IT Risk Assessment Methodology

LISA SIEDZIK, CISA, IAP, MBA

Agenda

Introduction

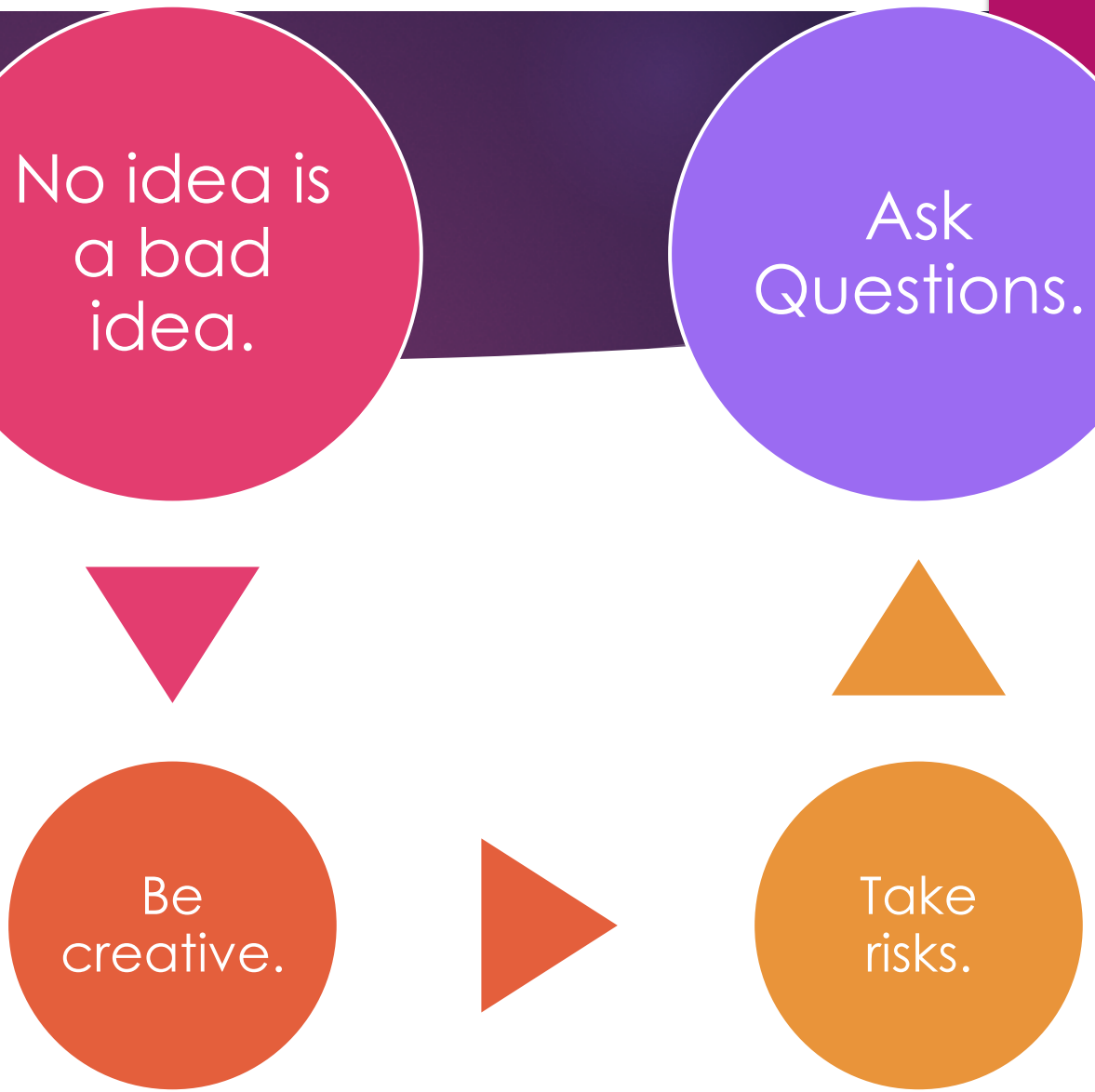
Learning objective

Questions, activities, cases studies – oh my!

