



INSPECTOR GENERAL

INSTITUTE ®

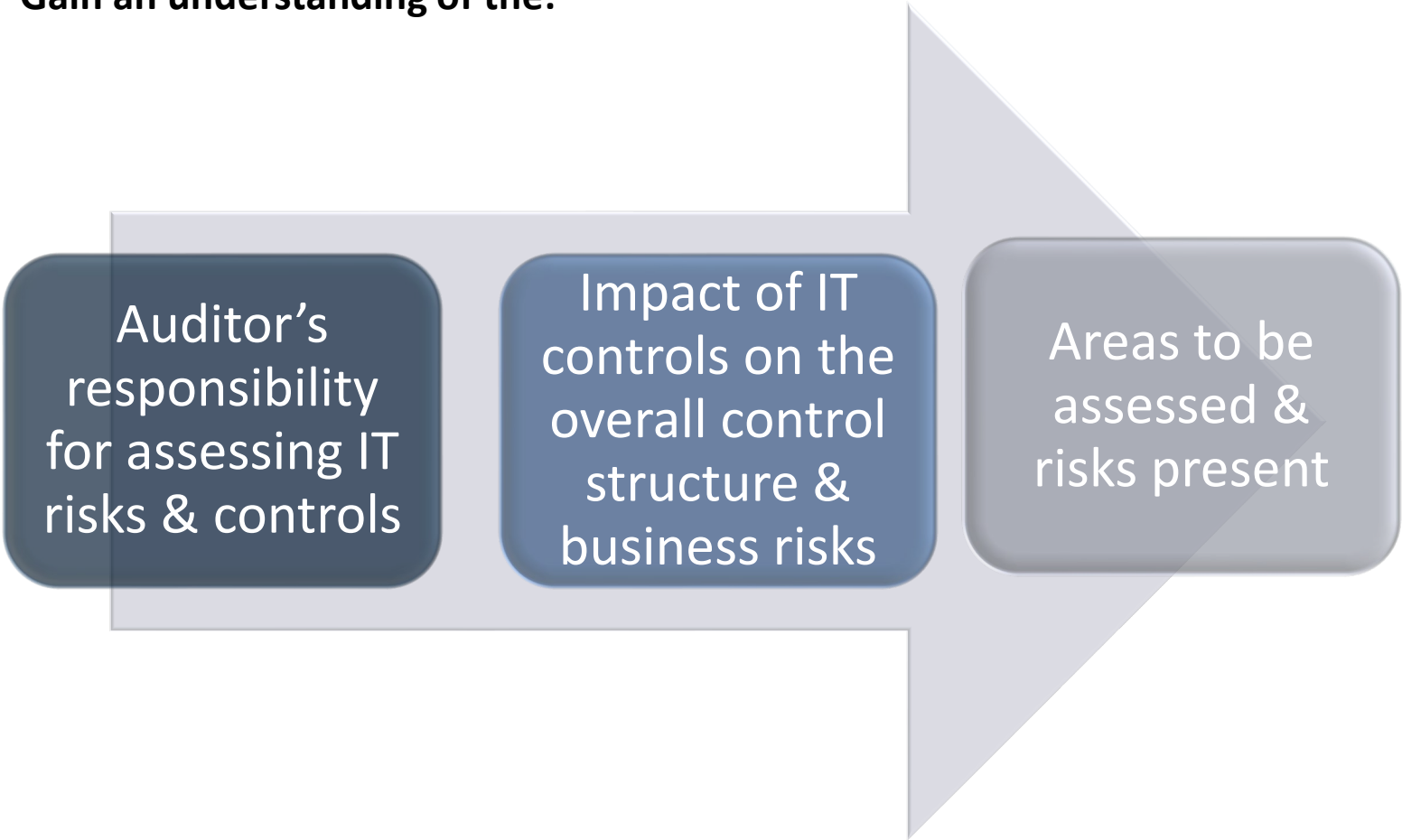
Association of Inspectors General

Information Technology Auditing IT Controls

Kate M. Head, CPA, CFE, CISA, CIG
USF System Audit
University of South Florida

Class Objectives

Gain an understanding of the:



Auditor's
responsibility
for assessing IT
risks & controls

Impact of IT
controls on the
overall control
structure &
business risks

Areas to be
assessed &
risks present



IIA Standards
for the
Professional
Practice of
Internal
Auditing-
Standard
1210.A3

“Internal auditors must have sufficient knowledge of **key information technology risks and controls and available technology-based audit techniques** to perform their assigned work.”

**Does not require specialized expertise in IT Audit*



IIA Standards
for the
Professional
Practice of
Internal
Auditing-
Standard
1210.A2

“The internal audit activity must assess whether the information technology governance of the organization supports the organization’s strategies and objectives.”



IIA Global Competency Framework 2013

Core Competencies

- ✓ Assesses and takes account of how IT contributes to organizational objectives, risks associated with IT, and relevance to the audit engagements.
(Staff and Managers)
- ✓ Assesses IT governance
(Manager, CAE)



INSPECTOR GENERAL

INSTITUTE®

ASSOCIATION OF INSPECTOR GENERAL

Certified Internal Auditor Exam

Part III, IT Section

I. Security

- System security (access controls, application authentication, encryption)
- Physical security

II. Application Development

- End user computing
- IS, system & application development methodology

III. System Infrastructure

- Hardware and software components
- STACK (network, operating system, database, and application)
- IT control frameworks

IV. Business Continuity/IT contingency planning



INSPECTOR GENERAL

INSTITUTE®

ASSOCIATION OF INSPECTORS GENERAL

Certified
Public
Accountant

Business
Environment
& Concept-
Area IV, IT

I. Understanding of IT:

- Organization & governance, systems & processes, and data

II. Risk Associated with IT:

- Processing integrity & security, availability, confidentiality, & privacy

III. Controls that respond to risks associated with IT:

- Application controls
- General controls
- Logical & physical controls
- Continuity & recovery plans



All Auditors should understand:

- I. How to assess IT risks,
- II. Basics of IT security,
- III. Application development & maintenance frameworks,
- IV. System infrastructure and how it impacts risks,
- V. Business continuity & recovery planning, and
- VI. IT governance requirements.



