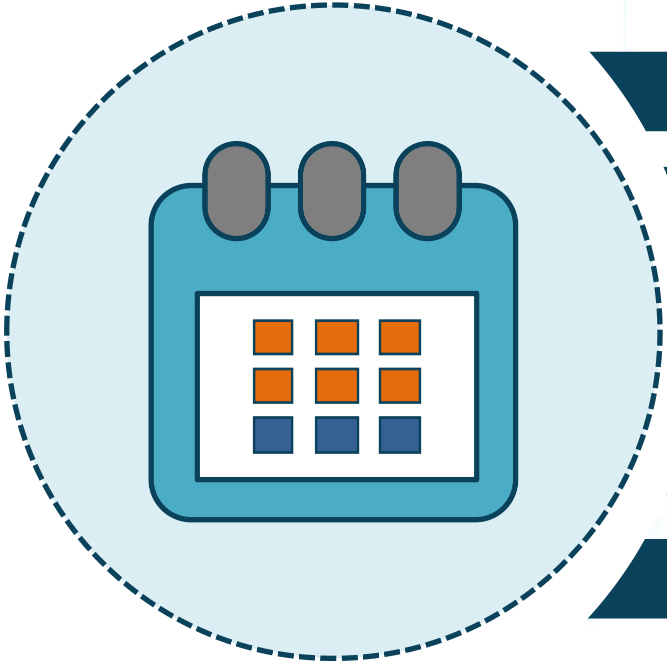
Audit Resource Planning

- Budget
  - External auditor travel and related expenses
  - External audit service fees
  - Internal audit team time allocation, training, and conferences
  - Costs of implementing remediations
  - Technology solutions
    - Storage for logs and tracking
    - Creation of scripts to test security controls

Audit Scheduling

- Part of the initial audit engagement letter or Statement of Work (SoW)
- Invoicing schedule (external auditors)

Audit Scheduling



- Audit commencement
- Audit progress communication
- Periodic audit status meetings
- Final deliverables (reports)
- Audit closing meeting

Audit Scheduling

Remediation follow-up meeting

Timing from audit completion will vary

Have recommended remediations been put in place?

Client may need direction with applying remediations

Urgent Incident Discovery

- The auditor has a responsibility to communicate the finding to the client immediately
- Technical or user related
- Intentional or unintentional

Urgent Incident Discovery

- ISACA Auditing Standard 1204: Materiality
  - Weak or absent controls result in a failure to meet control objectives

Urgent Incident Discovery

Fraud

- Internal and external threats
- Ineffective internal controls
- Preventative controls
- Detective controls when preventative fails

- Repo 105 (fraud 101)
  - Illegal financial statement manipulation
  - Short term loans are recorded as sales

Why Do People Partake in Fraud?

- Greed
- They think they will get away with it
- Shareholder and market expectations