Next steps

How I Got Here

Rules



Learning objective

Why its so important for government

Definitions

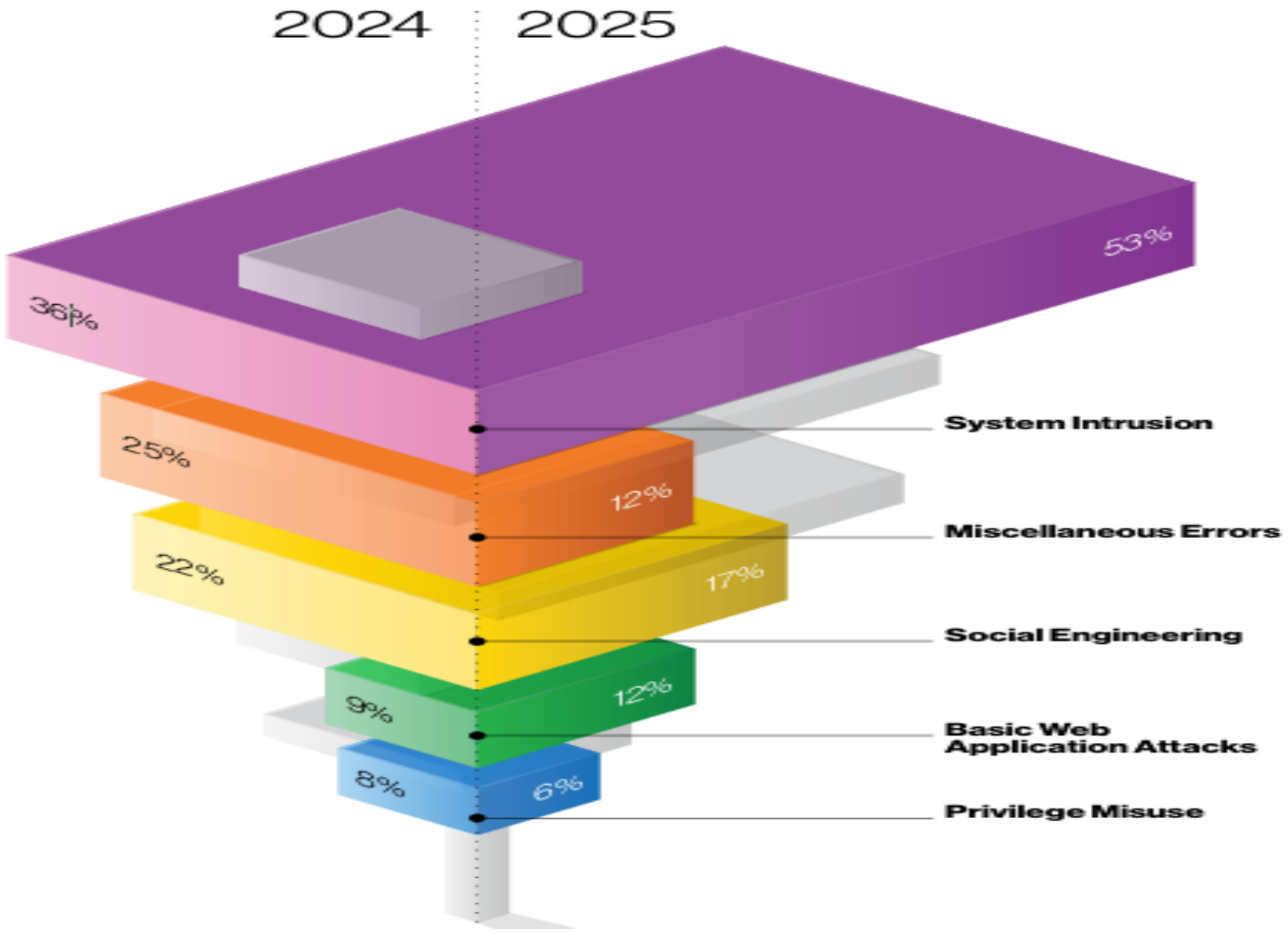
Basic concepts

Process

Why It is So Important to Government

THE RISK IS HIGH AND IT IS COSTLY!

Public Sector Snapshot



Verizon Data Breach Investigations Report, 2025

Types of Cyberattacks on Municipalities

- Phishing
- Malware
- Ransomware
- Data Breaches
- Denial of service (DoS) attacks
- Distributed denial of service (DDoS) attacks

Miliefsky, Gary. "Cyberattacks on City and Municipal Governments". Cyber Defense, August 4, 2023

Examples of recent attacks in cities within the United States

	Where	What	Cause & Effect
June 2023	Dallas, TX	Ransomware	Cause: vulnerability in city's email system Effect: estimated cost of recovery $1 million
June 2023	Lowell, MA	Data breach	Cause: vulnerability in city's website Effect: exposed personal info of over 10,000 residents
June 2023	Nashua, NH	Data breach	Cause: vulnerability in city's payroll system Effect: exposed personal info of over 5,000 employees
June 2023	San Jose, CA	Ransomware	Cause: vulnerability in city's network Effect: estimated cost of recovery $10 million
June 2023	Austin, TX	Data breach	Cause: vulnerability in city's website Effect: exposed personal info of over 20,000 residents
June 2023	Cincinnati, OH	Ransomware	Cause: vulnerability in city's email system Effect: estimated cost of recovery $5 million

Impact of city attacks for 2023

All resulting in lost revenue, reduced services and the loss of citizen trust.

- Financial loss and challenge of allocating capital to prevent attacks
- Loss of sensitive data such as employee and resident data, financial data and intellectual property
- Disruption of critical services and critical infrastructure such as water and power systems
- Inability to provide services to residents

Reasons

- Sophistication of hackers.
- Increasing use of cloud computing.
- More tech, more risk.
- Lack of funding.
- Common weak spots. Services that are not properly secured such as use of public internet for file sharing and remote desktop access.
- Known vulnerabilities. Outdated software with security issues – no patching.

Definitions

Key Definitions

Phishing – attacker sends an email or text message that appears to be from a legitimate source. The email or text contains a link or attachment that, when clicked, downloads malware onto the device.

Malware – type of software designed to damage or disable a system. It can be spread through phishing, email attachments, and infected websites.

Ransomware – encrypts files and demands a payment to decrypt them.

Data breaches – theft of sensitive data, such as personal information or financial data. Caused from hacking, phishing and malware.

Denial of Service (DOS) – designed to make a computer system or website unavailable to the user. Typically carried out by flooding the system with requests or by attacking the system's infrastructure.

Distributed Denial of Service (DDOS) – same as DOS above but carried out by multiple computers. These are difficult to defend against.

