

# IT Audit Universe

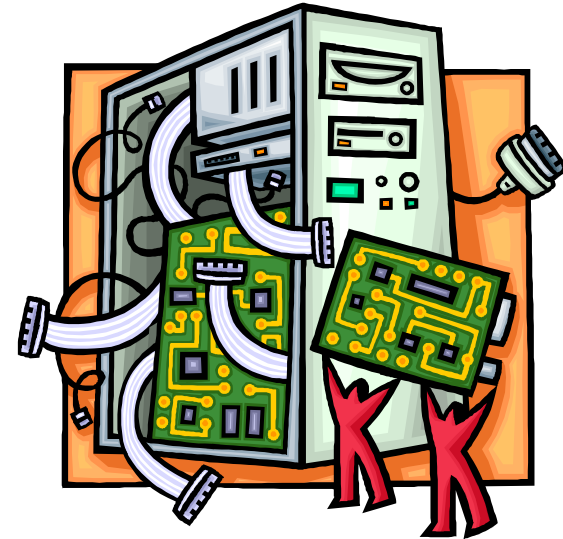
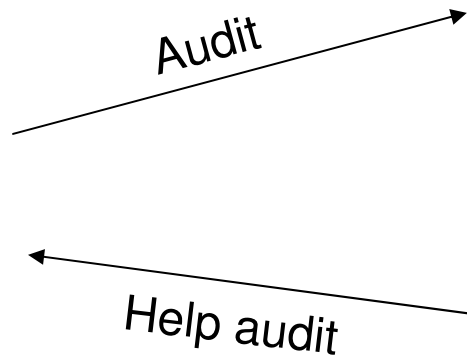
Lily Bi

Director, Technology Practices

- ◆ To provide a quick overview of IT
- ◆ To explore the relationship between IT and Business
- ◆ To define IT audit universe
- ◆ To develop IT audit plan from the IT audit universe
  - Risk assessment
  - Formalize audit plan
- ◆ To provide an example of developing an IT audit plan

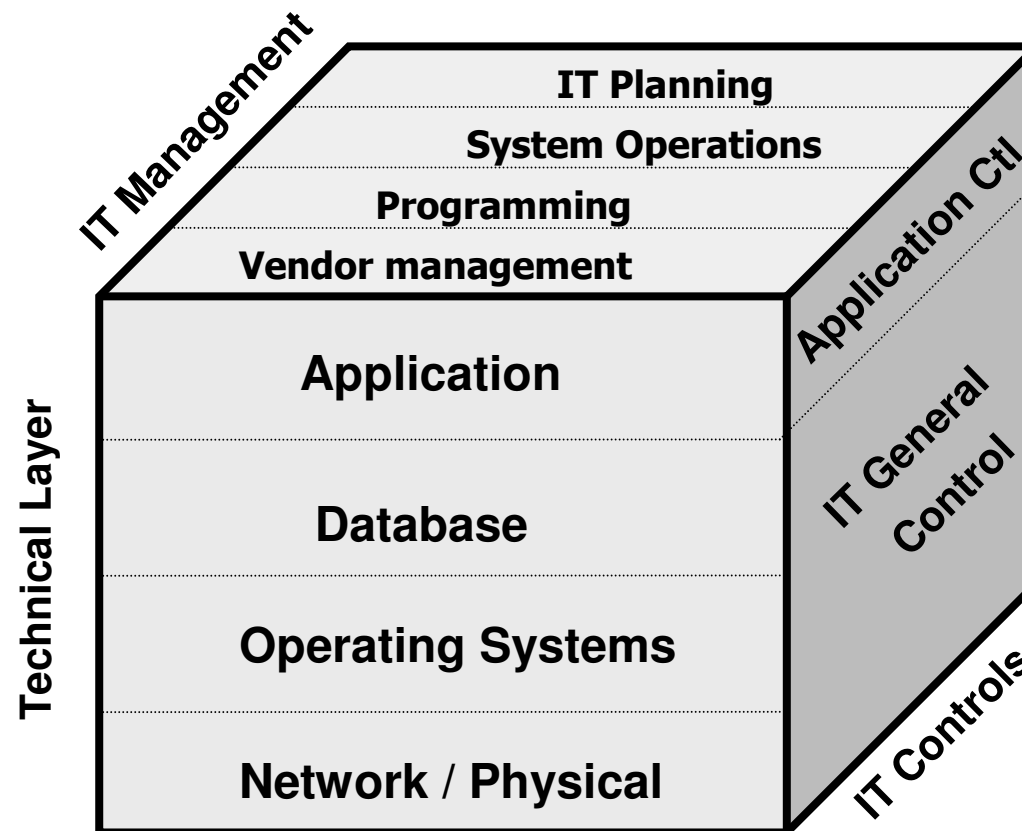
**To you – the internal auditor, what is IT?**