Audit Reporting

Educate

Remediate

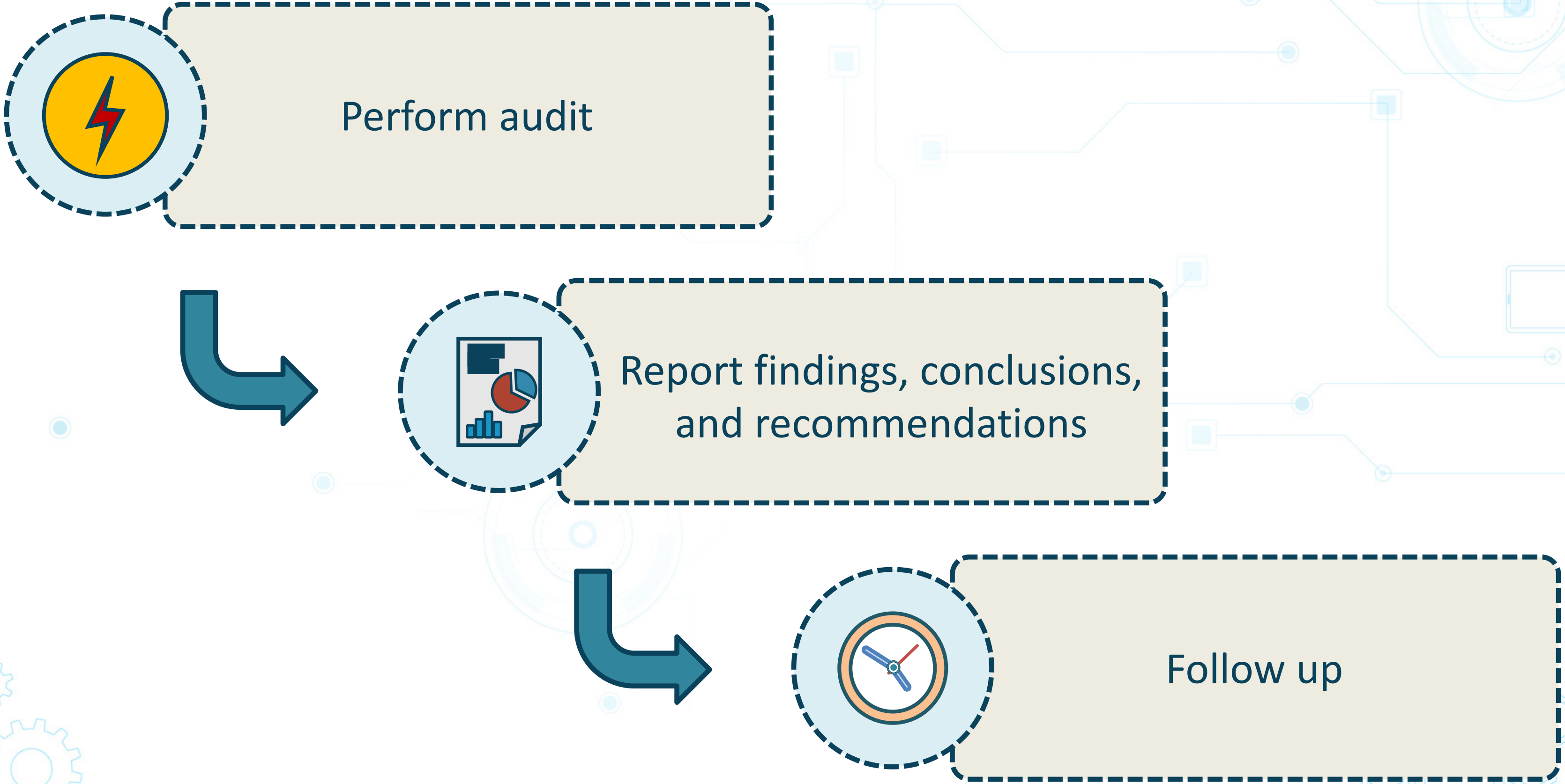
Audit Reporting

- Could consist of one or more reports
  - Certified signatures may be required
- Evidence must support audit findings
- Clearly state
  - Findings, conclusions, and recommendations
  - Information sources
- Fieldwork documentation
  - Tools and techniques used

Audit Reporting

- Recipients
- Is copying/printing/forwarding allowed?
- Audit report file integrity (prevent tampering)
- Documented management response may be required

Audit Findings Remediation Follow-Up



Perform audit

Report findings, conclusions, and recommendations

Follow up

Audit Findings Remediation Follow-Up

- ISACA Standard 2402: Follow-up Activities
  - Timely actions taken by management based on audit report recommendations

Audit Findings Remediation Follow-Up

- Timing is specified in the audit SoW
- Internal audits are often used to verify remediation effectiveness
- Controls that fail testing must be added to near-future testing list
- Compensating controls are sometimes necessary

In this exercise, you will

- Explain the purpose of information system auditing
- Provide an example for each control type
    - Deterrent
    - Preventative
    - Corrective
- Provide an example of a control objective and related control

The Purpose of Information System (IS) Auditing

- Do existing controls adequately protect assets?
- Identifies the current security posture of the organization to stakeholders

Control Type Examples

- Deterrent
  - Video surveillance cameras
  - Computer sign-on banners
- Preventative
  - Firewall ACL
  - Employee background checks
- Corrective
  - Applying patches
  - Recovering data from backups due to data corruption

Control Objectives and Control

- Control Objective
  - Database availability in the event of a natural disaster
- Control
  - Replicate the database to a different geographical region