Auditing IT Controls

Presented by: Kate M. Head, CPA, CISA, CFE, CIG

Course Objective: Increase Knowledge of

AUDITOR'S RESPONSIBILITY IN ASSESSING IT RISKS

THE IMPACT OF IT CONTROLS ON THE OVERALL IC STRUCTURE

HOW TO AUDIT IT CONTROLS

IA Responsibility for Assessing IT Risks

Auditors must have sufficient knowledge to perform their assigned work

This includes:

- **Key information technology risks and controls**
- **Available technology-based audit techniques**

Auditor is not required to have specialized expertise in IT audit.

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

IIA Global IA Competency Framework

Environment Knowledge Area: Information Technology

Level 1: General Awareness

- Recognize the purpose and application of IT Control frameworks and basic IT controls
- Describe the various risks related to IT, information security, and data privacy
- Describe the basic concepts of IT and data analytics

IIA Global IA Competency Framework

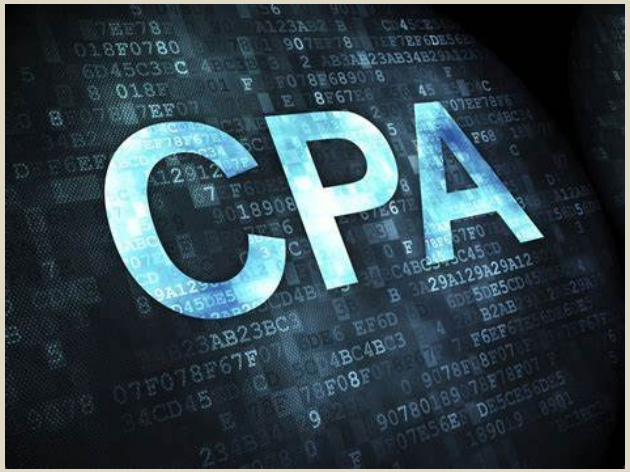
Environment Knowledge Area: Information Technology

Level 2: Applied Knowledge

- Apply IT control frameworks
- Identify and assess various risks related to IT, information security, and data privacy
- Apply data analytics and IT in auditing

Internal-Audit-Competency-Framework.pdf (theiia.org)

How many Participants are:

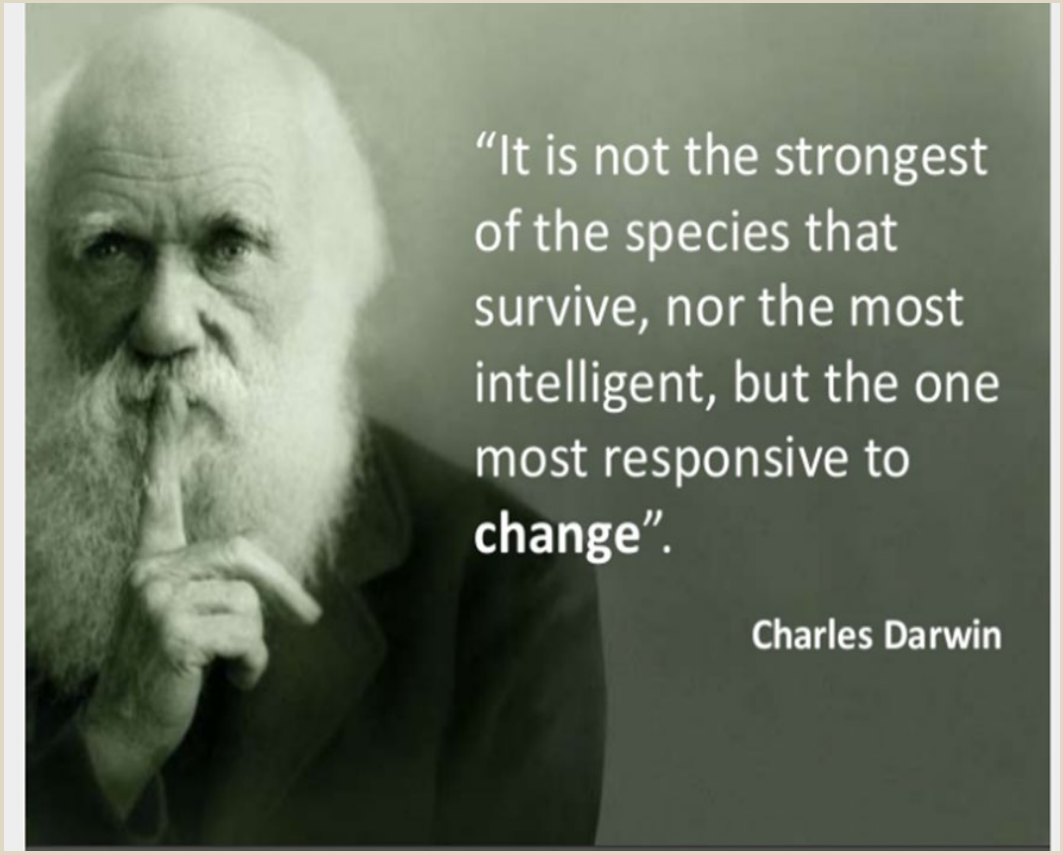


Assessing IT Risks vs Non IT Risks

IT risk cannot be assessed in Isolation without considering business risks

Operational and financial risk cannot be assessed without considering reliance on technology

Assessing Impact of IT Risk



Impact of IT risk must be considered throughout the <u>entire</u> IA planning process:

- **Audit plan development**
- **Determination of engagement scope & objectives**
- **Assignment of staff/resources**

Top-Down IT Risk Approach

Identify business objectives for which risks are being assessed

Identify key controls (manual, application and IT general controls)

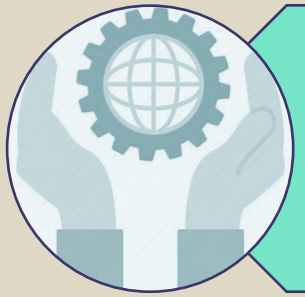
Identify critical IT functionality relied upon by the business process and applications in which they reside

IIA Practice Guide: GAIT for Business and IT Risks

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

Classification of IT Controls by Level



Entity (IT Governance)

Organization

(General Controls)

Application

(Application Controls)

General IT Controls- Defined

General IT Controls (GITCs)

- Provide the foundation for reliance on data, reports, automated controls, and other system functionality
- Ensure proper development and implementation of applications
- Impact integrity of programs, data files, and computer operations

GITCs are controls which:

1. Relate to the environment with which computer-based application systems are developed, maintained and operated
2. Are applicable to all applications

Key Consideration of IT General Controls

IT general controls may be relied upon to provide assurance of the continued and proper operation of automated key controls with applications and systems

Impact of Failure of GITCs

- Hinders the ability to prepare accurate financial and operating reporting
- Increases the risk of fraudulent transactions and/or fraudulent reporting
- Governance failures impacts availability of IT resources
- Higher risk of unintentional or intentional data processing errors

Impact of Pervasive IT General Control Failures ★

Subset of GITCs which focus on the management and monitoring of the IT environment.

Pervasive IT controls effect reliability of:

a. **Application controls in the business process systems**

b. **Detailed IT controls over data availability, application program development, system implementation, security administration and backup procedures**

COBIT IT Auditing Framework (ITAF 220.7.3) states “Weak pervasive IT controls, and thus weak management and monitoring of the IT environment should alert practitioners to the possibility of a high risk that the controls designed to operate at the detailed level may be ineffective.”

IT Governance Vs. IT Management

IT **Governance** (leadership)

Establishes the IT governance framework to ensure:

i. **IT strategies are aligned**

ii. **IT investments are optimized**

iii. **Risks are identified and managed**

iv. **IT resources are managed effectively**

v. **Performance is monitored**

IT **Management** (operations)

i. **Implements the policies set by the governance team**

ii. **Develops and implements processes related to the management of the IT operations**

   a. **IT operational strategy**

   b. **Strategy for defining, acquiring and implementing IT solutions**

   c. **Operational delivery and support of IT services including security Performance monitoring and conformance with IT performance targets, IC Objectives, and external requirements**

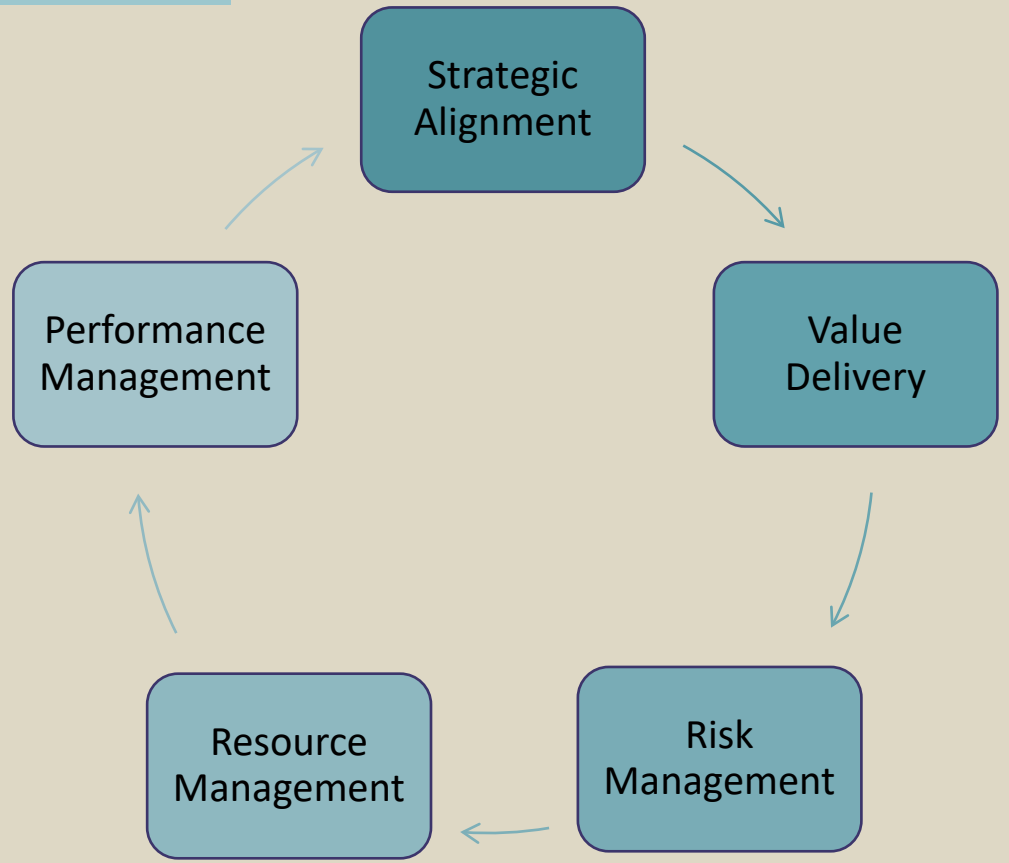
Assessment of IT Governance

IA of IT governance should focus on the organization's implementation of governance practices which include:

- clearly defined policies, procedures
- roles, and responsibilities of governing entities
- effective communication with stakeholder
- alignment of risk appetite with strategies
- management of IT value
- clear accountability for performance
- appropriate tone from the top

IT Governance Framework Components

The focus of IT governance is on creating alignment between organizational priorities and IT objectives to ensure that IT efforts concentrate on processes or projects that support strategic goals



Common ITGC Areas

- Identify and Access Management (logical security)
- Change Management
- Physical and Environmental Controls
- Business Continuity & Disaster Recovery (corrective controls)

Identity & Access Management (IAM)

Identify	• Issue and manage digital identities allowing them to be uniquely authenticated (identified) before being granted access to IT assets
Authorize	• Provide assurance that only authorized users have access to sensitive business applications, information and operating environments
Align	• Align the IAM strategy with the organization's identity policy and IT architecture

CIA: IS Policy Objectives ★

Confidentiality

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

Availability

Data, services and applications are available and service is not denied to authorized user

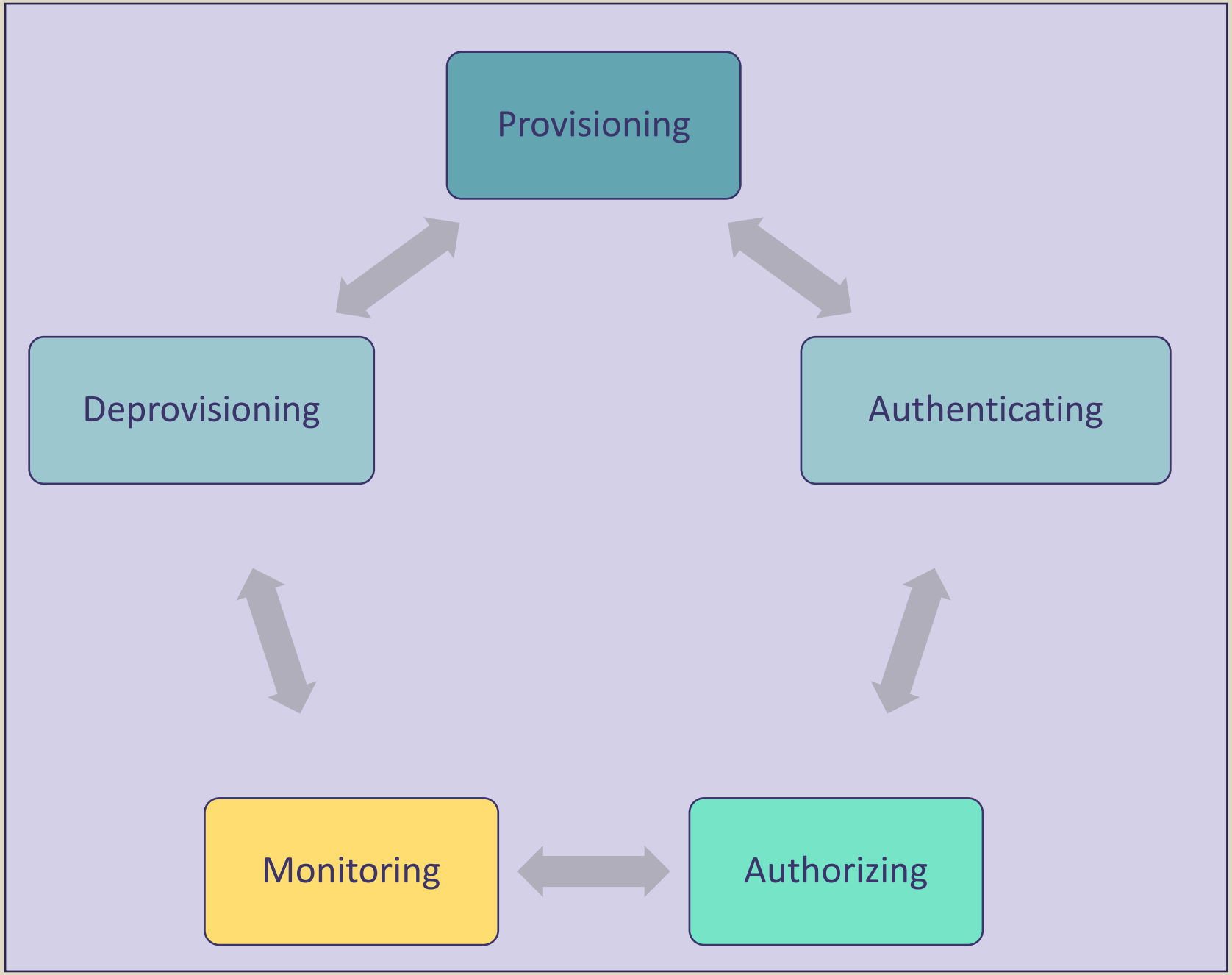
Integrity

Data Integrity refers to the accuracy and completeness of data. Data has not been altered in an unauthorized manner during processing, in transit, or at rest

System Integrity is performing in an unimpaired manner free from unauthorized manipulation.