- ◆ To internal auditors, IT is two things
  - A domain subject to audit
  - A tool to help audit



## ◆ IT Domain – 3 Dimensions

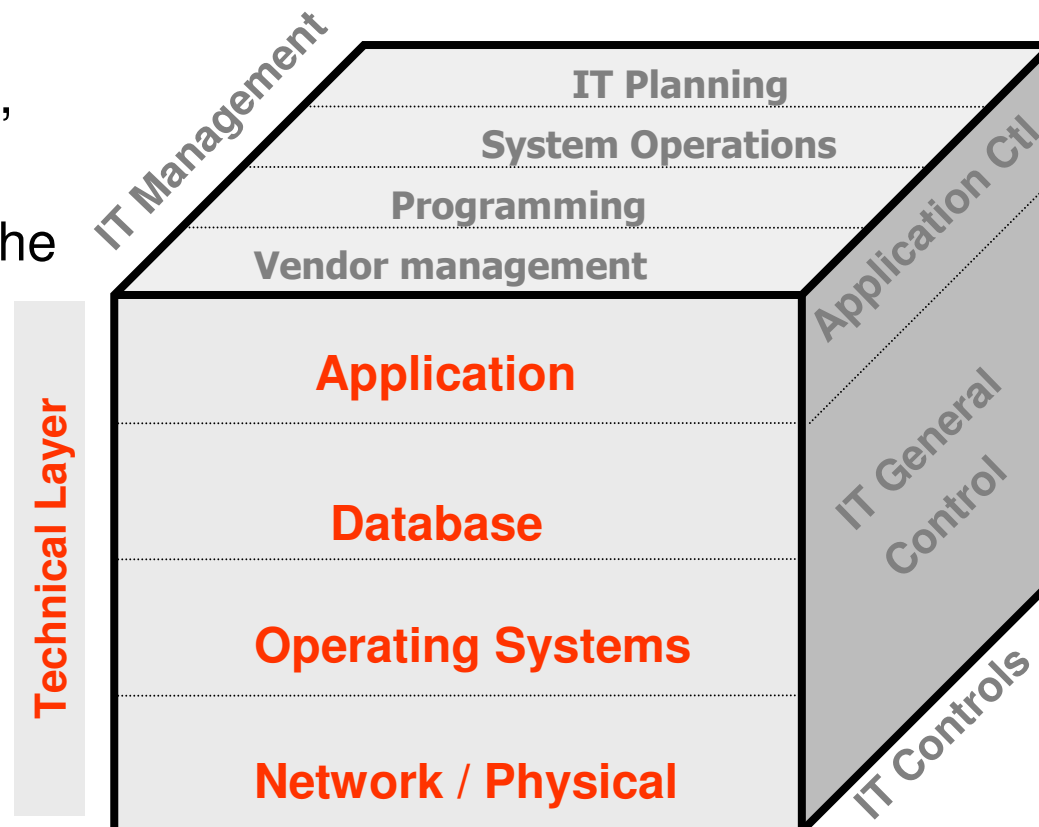
- Technical layer
- IT management
- IT controls