INSPECTOR GENERAL

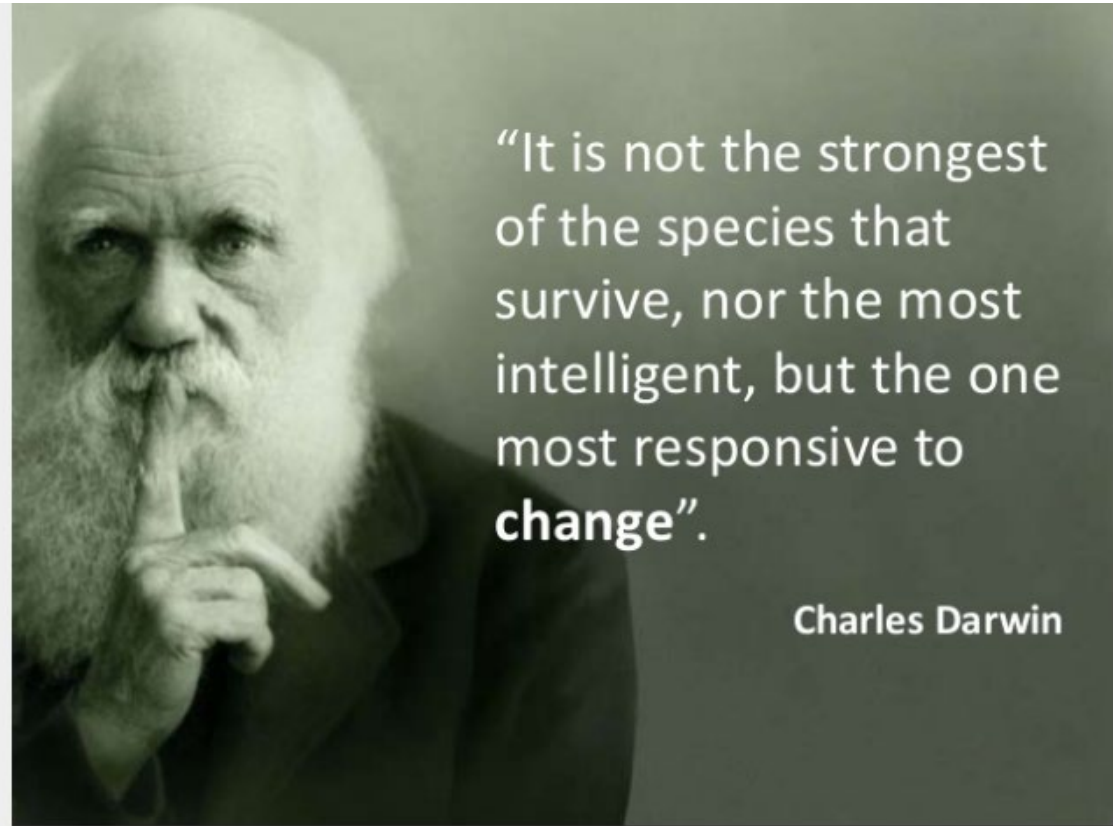
INSTITUTE®

Association of Inspectional General

GTAG: IT Risk & Controls

Developing the IT Audit Plan

Assessing IT Risk



“It is not the strongest
of the species that
survive, nor the most
intelligent, but the one
most responsive to
change”.

Charles Darwin

Consideration of IT Risks & Controls in Engagement Planning*

IT risks, like other business risks, must be included in the:

- Development of a risk-based audit plan
- Preliminary assessment of risk that drives the engagement, objectives, & scope, and
- Determination of appropriate and sufficient resources.



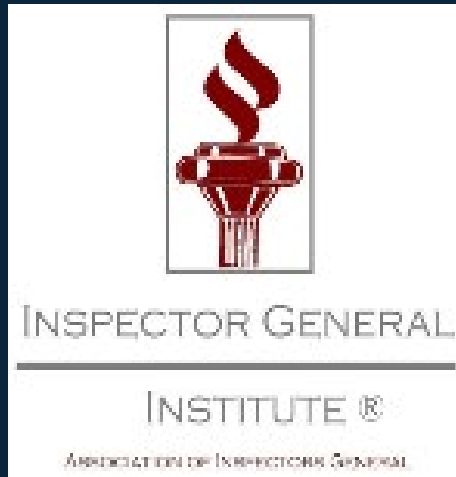
INSPECTOR GENERAL

INSTITUTE®

Association of Inspector General

IIA Standards:

- 2010 Planning
- 2210 Objectives
- 2220 Scope
- 2230 Resource Allocation



IIA Practice Guide: GAIT for Business & IT Risks

Assessing technology risk utilizes the same top down approach as operational and financial risks:

- I. Starts with identifying the business objectives for which the controls are to be assessed,
- II. Flows down to an assessment of key controls within the business processes (automated and IT general controls), and
- III. Identifies the critical IT functionality relied upon, among the key business controls and the application in which they reside.



IT Risk Considerations*

- The failure of technology is only a risk that needs to be assessed, managed, and audited if it represents a risk to the business.
- Both manual and automated controls must be assessed to determine whether the business risks are effectively managed by the appropriate combination of controls.

IIA Practice Guide:
GAIT for Business &
IT Risks



IT Risk Considerations*

- IT general controls may be relied upon to provide assurance of the continued and proper operation of automated key controls.
- Each IT general control operates at the four layers of each applications IT infrastructure.

IIA Practice Guide:
GAIT for Business &
IT Risks



General Controls apply to all systems, components, processes, and data in a given environment.

- IT governance & risk management
- Resource management & IT operations
- Application development & maintenance
- User management, logical security, and physical security
- Change management, backup and recovery, and business continuity

Application Controls pertain to a individual business process or application.

- Controls within an application around input, processing, and output
- Segregation of business functions
- Balancing of processing totals and data as it moves between applications
- Transaction logging and error reporting

GTAG: IT Risk & Controls

Control Classification

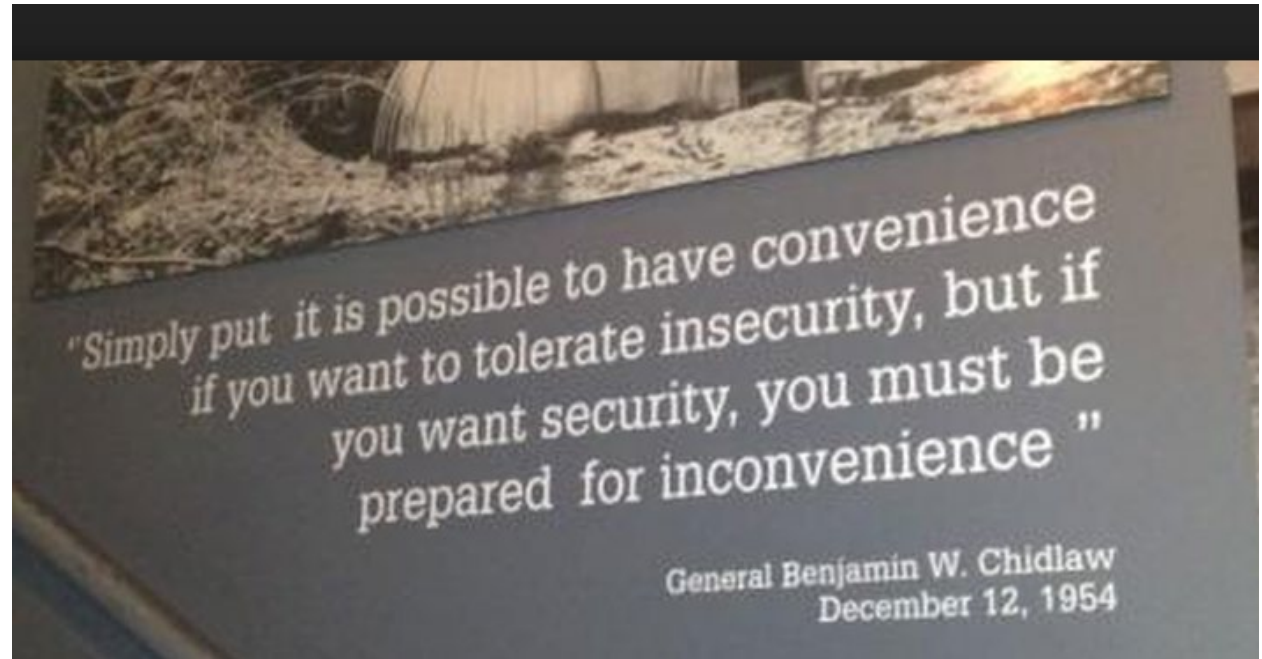


INSPECTOR GENERAL

INSTITUTE®

Association of Inspectional General

Basics of IT Security





INSPECTOR GENERAL

INSTITUTE®

Association of Inspector General

Control Objectives (CIA)*

Confidentiality

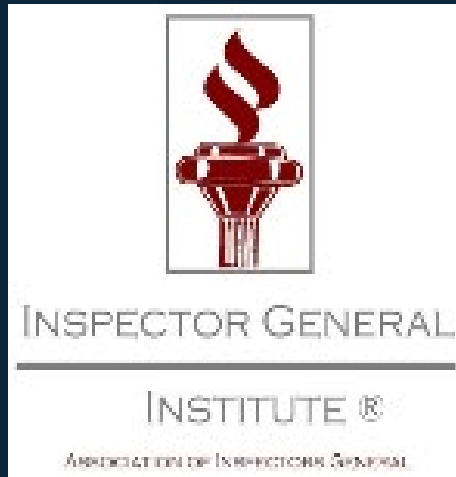
- **Data** which is private or confidential is not disclosed to unauthorized individuals during processing, in transit, or at rest.