IAM Framework Governs:

I. **Identity management strategy**
II. **Strategy to provision and deprovision access**
III. **Assignment or risk levels to key systems and related data**
IV. **Authentication standards for access based on risk levels**
    a. Password standards
    b. Multi-factor authentication
V. **User access controls**
    a. Appropriate use of access and consequence for violation of standards
    b. Background checks for employees
    c. Security awareness training requirements



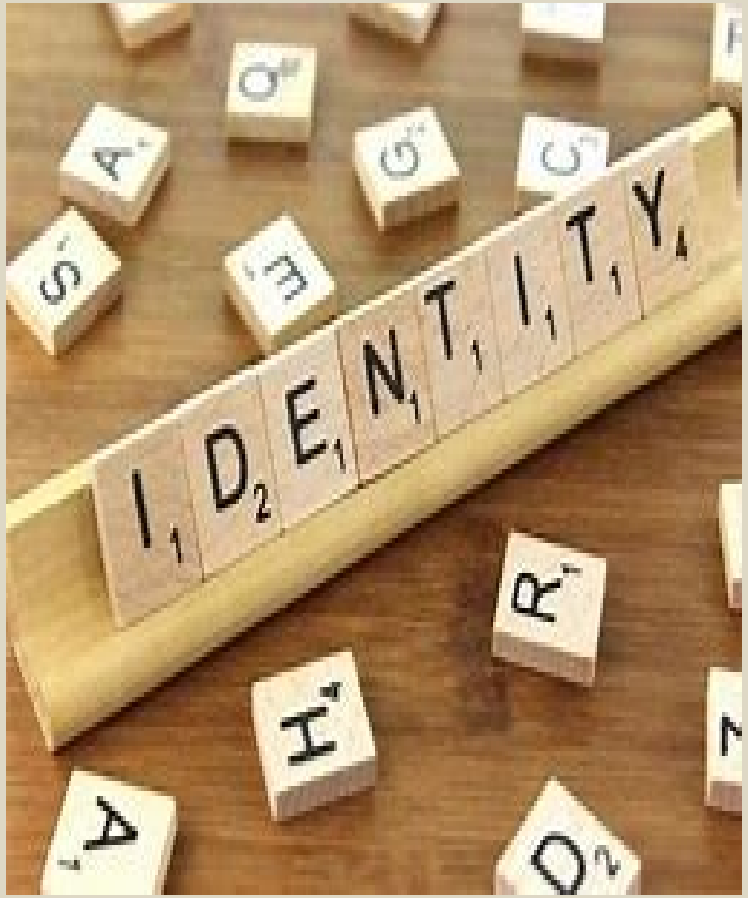
IAM Process

- **Initial Provisioning and maintenance of user identities through out the life cycle**
- **Authentication and monitoring processes**
- **Managing user permissions (Authorizing)**

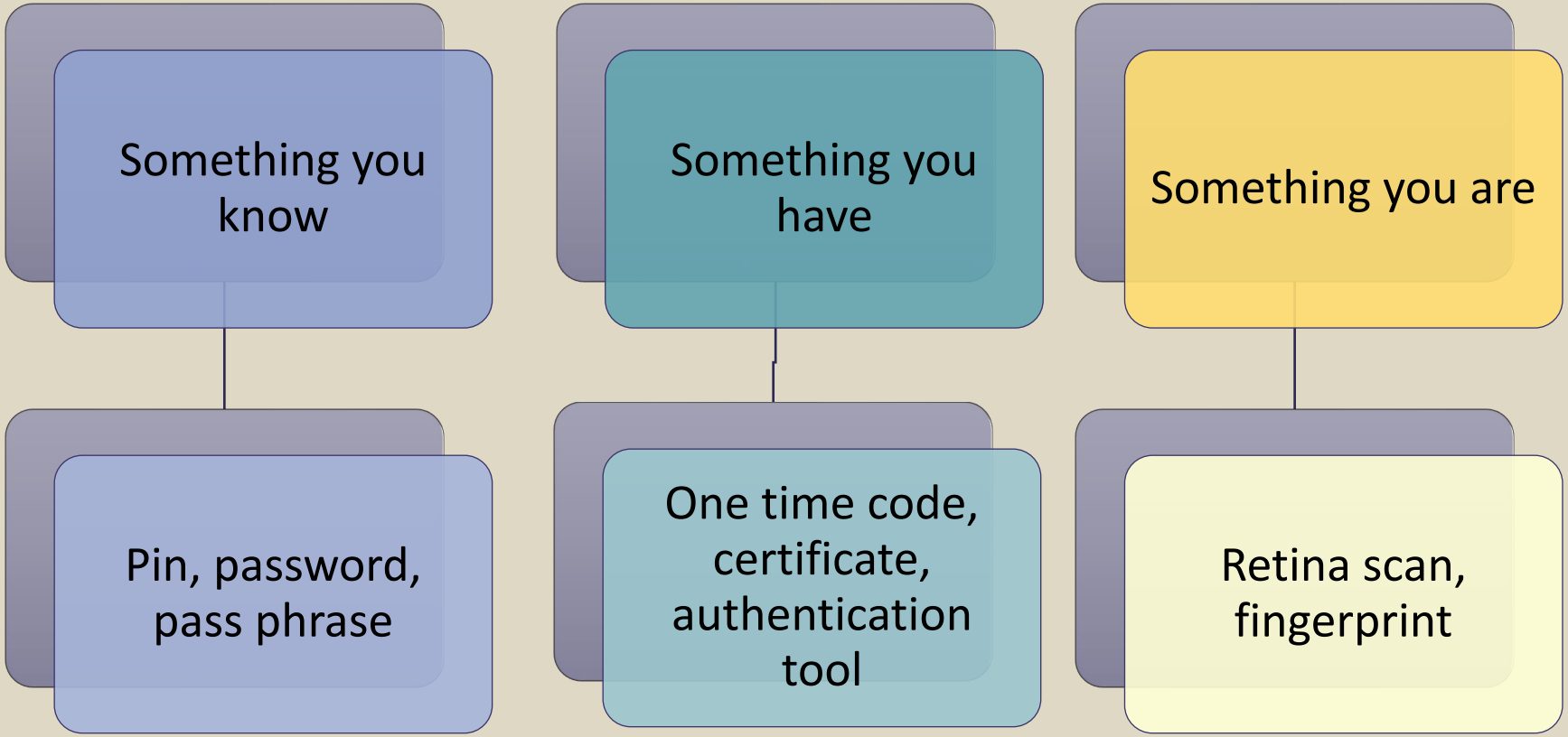
Identity Management: Who are you?