## Layer 1 - Technical Layer

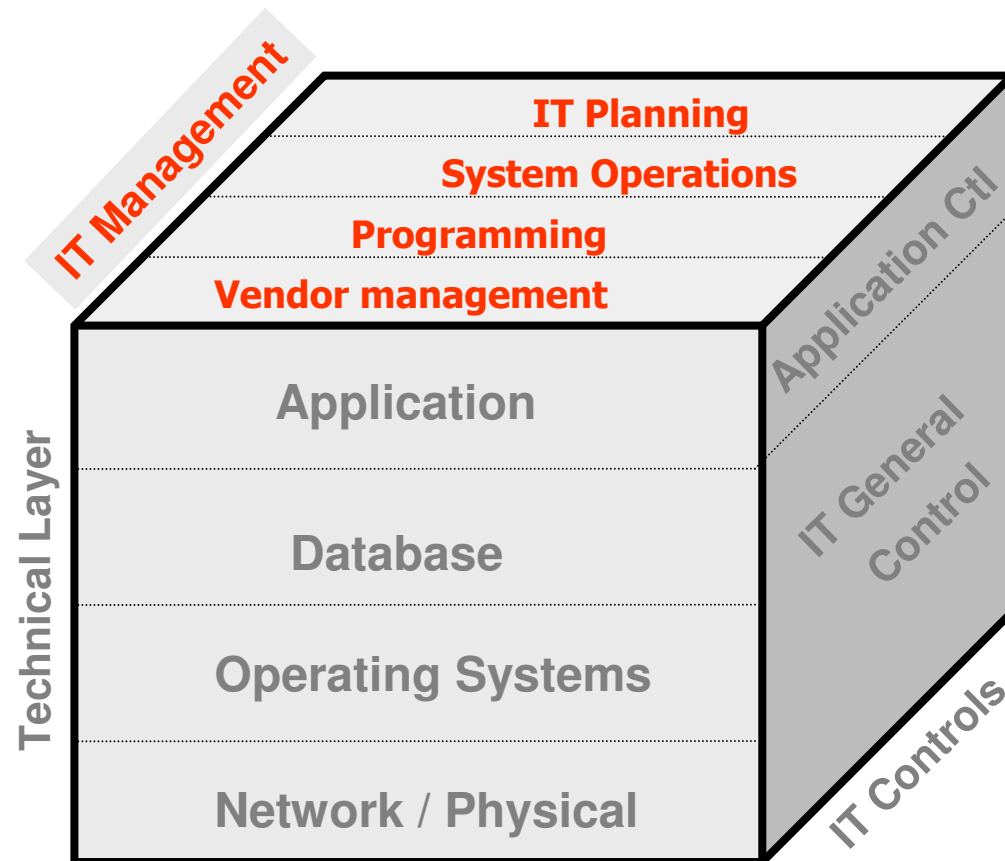
◆ Includes business applications, and the IT infrastructures that underlie, support, and enable the applications.

- Application systems
- Databases
- Operating systems
- Networks



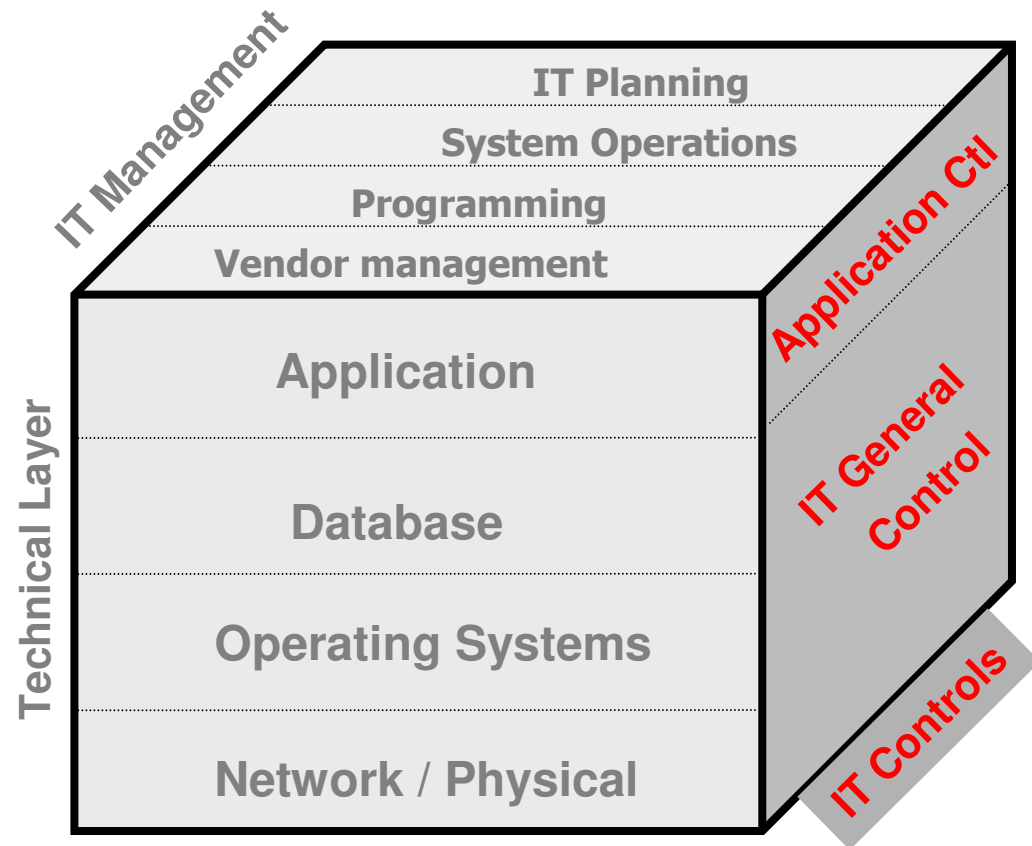
## Layer 2 - IT Management

- ◆ Comprises the set of people, policies, procedures and processes that manage the IT environment.
  - Planning
  - System operations
  - Programming
  - Vendor management