Integrity

- **Data** has not been altered in an unauthorized manner during processing, in transit, or at rest.
- **System** is performing in an unimpaired manner free from unauthorized manipulation.

Availability of Systems and Data

- **Services and applications** are available and service is not denied to authorized user.



Data Integrity Means*

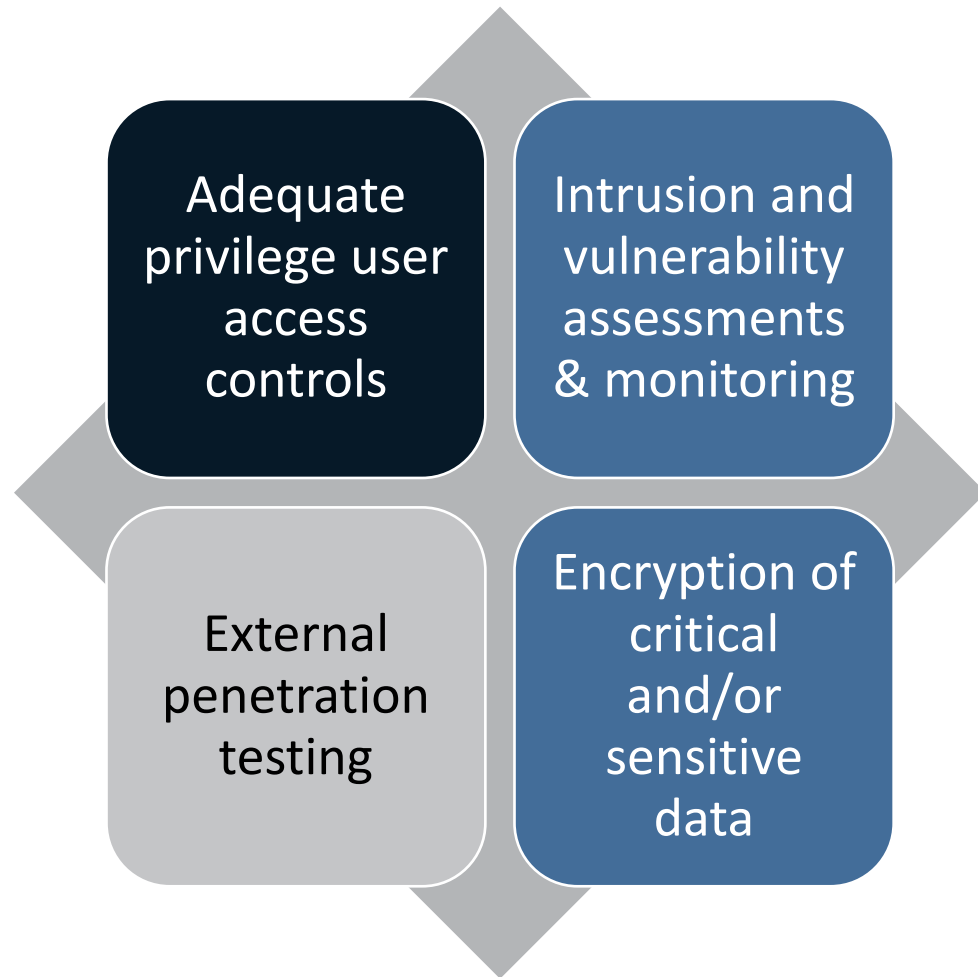
- Data entered into a application is accurate, valid, and consistent.
- Data uniqueness and referential integrity is maintained as data moves within the application.
- The assurance that information can be accessed or modified only by those authorized to do so.



INSPECTOR GENERAL

INSTITUTE®

Association of Inspector General





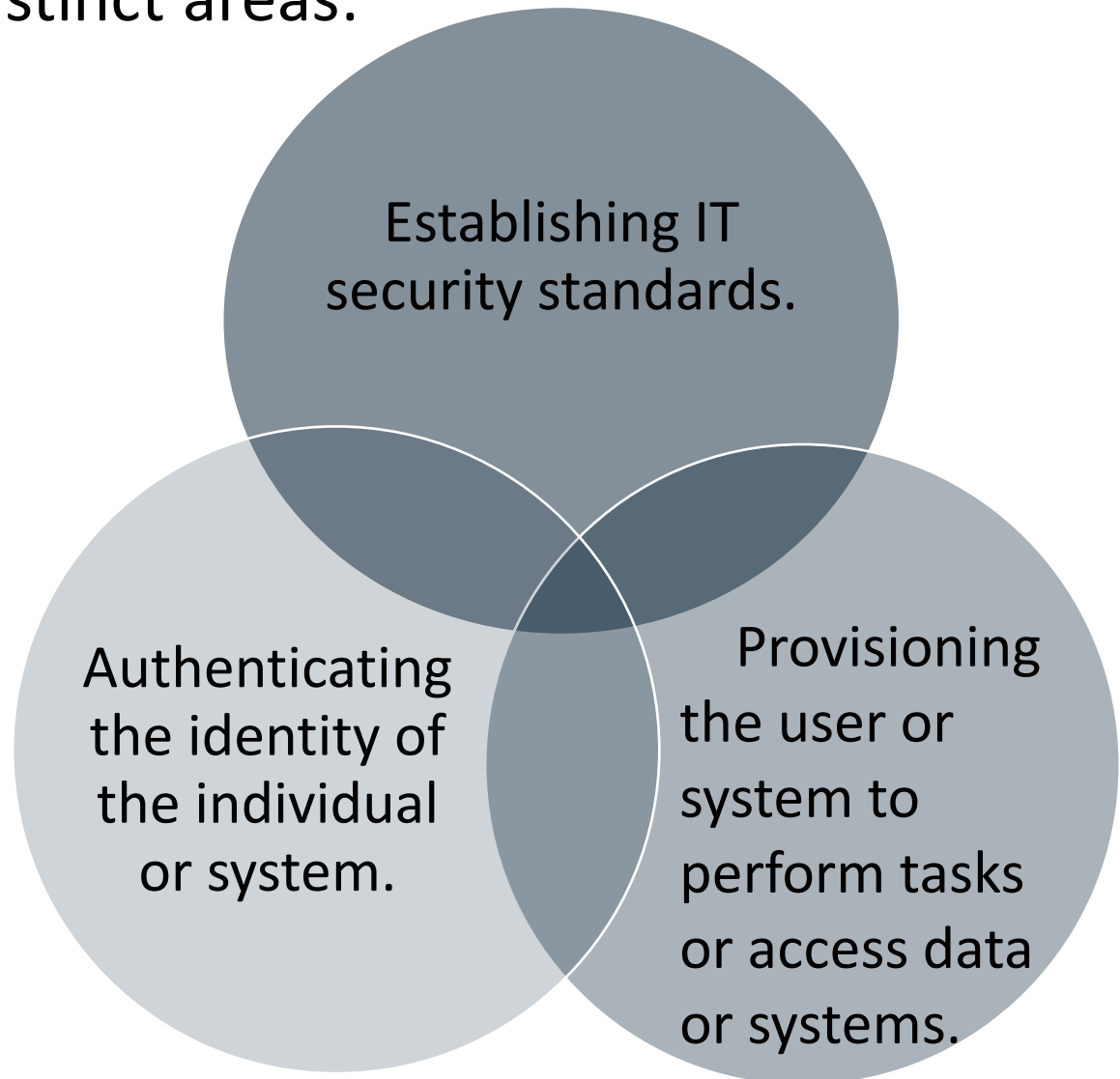
INSPECTOR GENERAL

INSTITUTE®

Association of Inspectional General

GTAG: Identity and Access Management

Identity management has three distinct areas:



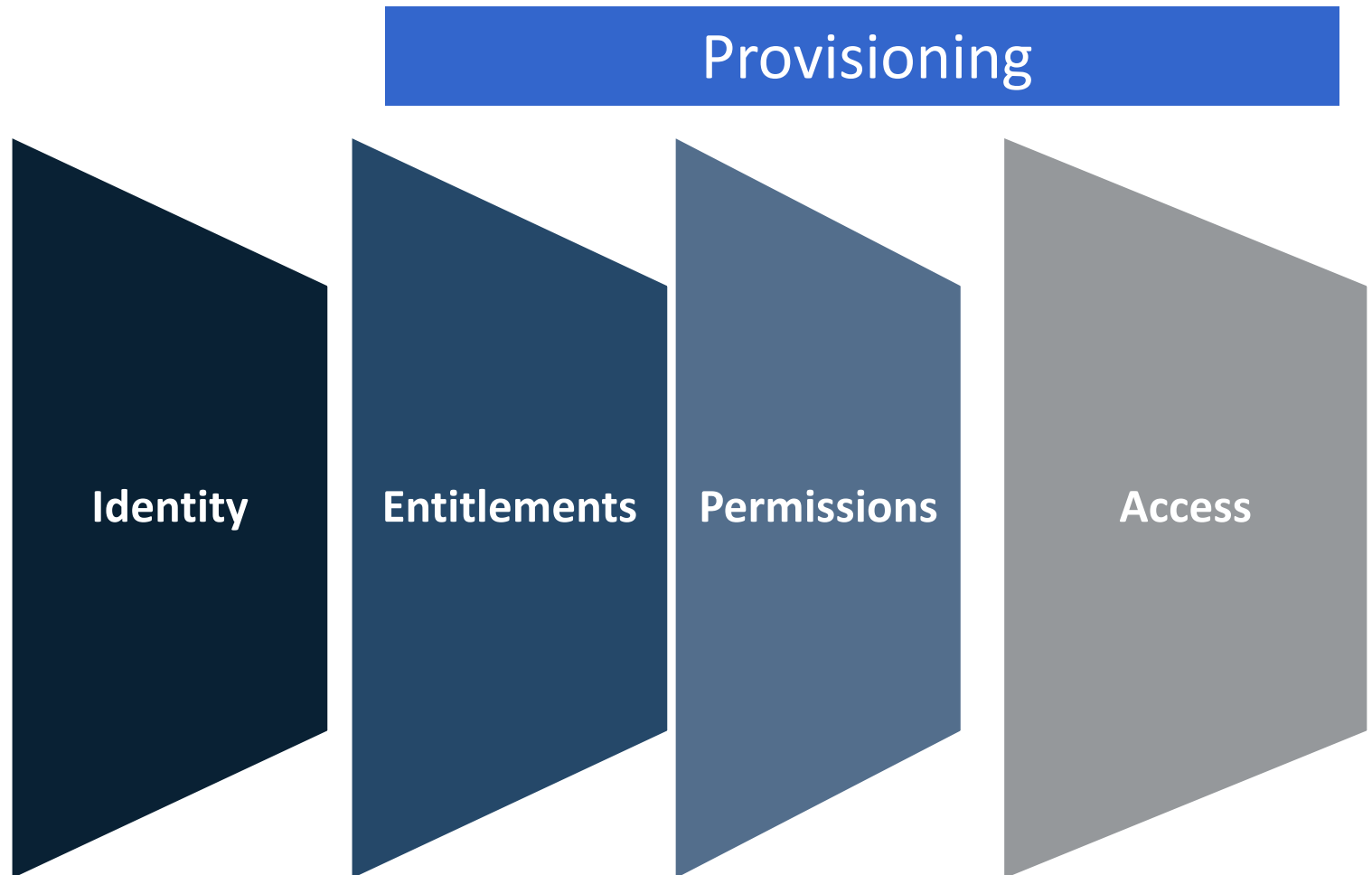


GTAG: Identity and Access Management

Identity management and entitlement policies should address the following:

- Security awareness training requirements.
- Standards for identity management.
- Background checks for employees.
- Password standards (complexity, expiration, number of invalid attempts, etc.).
- Appropriate use of access.
- Consequence for violation of standards.
- Overall strategy for provisioning access.

Identity Management Concepts





GTAG: Identity and Access Management

Identity Management starts with:

- Validating the user's physical identity,
- Determining the role the user plays in the organization, and
- Aligning access needs with the role based on the “least privileged” access model.



GTAG: Identity and Access Management

Provisioning/De-provisioning

- Automated provisioning/de-provisioning is based on the individual's role in the organization.
- Manual provisioning is based on access request and should include:
 - A formal process for requesting and approving access.
 - Review of other roles assigned to ensure proper separation of duties.
 - Approval of the access rights being granted for appropriateness.
- Monitoring for terminated users or others who no longer need access.
- Logging and monitoring of changes to user accounts.



GTAG: Identity and Access Management

Determining which Roles or Users are the Highest Risk

- Local Administrative Accounts
- Privileged User Access
- Domain Administrative Accounts
- Emergency Accounts
- Service Accounts
- Active Directory or Domain Service Accounts
- Application Accounts
- Access to Correction Mode
- Vendor Accounts