The required strength of the evidence is based on:

- **Laws & regulatory guidelines**
- **Access to sensitive information**
- **Potential Impact to organizational risks, which may result in:**
  a. **Damage to reputation**
  b. **Financial losses including potential civil and criminal violations**
  c. **Personal and public safety concerns**
  d. **harm to organizations programs**



Authentication Methods



Access Management

Manage & Monitor	Managing roles, responsibilities, access privileges and levels of authority for information including ensuring segregation of duties
Provision	Provisioning access rights on a need-to-know and least privilege basis aligned with user's job requirements and business need
Deprovision	Ensuring timely deprovision upon termination or transfer

The process used to provision, deprovision, and monitor access to IT resources aligned with the IT Governance strategy and risk.

Change Management (CM)

Ensures that all changes to business processes, applications and infrastructure are processed in a controlled manner and that change requests are handled quickly, efficiently, and effectively

Provides the organization with a repeatable, measurable, and auditable process that captures all technology-related changes

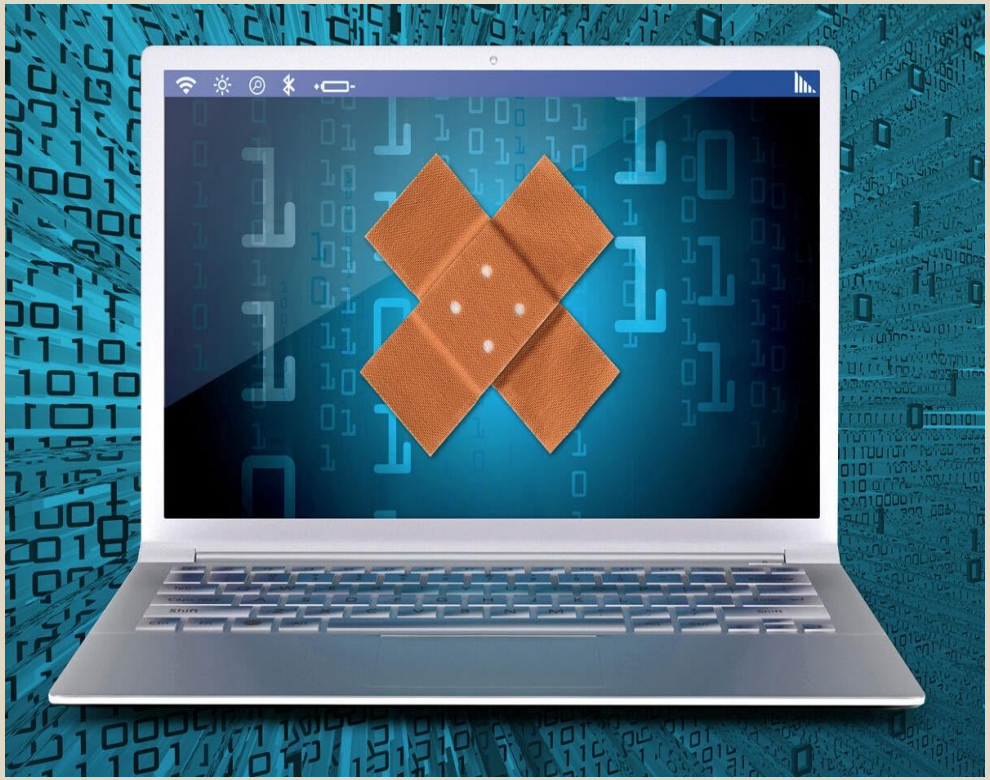
Reduces potential of issues related to Confidentiality, Integrity and Availability

Categorization of Change:

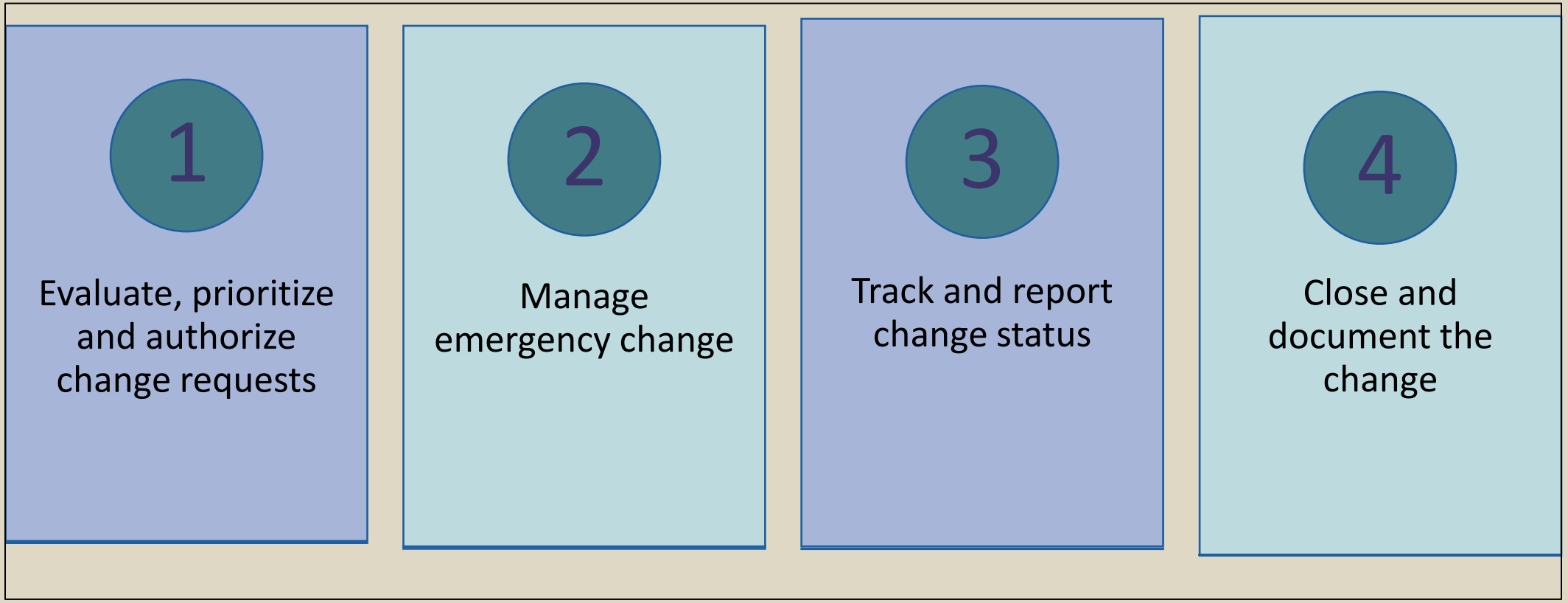
Routine/Standard: frequently occurring, low risk changes that can be preapproved

Regular/Normal: application, middleware, operating system or network hardware and software upgrades or changes. Requires review prior to approval

Emergency: urgent corrective actions needed to prevent service failure or disruption



Key Control Attributes

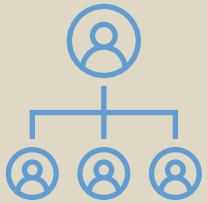


Roles and Responsibilities

Process and System Owners

Initiate change request

Participate is acceptance testing



Change Manager

Responsible for the change management system and database, policies, procedures and standards, as well as leadership of a change advisory board