Basic Concepts

IT RISK ASSESSMENTS – IN A NUTSHELL

Guides and Resources: Risk Assessment

GAO	'Government Audit Standards 2024 Revision'
IIA Global Practice Guide	'Developing a Risk-Based Internal Audit Plan'
IIA Global Practice Guide	'Building an Effective Internal Audit Function in the Public Sector'
IIA GTAG	'Developing the IT Audit Plan'
IIA GTAG	'Management of IT Auditing'
Audit Software or GRC ?	

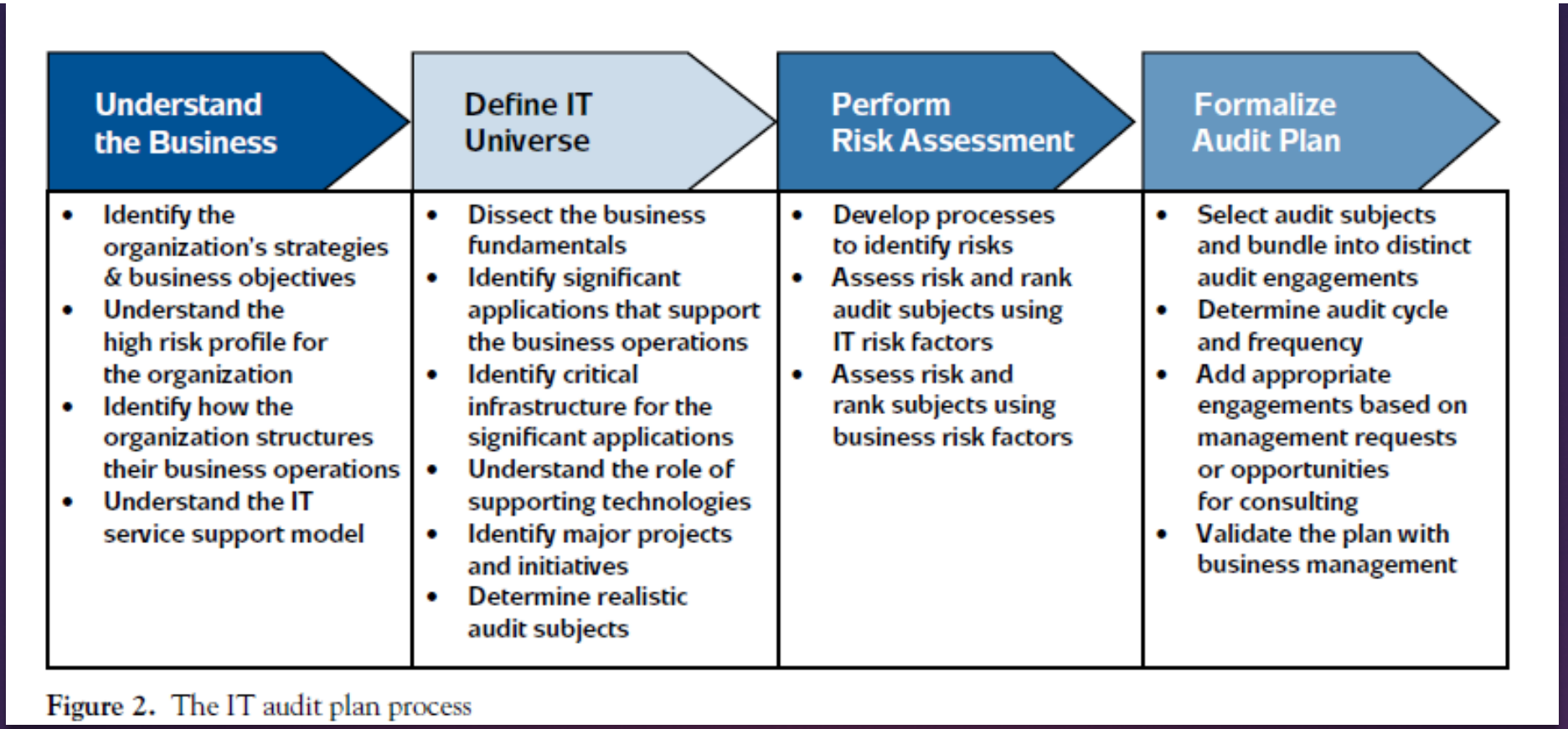


Figure 2. The IT audit plan process

The Overview

STAGE METHODOLOGY

Brainstorming Activity

- How would you approach understanding the business?
  - What would you include?
  - Would you rely on historical information?
  - Would you talk with stakeholders?
  - What is an IT universe? How would you even think to begin?
  - Does the audit division have skill gaps for IT?