## ◆ Layer 3 – IT Controls

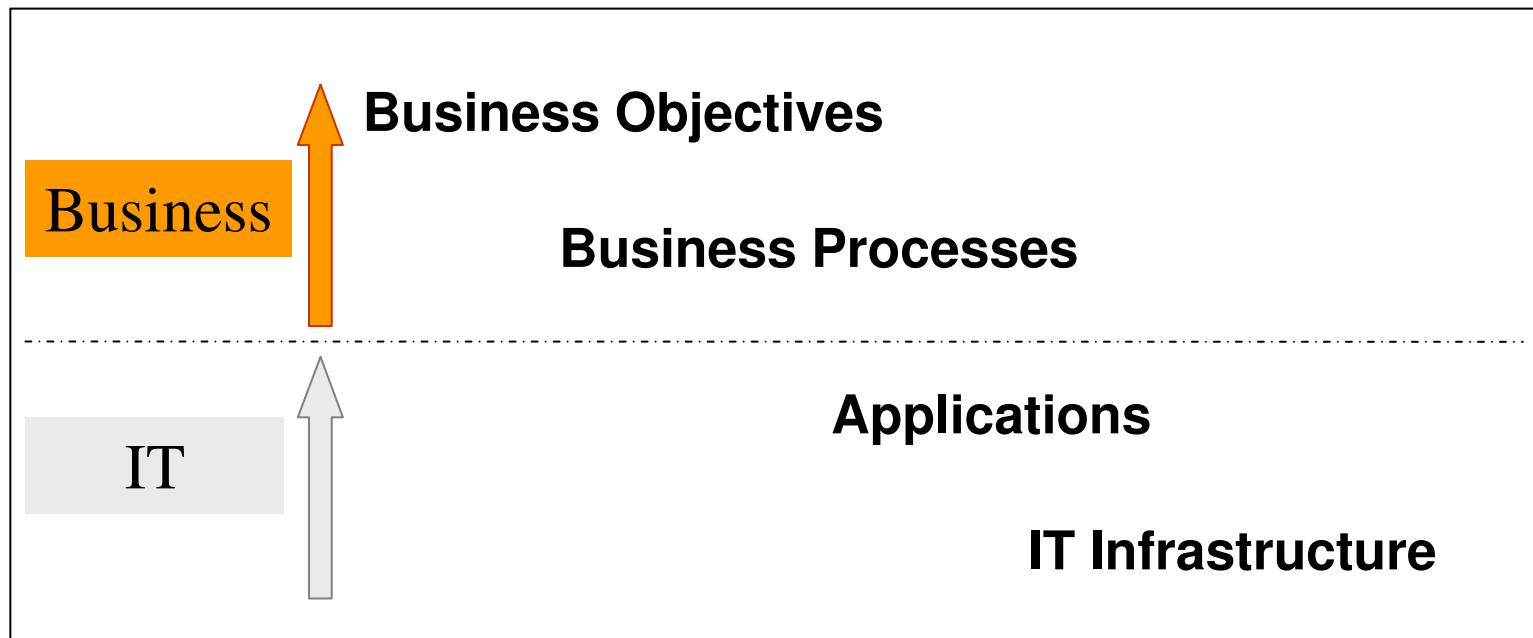
- IT General Controls
  - Systems development
  - Change management
  - Data center security
  - Backup & restore
  - ...
- Application Controls
  - Authorization
  - Data integrity check
  - Segregation of duties
  - ...