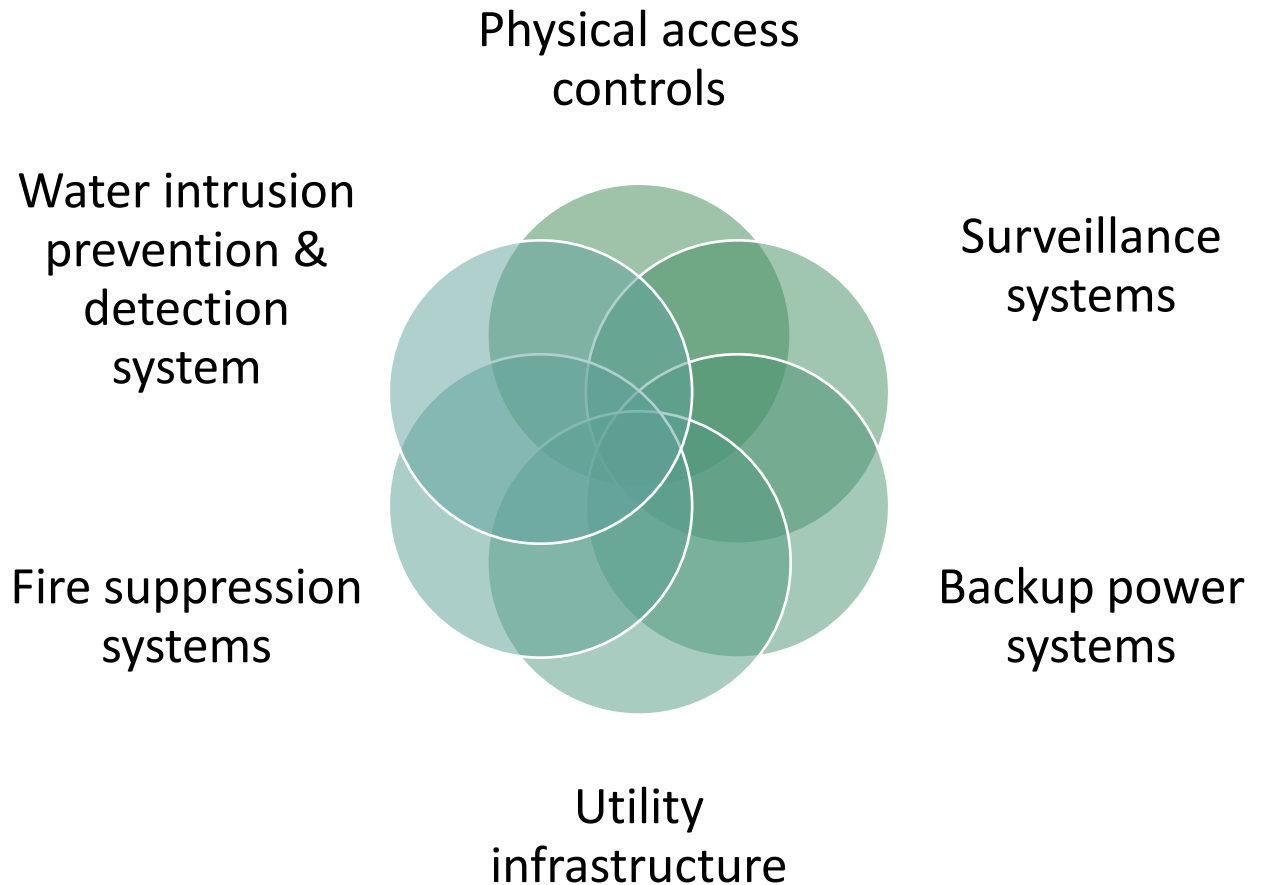


INSPECTOR GENERAL

INSTITUTE®

ASSOCIATION OF INSPECTOR GENERAL

Physical & Environmental Controls



Physical Access Controls – Best Practices

- ✓ The physical sites for IT equipment supports the technology strategy.
- ✓ Access control policy is defined and implemented.
- ✓ Logs are used to record access to sensitive areas.
- ✓ Information about sensitive IT sites and their design plans is limited.
- ✓ External signs and other identification of sensitive IT sites do not obviously identify the site.
- ✓ Vendors and external parties are not left unattended in sensitive areas.
- ✓ A process exists to ensure that storage devices containing sensitive information are physically destroyed or sanitized.

Environmental Controls – Best Practices

- ✓ IT facilities are situated and constructed in a way to minimize and mitigate susceptibility to environmental threats.
- ✓ Suitable devices are in place that will detect environmental threats.
- ✓ Alarms or other notifications are raised in case of an environmental exposure.
- ✓ Uninterruptible power supplies (UPS) are acquired and meet availability and business continuity requirements.
- ✓ Cabling external to the IT site is located underground or has suitable alternative protection.
- ✓ Cabling within the IT site is contained within secured conduits and hardened against environmental risk.
- ✓ Wiring cabinets are locked with restricted access.



INSPECTOR GENERAL

INSTITUTE®

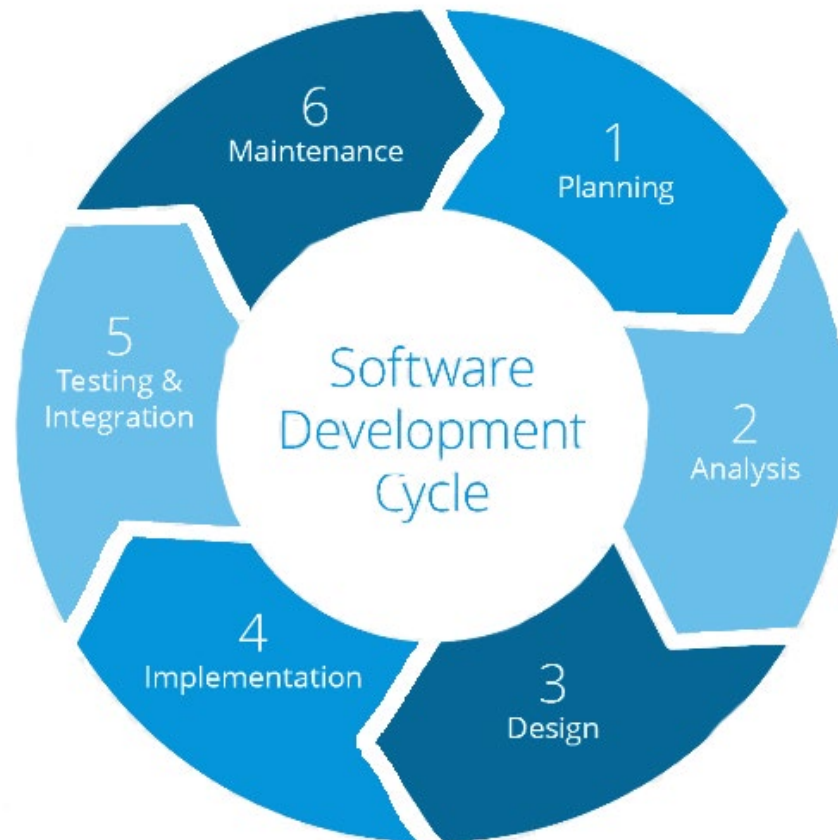
Association of Inspector General

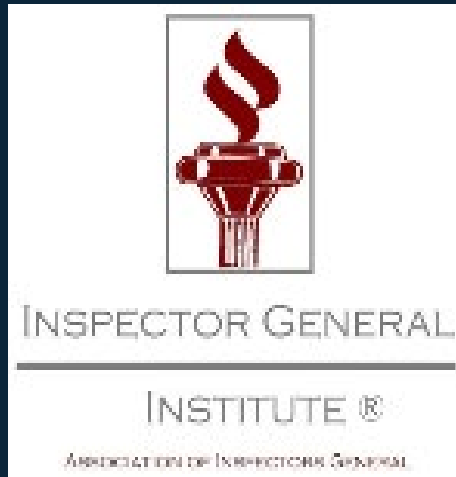
GTAG: Auditing IT
Projects

Auditing User –
developed
Applications

Change & Patch
Management
Controls

Application Development & Maintenance





GTAG
Auditing
User
Developed
Applications

June 2010

Applications that are developed by end users, usually in a non-controlled IT environment to automate and facilitate business processes.

- Spreadsheets
- Access databases
- Queries, scripts, or output from various reporting tools

End User Developed Application often lacks:

- Structured development processes and change management controls resulting in:
 - Lack of formal testing in non-production
 - Increased complexity over time
 - No version controls
 - Limited access controls
- Integrity over data downloaded from IT-developed or supported applications.
- Data validity controls within the application
- An experienced team of developers resulting in:
 - Minimal documentation
 - No future support for application



GTAG:
Change &
Patch
Management
Controls

“A set of processes executed within the organization’s IT department designed to manage the enhancements, updates, incremental fixes, and patches to production systems including application code revisions, system upgrades and infrastructure change.”