Process

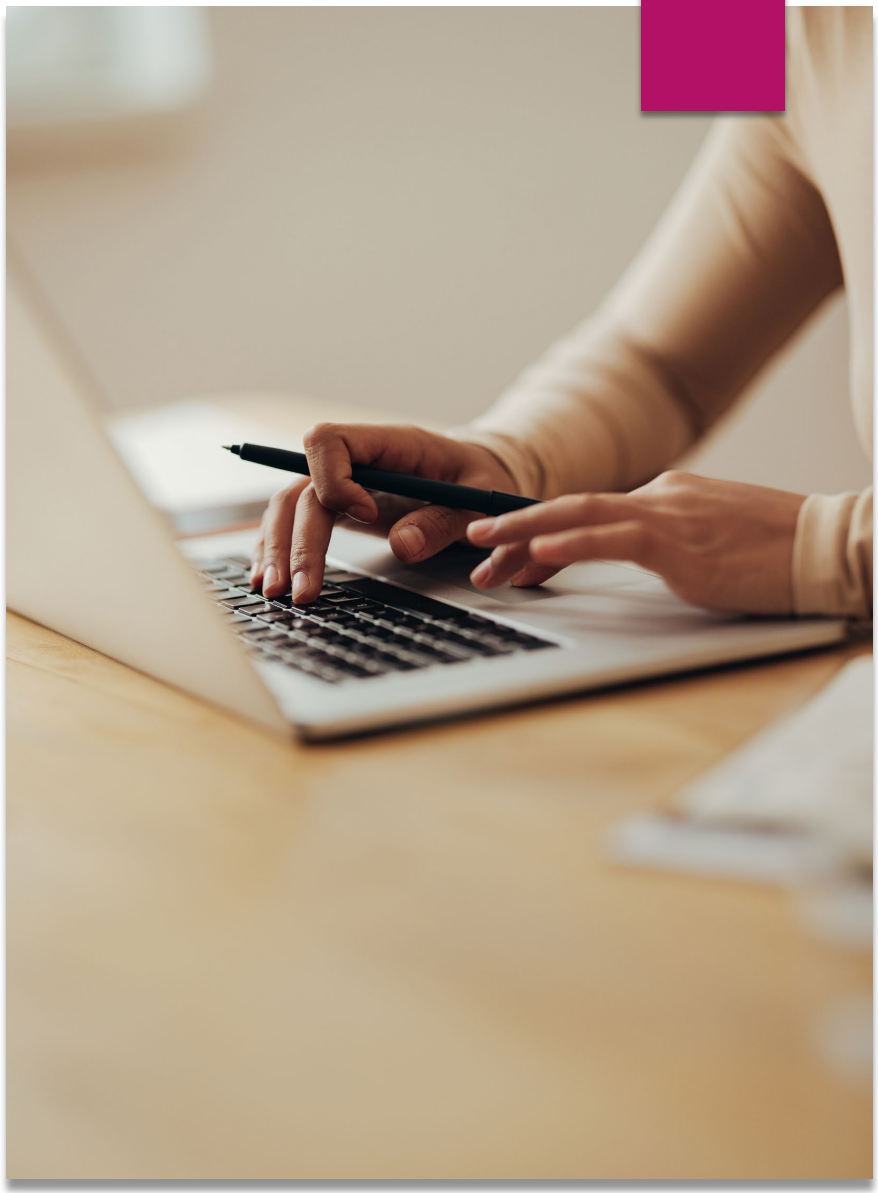
THE NITTY GRITTY

Stage 1: Understand the Business

- Identify the IT System Inventory
- Identify all the IT Processes
- Identify organization strategies and business objectives
- Understand high risk profile of organization
- Identify how organization structures its business operations
- Understand the IT service support model and environment

Sample – Our Stage 1 Approach

- Timeline
- IT provider questionnaire
- Department questionnaire
- Obtained IT service provider's mission statement, strategy, etc.



Case Study – Exercise 1

Case Study Check

- **ERP System Integration and Efficiency:** Concerns around the effectiveness and integration of the ERP system across business processes including production, HR, and finance.
- **CRM System Effectiveness:** Challenges in the operational effectiveness of CRM system's capabilities in managing customer interactions, data accuracy, and its contribution to sales strategies.
- **R&D Systems and Innovation Management:** Inefficiencies in the systems supporting R&D for their effectiveness in fostering innovation, managing prototypes, and integrating with other business units.
- **Manufacturing Execution System (MES) Compliance and Performance:** Instances of non-compliance with industry standards and inefficiencies In production processes for MES.
- **Cloud Computing and Data Storage Security:** Issues noted with cloud services for data security, compliance with data protection laws, and efficiency in storage and retrieval processes.
- **Network Infrastructure and Security:** Assess the robustness, security, and efficiency of the company's LAN and WAN, including vulnerability to cyberthreats.
- **Cybersecurity Measures and Protocols:** Evaluate the effectiveness of cybersecurity measures including firewalls and intrusion detection systems, and adherence to security protocols.
- **IT Governance and Policy Compliance:** Inspect the IT governance framework for its effectiveness in policy implementation, regulatory compliance and alignment with corporate objectives.
- **Data Analytics and Decision Support Systems:** Audit data analytics processes for their role in strategic decision-making, accuracy of insights, and integration with business functions.
- **Employee IT Training and Awareness Programs:** Review the effectiveness of IT training programs for employees, focusing on awareness and adherence to IT policies and cybersecurity best practices.

Stage 2 - Define the IT Universe

- Catalog hardware, software, applications, data, and third-party vendors.
- Map the IT universe to business processes

Guides and Resources: Frameworks

- Cobit 2019
- NIST Cybersecurity Framework (CSF 2.0) or other
- ISO 27001 and 27002
- IT General Control (ITGC)
- CIS Critical Security Controls
- Secure Controls Framework
- COSO Internal Control – Integrated Framework