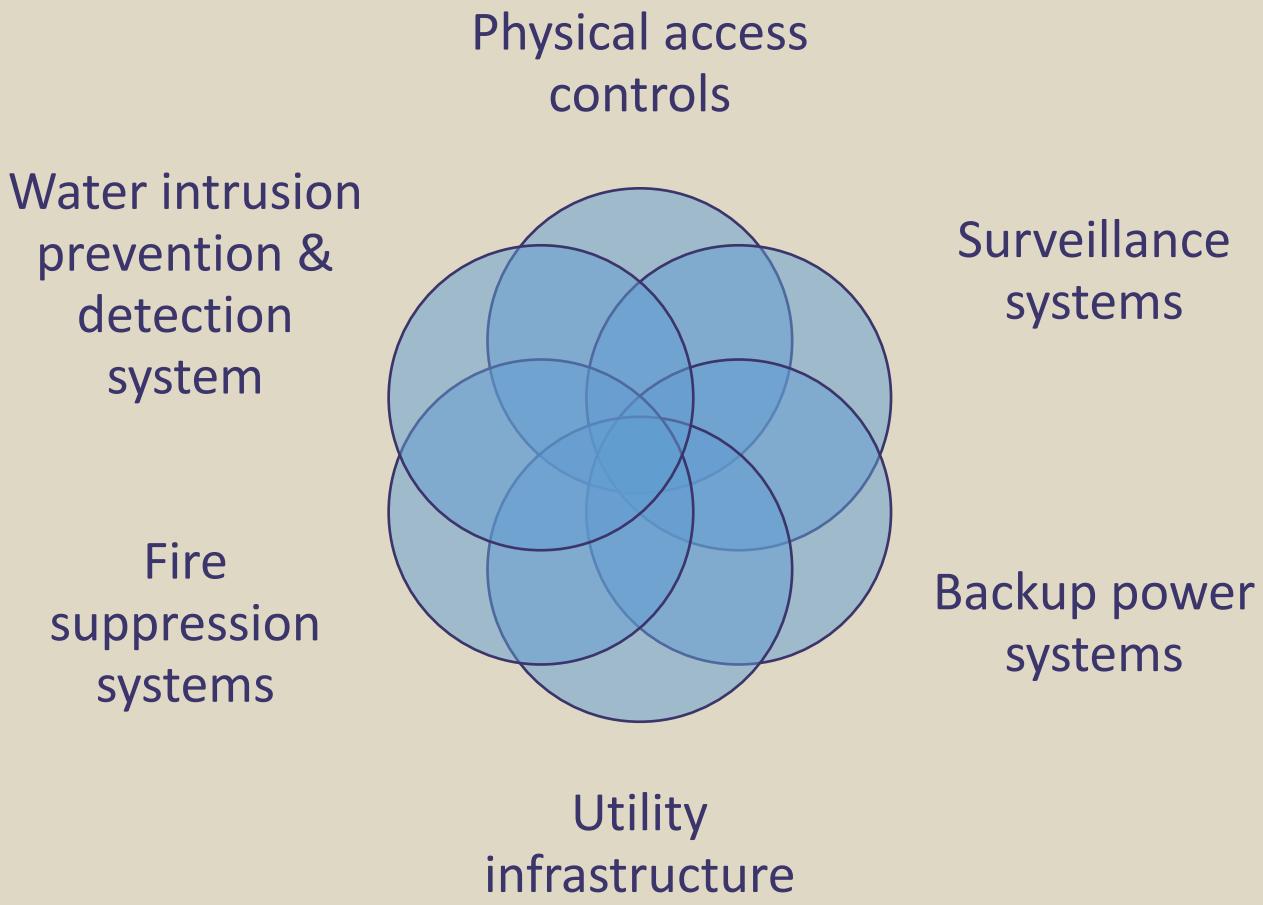
Change Advisory Board

Responsibility for the review and approval of change requests

Should include a diversity of stakeholders include system owners and business owners

Membership should provide management with adequate understanding of, and control over, changes

Physical & Environmental Controls



Disaster Recovery & Business Continuity

Business continuity plan (BCP):

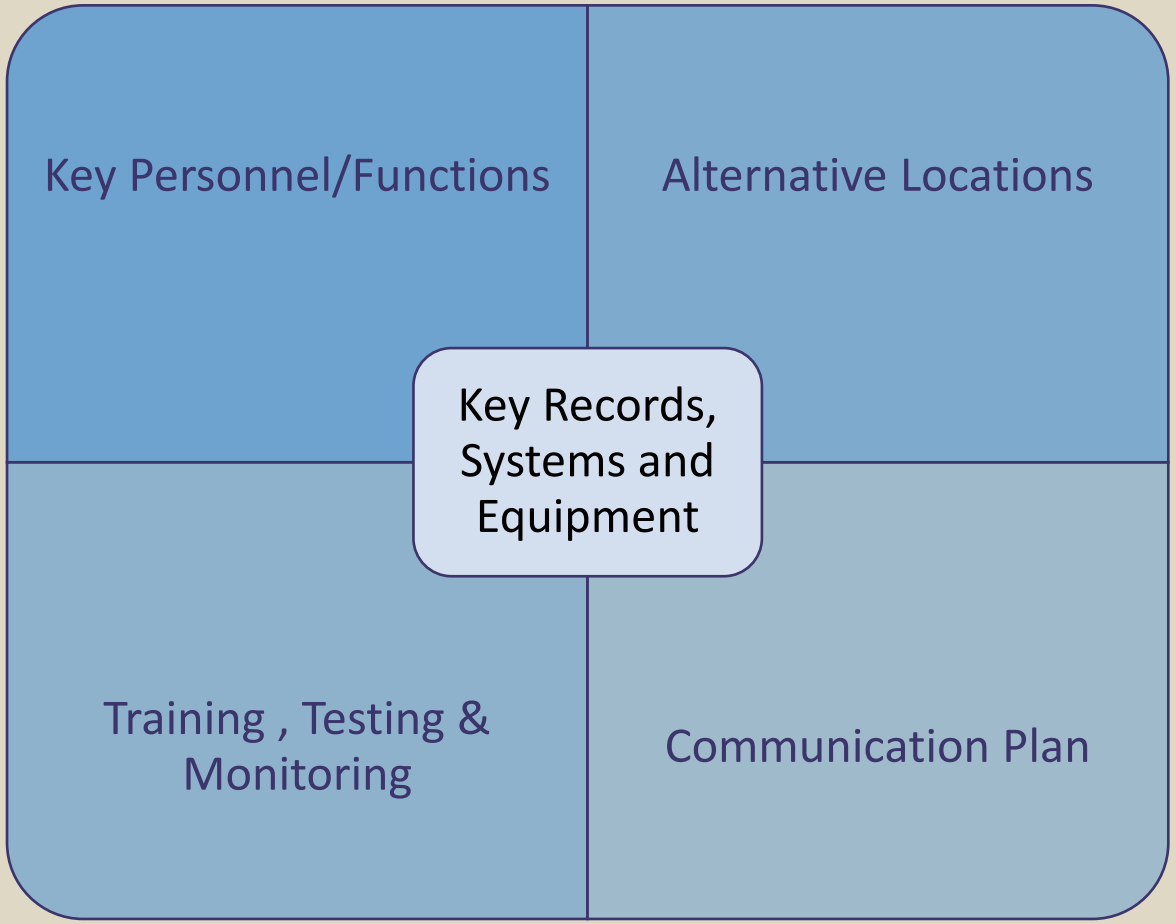
- Focus on keeping business operational or limiting down time
  - Manual Operations
  - Alternative Locations
  - Critical Operations only