Change Management Best Practices

1. IT change management planning and implementation are integrated with changes in business processes.
2. Process is well developed and consistently followed.
 - Changes are subject to thorough planning and impact assessment.
 - Approval process for changes is in place.
 - Documentation is current and correct, with changes formally tracked.
 - Configuration documentation remains accurate.
3. There is a consistent process for monitoring the quality and performance of change management.

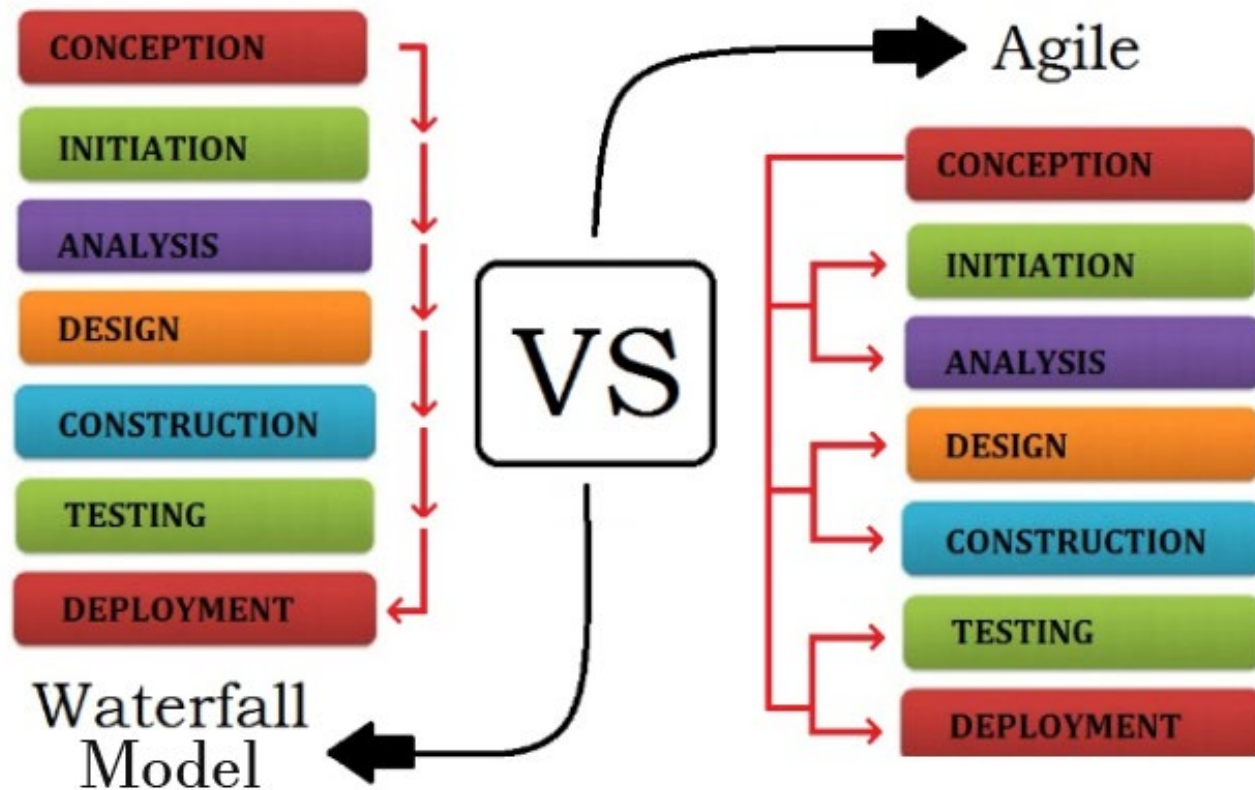


INSPECTOR GENERAL

INSTITUTE®

Association of Inspectional General

GTAG: Auditing IT Projects





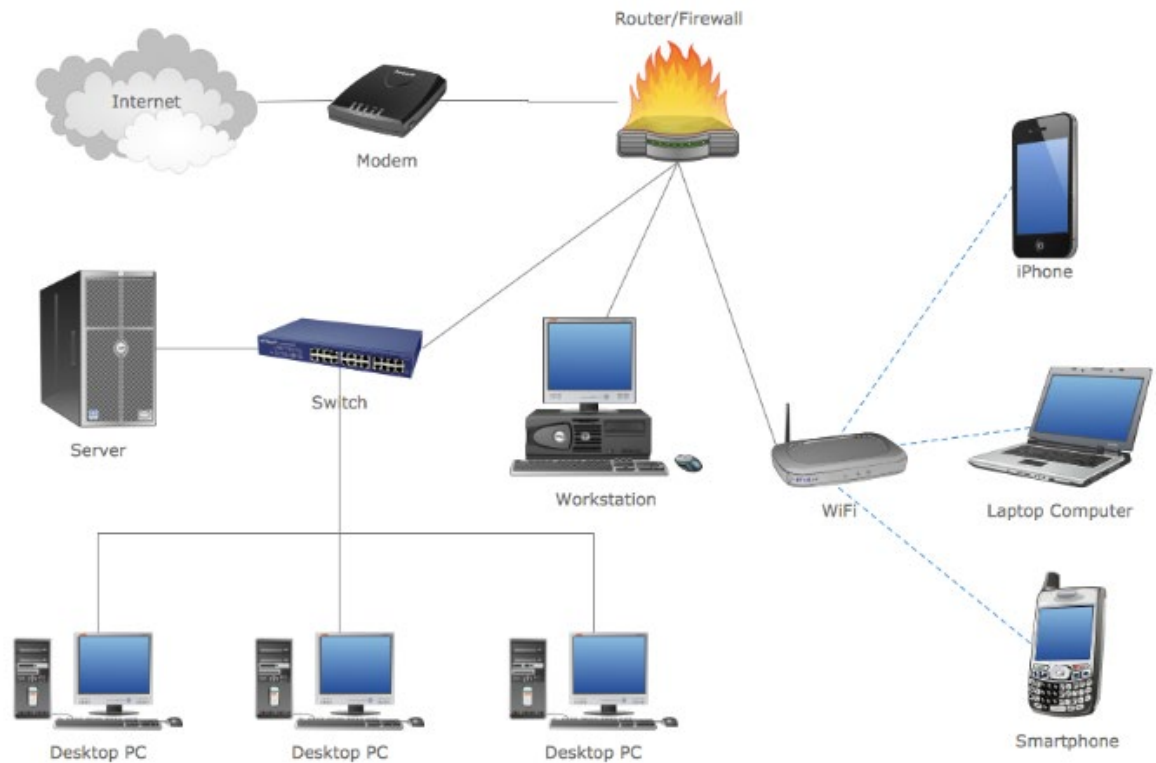
INSPECTOR GENERAL

INSTITUTE®

Association of Inspector General

System Infrastructure

Network Diagram



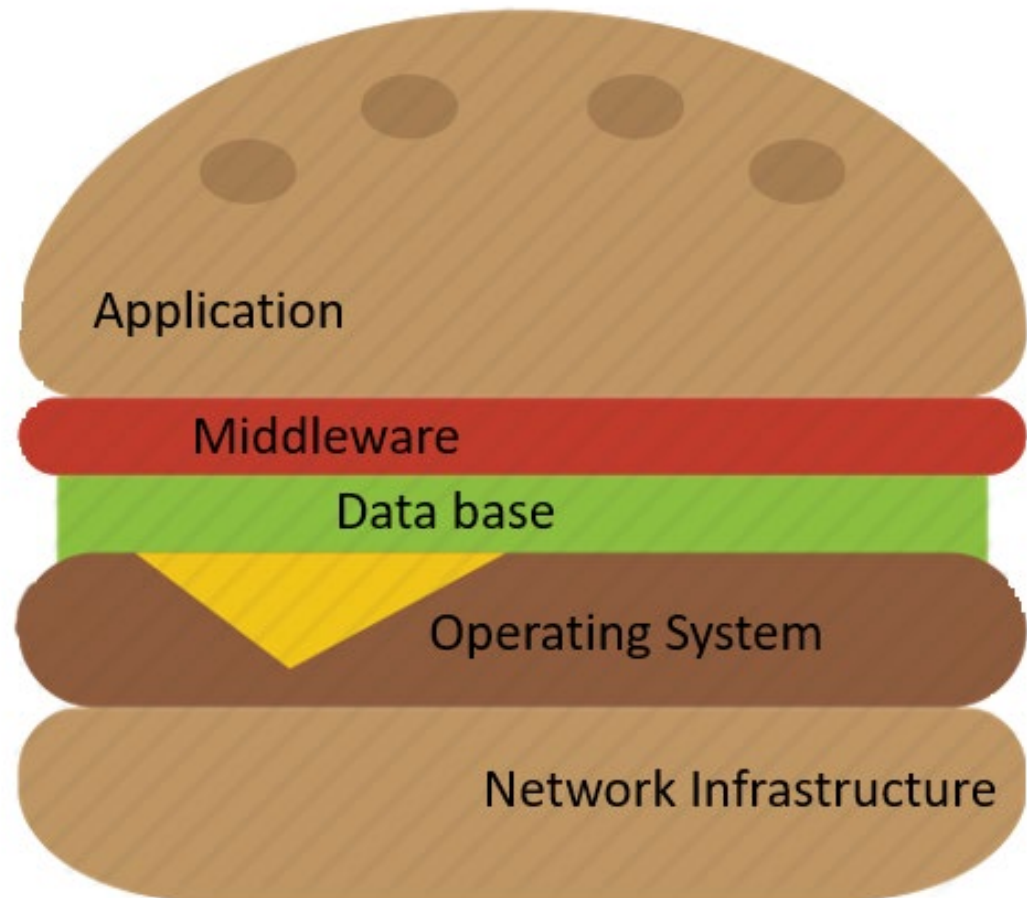


INSPECTOR GENERAL

INSTITUTE®

Association of Inspector General

Understanding the STACK





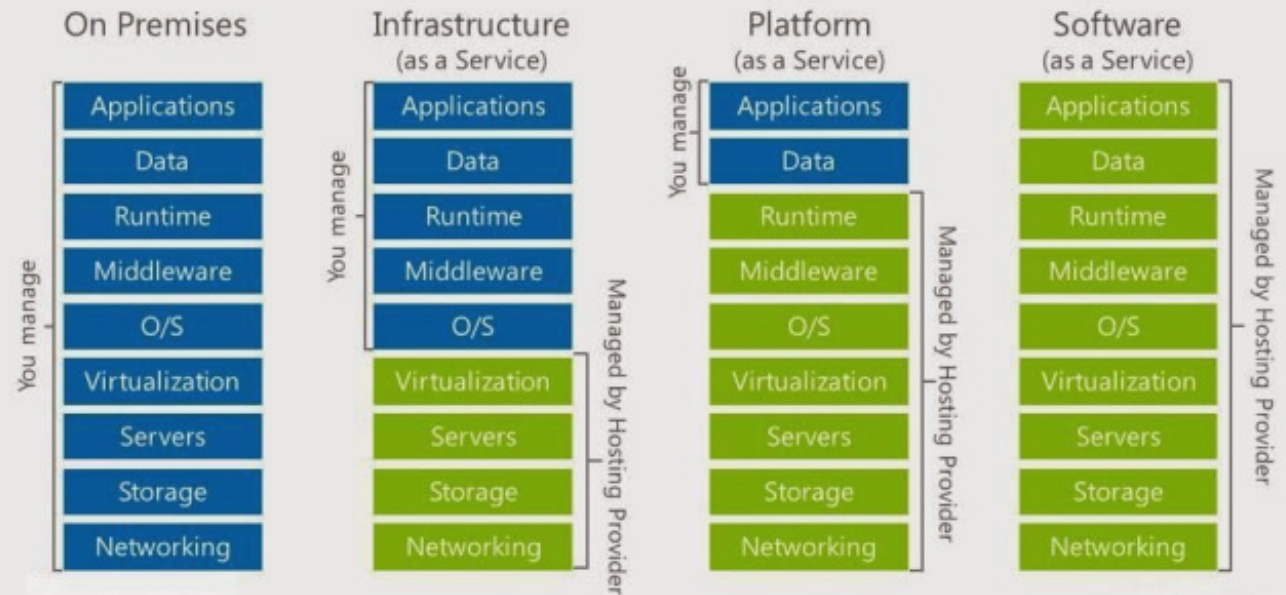
INSPECTOR GENERAL

INSTITUTE®

Associations of Inspector General

Impact of the cloud

Cloud Models





INSPECTOR GENERAL

INSTITUTE®

Association of Inspectional General

System Software

Network software

Communication software

Firewalls

Antivirus products

Identity access
management systems

Database management
systems



INSPECTOR GENERAL

INSTITUTE®

Association of Inspector General

System Hardware

Processing Devices

- Servers
- Computers
- Tablets
- Routers

Input Devices

- Pointing
- Audio Input
- Visual & Imaging
- Keyboards

Storage Devices

- Disk Drives
- Solid State Drives
- USB Drives
- Storage Arrays

Output Devices

- Printers
- Speakers
- USB Drives
- Monitors



INSPECTOR GENERAL

INSTITUTE®

ASSOCIATION OF INSPECTORS GENERAL

Determining what IT Assets are the most critical*

- The application and equipment housing this data inherits the level of criticality and sensitivity of the data it contains.
- Data is classified based on the criticality & sensitivity of the data



INSPECTOR GENERAL

INSTITUTE®

ASSOCIATION OF INSPECTORS GENERAL

Data Classification & Measuring Risk

Sensitivity - How freely can the data be handled.

- **Restricted:** Only authorized users can access.
- **Unrestricted:** Data is publically available.

Criticality - Importance of the data or system to the entity's operation.

- **Essential:** Critical to the operations, when unavailable for a short time, integrity is questionable.
- **Required:** Important but entity can function for a short period of time.
- **Deferrable:** Entity can function for an extended period without the data.