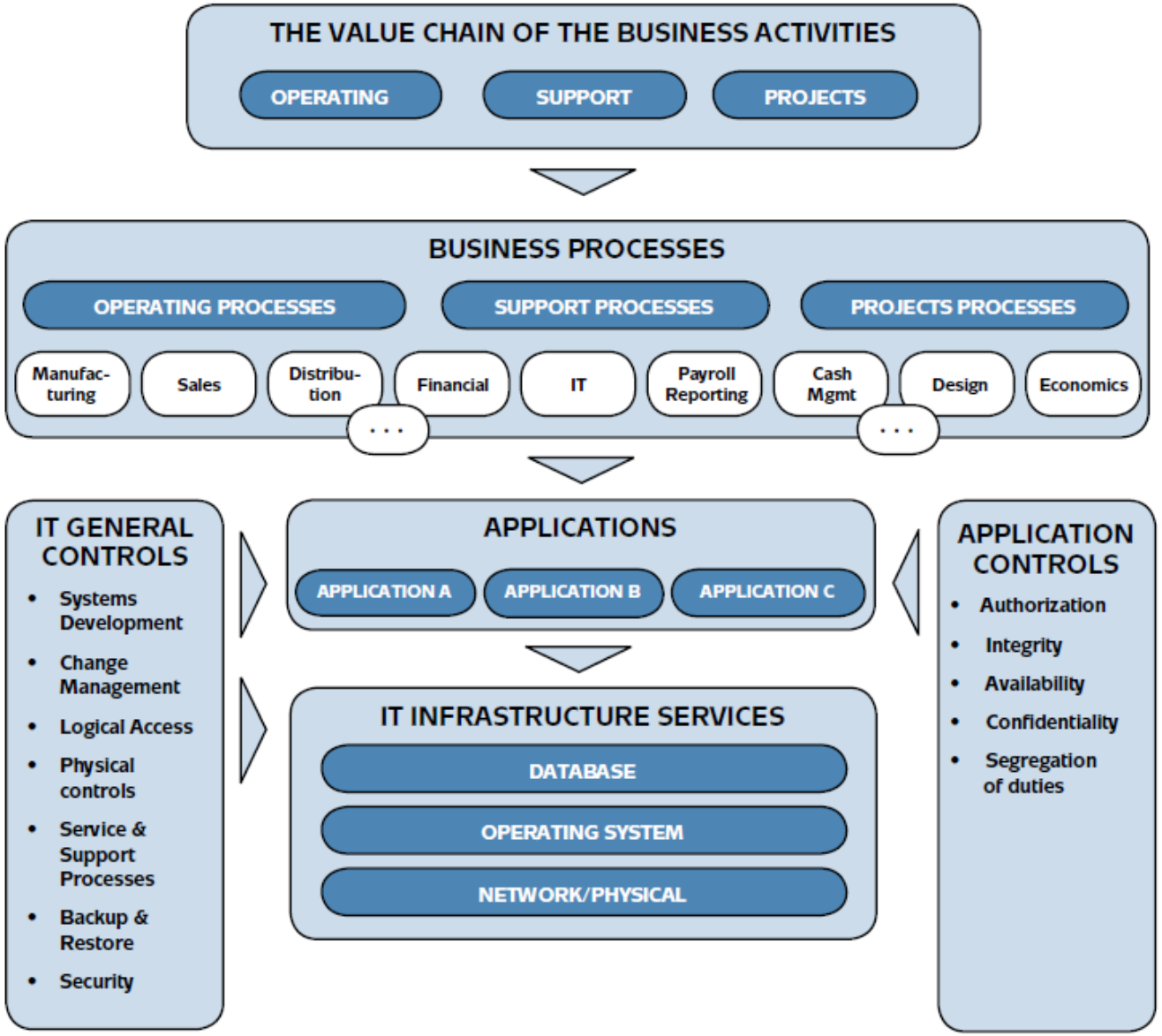


Figure 3. Understanding the IT environment in a business context

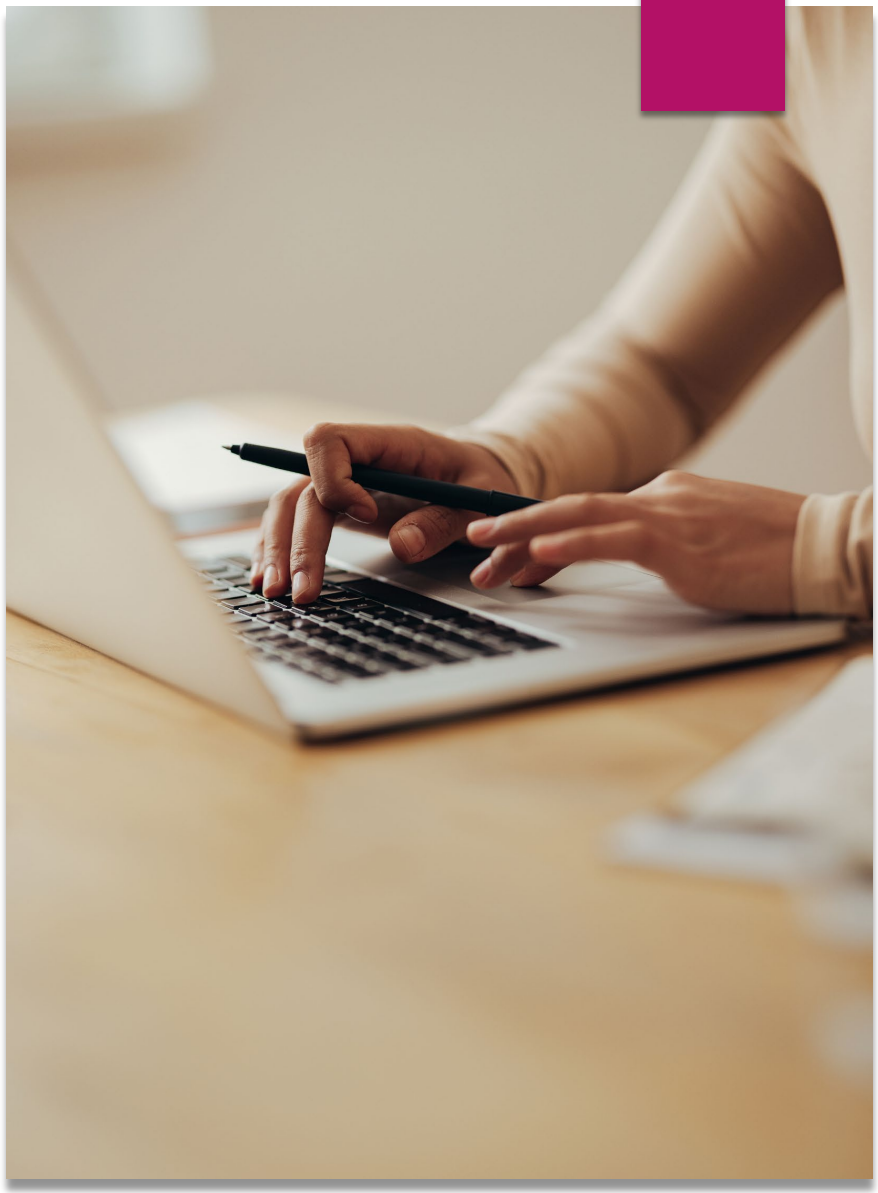
Figure adapted and revised from: *IT Control Objectives for Sarbanes-Oxley*, 2nd Ed., used by permission of the IT Governance Institute (ITGI). ©2006 ITGI. All rights reserved.