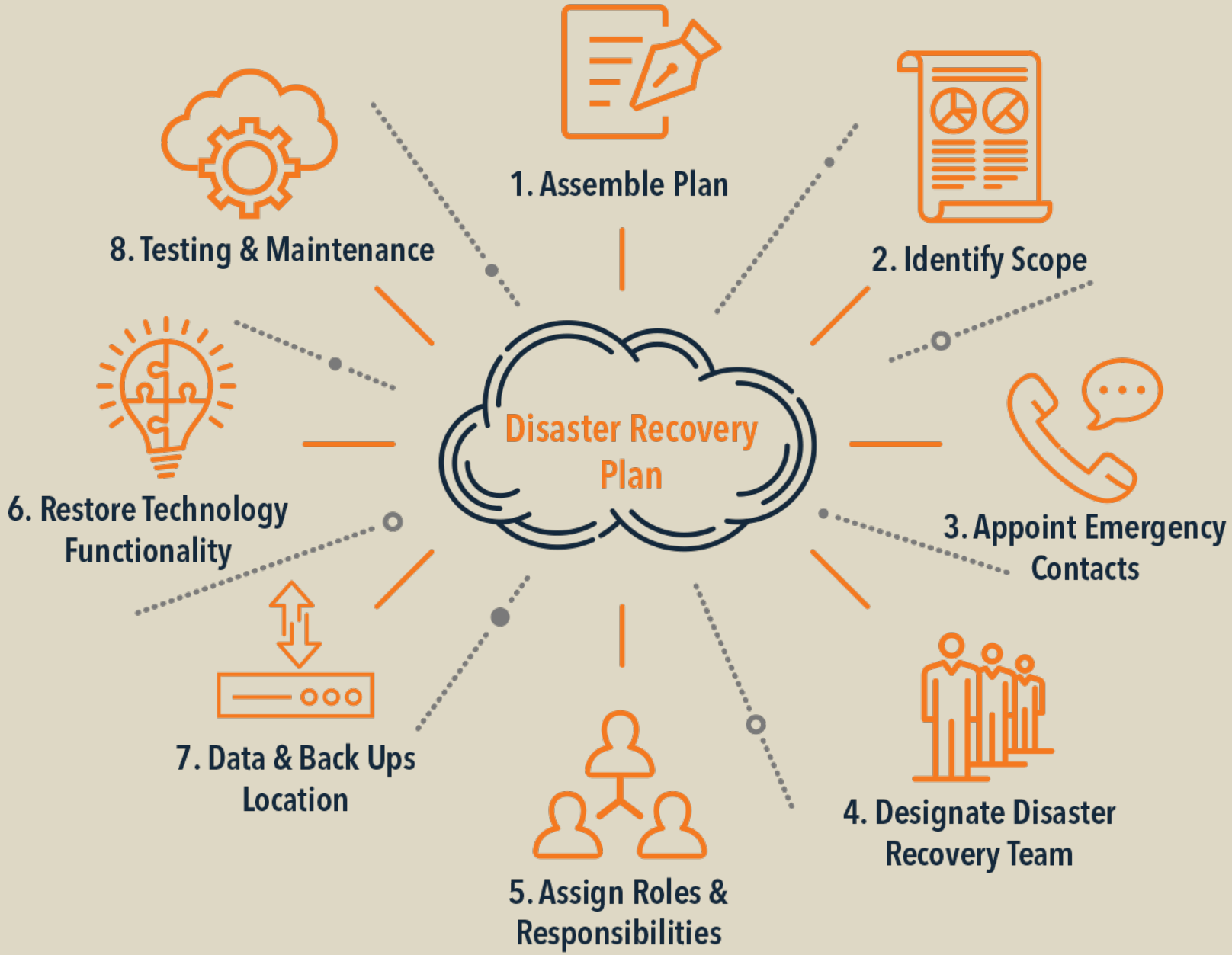
Disaster Recovery Plan

- Focus on restoring data, access to data, and IT infrastructure to normal
- Goal is to limit abnormal or inefficient system functions

Key Business Continuity Plan Steps

- 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 arrangement.
- Conduct post-resumption reviews




Disaster Recovery Plan
1. Assemble Plan
2. Identify Scope
3. Appoint Emergency Contacts
4. Designate Disaster Recovery Team
5. Assign Roles & Responsibilities
7. Data & Back Ups Location
6. Restore Technology Functionality
8. Testing & Maintenance

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

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

Impact on Application Risk

The degree of successful risk management is directly dependent upon the effectiveness of GITCs.

- The organization's risk appetite, or tolerance
- The appropriate align of IT Governance with key operational and financial strategies
- Appropriate Allocation of Resources to support the application

Impact on Application Risk

- The effectiveness of identity and access management controls impact the integrity of program and data files.
- The appropriate development and implementation of the application impact application process effectiveness and reduce unintended issues.

Impact on Application Risk

Physical& Environmental Controls

- Impact the availability of the application regardless of whether the institution hosts it.
- P&E controls must be in place at third party providers.

Business Continuity & Disaster Recovery

- Impact the ability to bring back up the application timely.
- Impact the ability to recover data.

Questions?
Comments?

Presented by:
Kate M. Head, Associate Director, USF Office of Internal Audit
Khead@usf.edu 813-974-3737