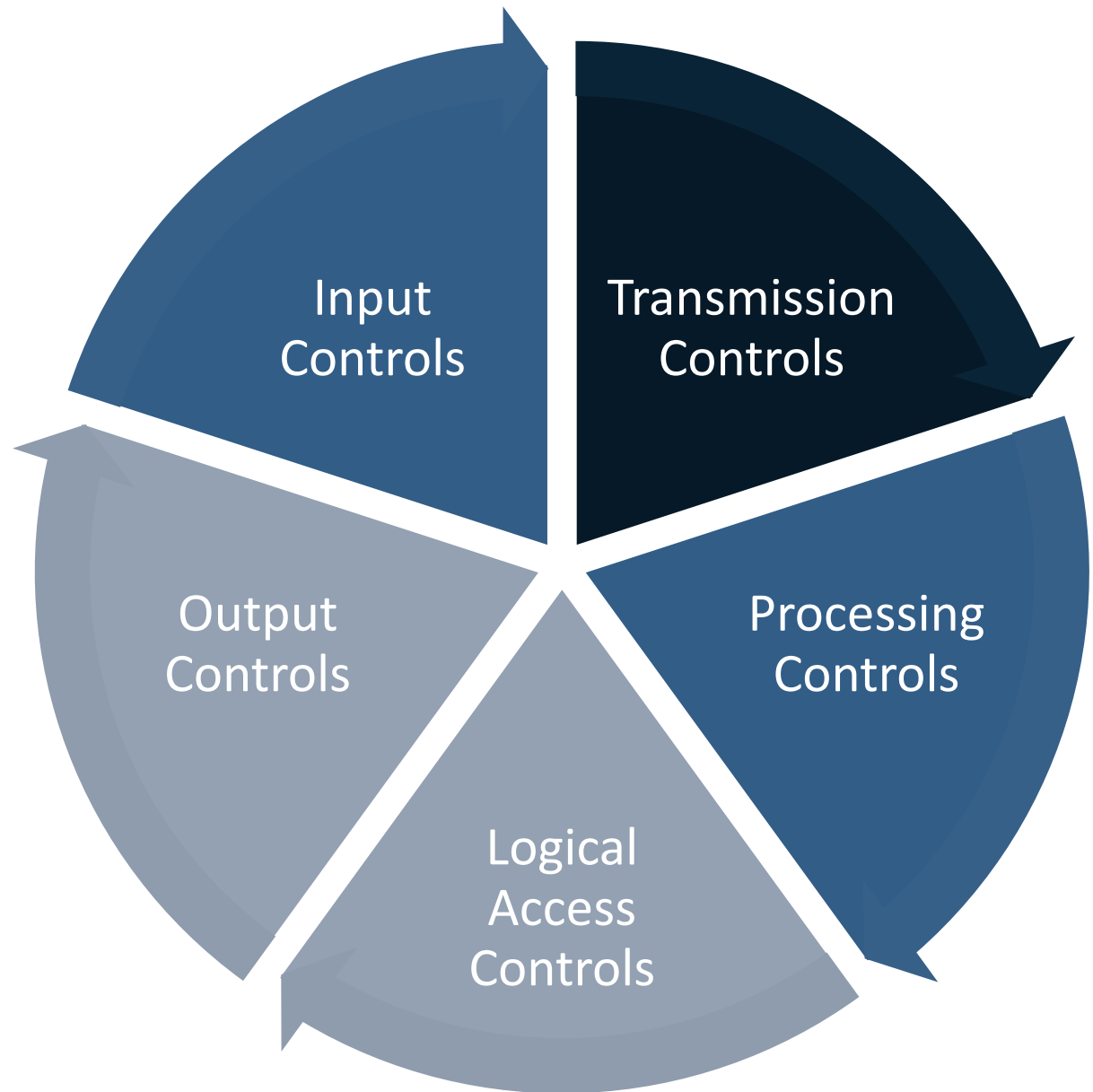


INSPECTOR GENERAL

INSTITUTE®

Association of Inspector General

GTAG Auditing Application Controls*





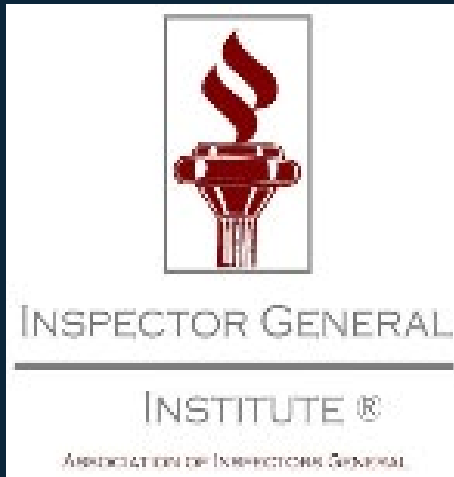
INSPECTOR GENERAL

INSTITUTE®

Association of Inspectional General

Business Continuity & Disaster Recovery





Disaster Recovery

- Disaster recovery operations protect an organization's mission-critical workloads against an infrastructure failure.
- Backups protect an organization against accidental deletions or modifications, or against ransomware attacks.



COBIT DSS 04

- Define business continuity policy and scope.
- Maintain a continuity strategy.
- Develop and implement a business continuity response.
- Exercise, test, and review the BCP.
- Review, maintain, and improve the continuity plan.
- Conduct continuity plan training.
- Manage backup arrangements.
- Conduct post-resumption reviews.



GTAG: Business Continuity Management

- Is there a fully documented up-to-date plan?
- Will stakeholders have access to the plan during an emergency?
- Is the plan based on risk?
- Are all critical business functions and systems covered?
- Have functional responsibilities for all key systems been assigned?
- Are the plans tested and revised based on the results?
- Do the plans call for coordination with local emergency services?



INSPECTOR GENERAL

INSTITUTE®

Association of Inspector General

GTAG: Auditing IT Governance

**Governance isn't
just about making
the "right"
decision; rather,
it's about the
process for
decision-making.**



INSPECTOR GENERAL

INSTITUTE®

Association of Inspector General

Governance: Policies & Standards

System and technology acquisition policies

System development and change management processes

System software configuration standards

System application control standards

Data classification standards

Documentation standards



INSPECTOR GENERAL

INSTITUTE®

ASSOCIATION OF INSPECTORS GENERAL

Organization and Management Controls

Best Practices

IT organizational structure is formally defined and aligned with the governance structure.

Management expectations are communicated.

Data and system ownership is established.

IT is placed appropriately in the organization relevant to criticality.

Procedures are in place to monitor compliance with procedures.

The information security policy is defined, maintained, and aligned with the overall enterprise and IT strategy.



INSPECTOR GENERAL

INSTITUTE®

Association of Inspector General

Organization and Management Controls

Management Control Examples

Systems and data is categorized based on criticality to the business operation and sensitivity of data.

An inventory of IT projects, services, and assets is maintained.

There is a formal process in place to prioritize and allocate resources based on risks.

IT-related financial activities are appropriately managed.

HR process supports the acquisition and retention of adequate, competent IT personnel.

Skills and competencies of personnel is maintained.

Service level agreements are in place.



INSPECTOR GENERAL

INSTITUTE®

Association of Inspector General

Other Global Technology Practice Guides (IIA)

IT Outsourcing

Continuous Auditing

Data Analysis Technologies

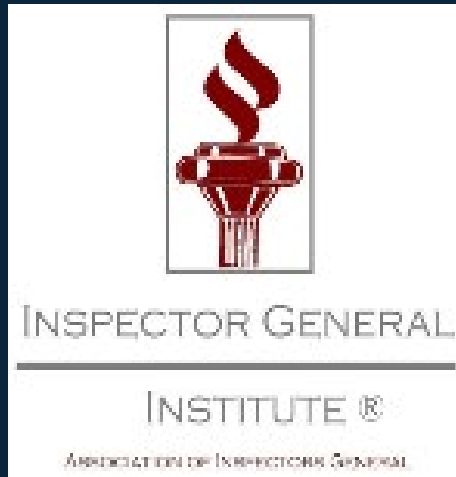
Assessing Cybersecurity Risk

Auditing Smart Devices

Understanding & Auditing Big Data

Auditing Insider Threat Programs

Fraud Prevention & Detection in an Automated
World



**Kate M. Head, CPA, CFE, CISA, CIG
Associate Director**

USF System Audit
University of South Florida
Tampa, FL

Khead@usf.edu
813-774-2457