Components

- Systems ➔ Enterprise resource planning, databases, cloud platforms, on premise systems, virtual machines, servers
- Processes ➔ Data backup and recovery, change management, user access, cybersecurity, incident response, software development lifecycles
- Departments/Functions ➔ Information security, IT operations, network administrations, IT support
- Locations ➔ Data centers, cloud providers
- Controls ➔ Specific security controls, access controls, regulatory compliance
- Other ➔ Use of USBs, external hard drives, drones, other areas?

Sample – Stage 2 Approach

- Timeline
- Obtained export of all contracts that were categorized as IT (for GG only)
- Requested and obtained all IT policies and procedures, export from all servers that included the applications, databases, systems, any dedicated servers, routers and storage devices, and any relevant data diagrams.
- Reviewed questionnaires and performed interviews
- Using Secure Control Framework, started modifying the template to meet our needs
- Input relevant information



Case Study – Exercise 2

Case Study Check

- Network Administration and Security
- Windows Server Administration and Security
- Server Administration and Security
- Database Administration and Security
- ERP Application and General Controls
- Payroll Application and General Controls
- Major Capital Projects
- Corporate Privacy Compliance
- IT Infrastructure Configuration Management
- IT Governance Practices

Stage 3: Perform the Risk Assessment

Key Important Notes:

- For this to be risk based, the IT universe must be link back to the business objectives and/or support the organization.
- The purpose is to identify those infrastructure, applications, and computer operations or components that could hinder the organization.
- If the risk assessment's methodology input (i.e., the IT universe and its link to the business audit universe) is deficient or is applied incorrectly, it is likely that the output (i.e., risk assessment results) will be incomplete in some capacity.

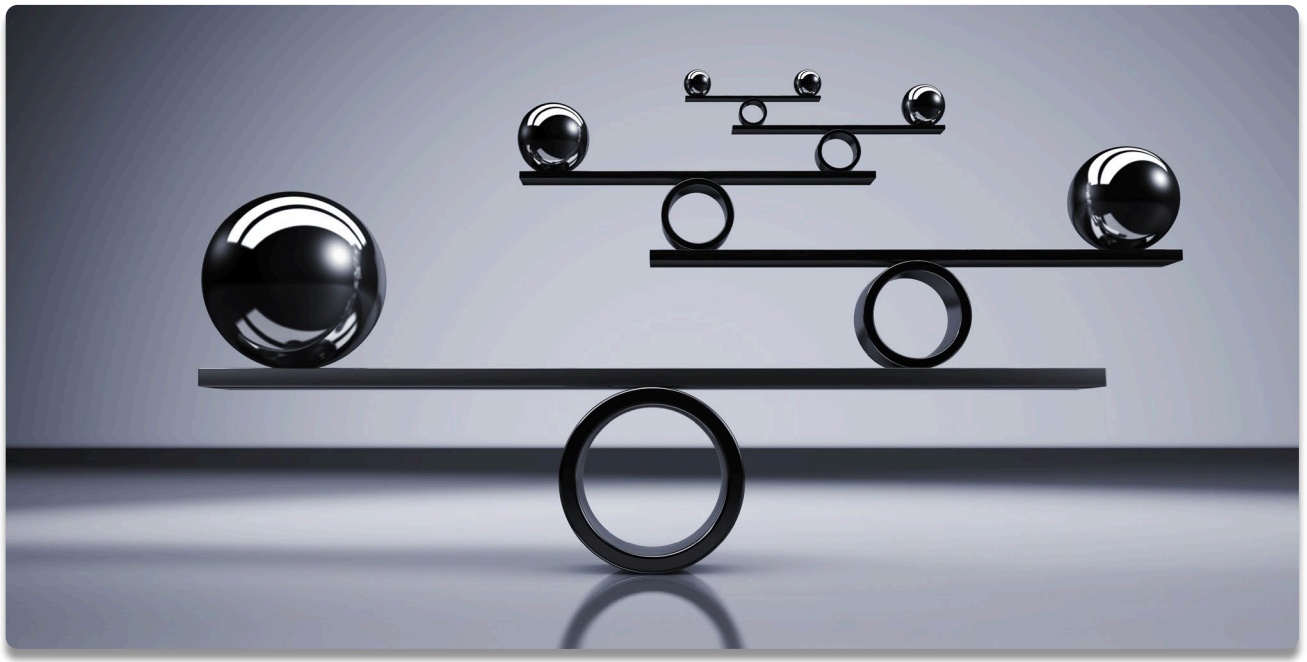
SYSTEM AND DATA AVAILABILITY, RELIABILITY, INTEGRITY AND CONFIDENTIALITY!

Control Assessment

- Purpose: Assess risk and rank audit subjects against IT risk factors based on the framework selected. But also, to assess risk and rank audit subjects against business risk factors.
- Threat & Vulnerability Identification
  - Identify internal and external risks, such as cybersecurity threats, misconfigurations, or data loss.
  - Evaluate existing security policies, firewall configurations, and access controls to identify gaps.
- Likelihood and Impact Analysis to determine severity and rank.

Considerations

- Are you going to risk assess process or applications or both?
- How are you going to organize the data obtained into a usable document?
- Consider categorizing
- What risk factors will you use to aid in identifying threats and vulnerabilities?



Risk Factor Options

Organizational Risk Category	Risk Description
Compliance Risk	Risk of loss due to noncompliance with policies, contracts, agreements, or grants.
Financial Risk	Risk of loss due to inadequate or ineffective controls around tax, accounting, financial reporting, capital and debt management, investments, and other financial processes.
Information Technology Risk	Risk of financial loss and service failure around privacy and confidentiality, security, cybersecurity, cloud computing, mobile device security and IoT, business continuity and disaster recovery, software asset management, user access management, data governance, and remote workplace processes and systems. **NOW AI for both the organization and third parties!**
Legal and Regulatory Risk	Risk of noncompliance with local, state or federal laws and regulations.
Operational Risk	Risk of loss due to ineffective or inefficient operations or services, or failed policies or systems that disrupt operations.
Public Safety Risk	Risk that communication policies, safety standards, physical security, emergency response training, routine security, and other related process and systems controls are not adequate to sufficiently mitigate safety risk for the public or employees.
Reputation Risk	Risk of decreased quality of services, community engagement, and trust, due to negative word of mouth or other neighbor communications.
Strategic Risk	Risk that the City's strategic priorities are not achieved. *Management goals and objectives should align with the City's strategic priorities.*
Third Party Risk	Risk of financial loss, inability to provide services, data breach, noncompliance with contract terms, or other failure related to third party agreements.

Ranking Methods

Three Methods

Oldest – only used by insurance

- **Direct probability estimates and expected loss functions or the application of probabilities to asset values to determine exposure for loss.**
- **Risk factors or the use of observable or measurable factors to measure a specific risk or class of risks.**
- **Weighted or sorted matrices or the use of threats versus component matrices to evaluate consequences and controls.**

Best if used for homogenous areas (i.e. plant audit

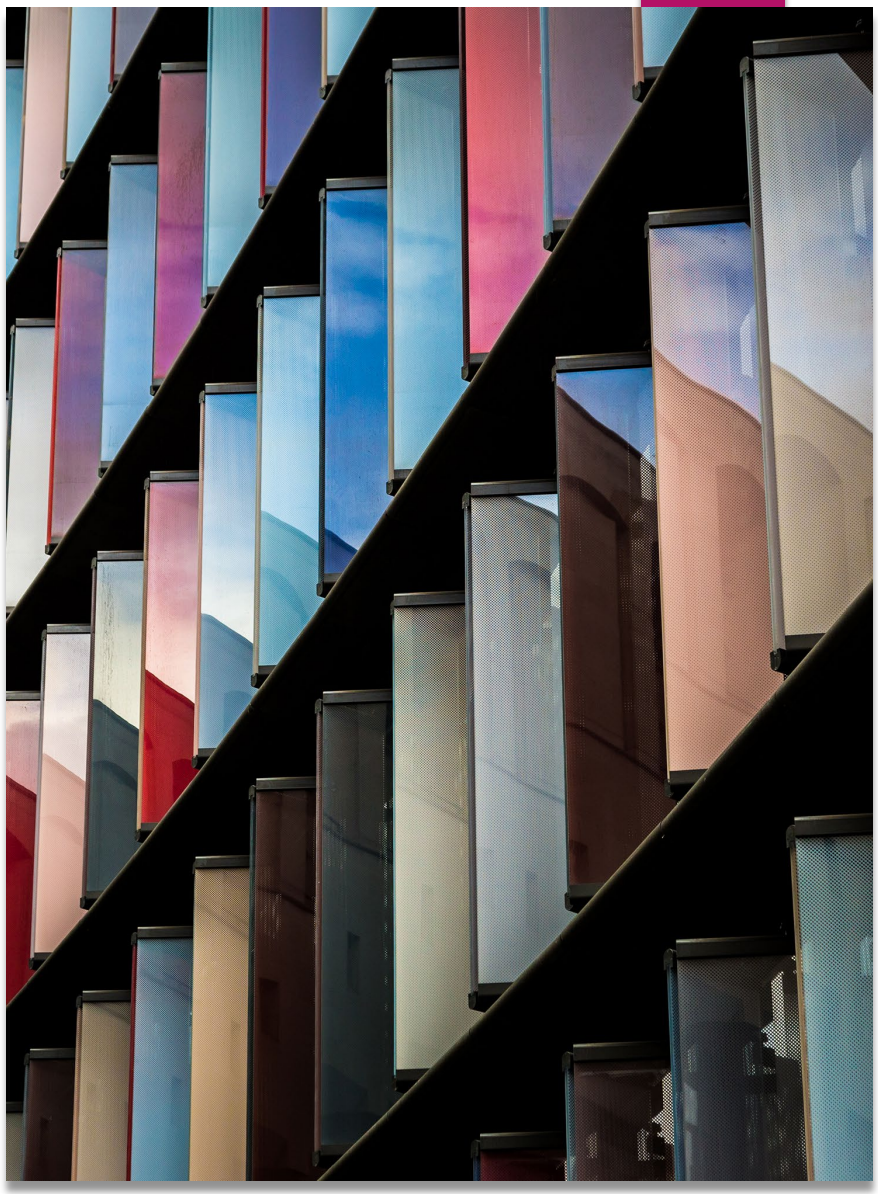
Weighted or Sorted Matrices

Likelihood Scale		
H	3	High probability that the risk will occur.
M	2	Medium probability that the risk will occur.
L	1	Low probability that the risk will occur.

Impact Scale (Financial)		
H	3	The potential for material impact on the organization's earnings, assets, reputation, or stakeholders is high.
M	2	The potential for material impact on the organization's earnings, assets, reputation, or stakeholders may be significant to the audit unit, but moderate in terms of the total organization.
L	1	The potential impact on the organization is minor in size or limited in scope.

Sample – Stage 3 Approach

- Timeline
- Performed two assessments:
  - Business process/domain for the IT service provider
  - Applications, systems, databases, cloud for reported areas
- Developed a formula to calculate overall risk



Case Study – Exercise 3

Case Study Check

- In terms of the risk assessment, the 10 entities identified in the IT Audit universe can be ranked on likelihood and impact along the following five dimensions:
  - Financial statement impact
  - Quality of existing internal controls
  - Confidentiality measures are designed to prevent sensitive information (Confidentiality)
  - The consistency, accuracy, and trustworthiness of data (Integrity)
  - Information should be consistently and readily accessible for authorized parties (Availability)

- Risk Assessment Evaluation

Windows Adm & Security	3	3	3	2	3	2	3	3	2	3	36 (H)
OS400 Adm & Security	2	3	3	2	3	3	3	2	2	3	33 (M)
Oracle Adm & Security	3	2	3	1	3	2	3	2	3	3	30 (M)
SAP ERP Application	3	3	2	2	3	3	2	3	3	2	34 (M)
Payroll Application	2	2	3	3	3	3	2	2	3	3	35 (H)
Major Capital Projects	3	3	1	2	1	1	2	3	3	2	24 (L)
Privacy Compliance	2	2	3	3	3	1	1	3	2	3	25 (L)

- Prioritized IT audit universe domains/business areas

Area	Score
IT Infrastructure Configuration Management	37 (H)
Network Administration and Security	36 (H)
Windows Server Administration and Security	36 (H)
Payroll Application and General Controls	35 (H)
SAP ERP Application and General Controls	34 (M)
OS400 Server Administration and Security	33 (M)
Oracle Database Administration and Security	30 (M)
Corporate Privacy Compliance	25 (L)
Major Capital Projects	24 (L)
IT Governance Practices	24 (L)

Stage 4: Formalize the Audit Plan

- Tomorrow, tomorrow, tomorrow

Area	Score	Risk Level	Timeline	Audit Days Allocated
IT Infrastructure Configuration Management	37	High	Q1	175
Network Administration and Security	36	High	Q1	150
Windows Server Administration and Security	36	High	Q2	150
Payroll Application and General Controls	35	High	Q3	120
SAP ERP Application and General Controls	34	Medium	Q2	100
OS400 Server Administration and Security	33	Medium	Q2	90 (Outsourced)
Oracle Database Administration and Security	30	Medium	Q4	85 (Outsourced)
Corporate Privacy Compliance	25	Low	Q2	60 (Outsourced)
Major Capital Projects	24	Low	Q2	60
IT Governance Practices	24	Low	Q4	60
Internal Controls Testing & Reporting	N/A	N/A	Q3, Q4	100
Follow-up on Findings	N/A	N/A	Q3, Q4	85

A step further…

Summarize

- Gather all relevant information from the organization using sources such as questionnaires, interviews and historical information.
- Determine the framework the organization follows and if none, select one that best fits your organization.
- Systematic approach when looking at domains/business processes and systems. Consider categorizing to aid in easier evaluation.
- Take small steps – its daunting. Set up a timeline to reasonably get the risk assessment done.
- Develop good working relationships with all who participate. Sometimes you may glean more than you expect!

Questions? Thank You.

Lisa Siedzik

https://www.gainesvillefl.gov/Government-Pages/Government/City-Auditor

Phone
352-393-8875

Email
siedzikl1@gainesvillefl.gov

Linked In: Lisa Siedzik