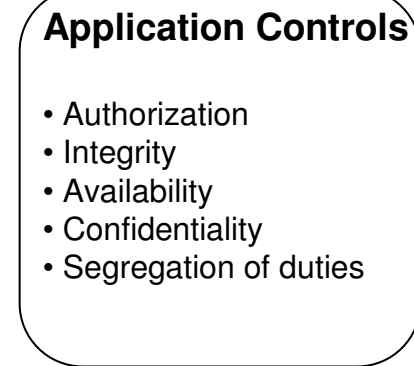
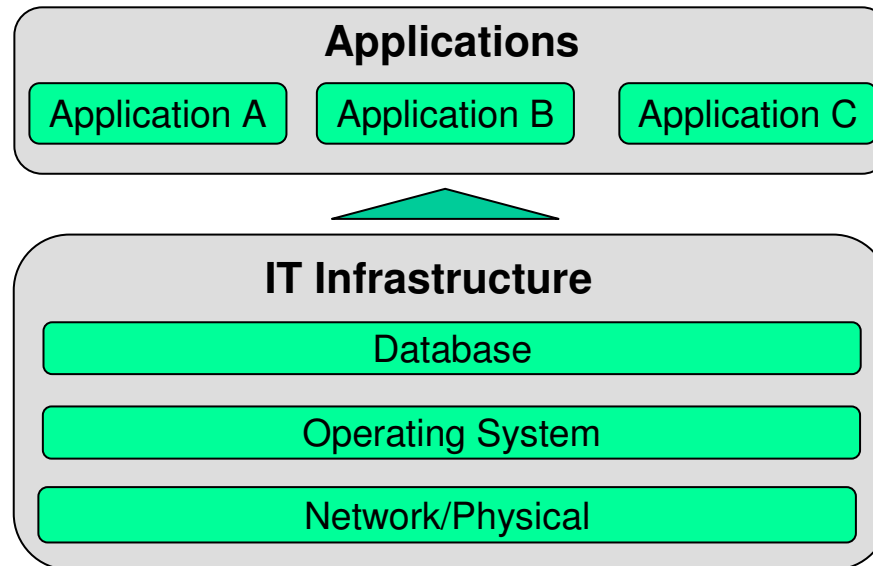
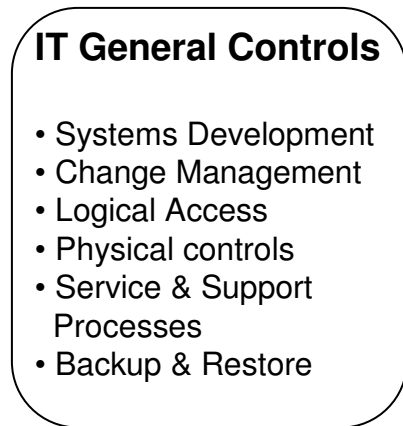
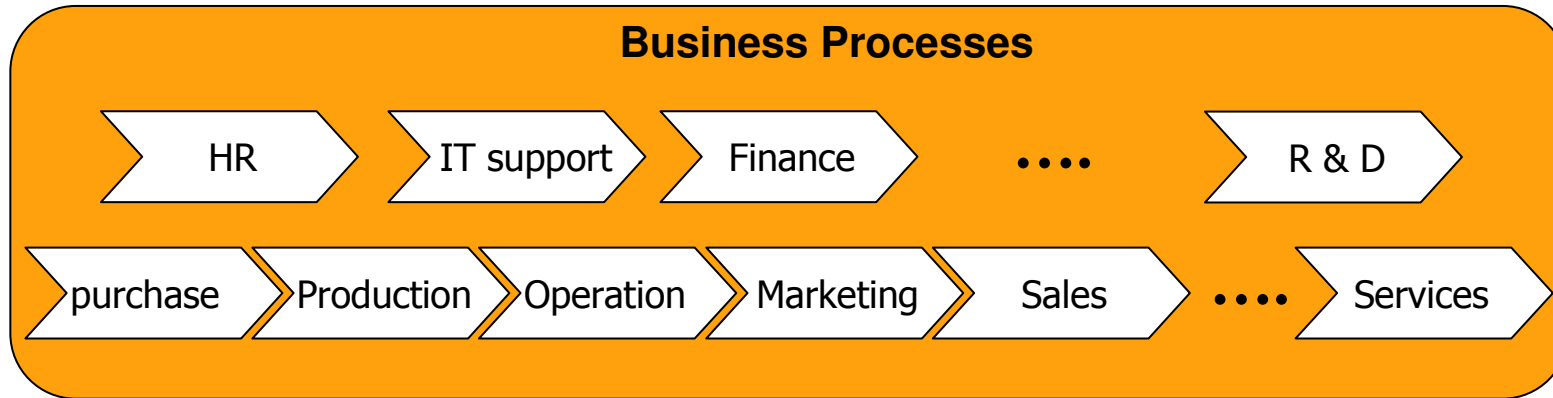


- ◆ IT audit universe -  
A collection of IT areas subject to audit.

**To define the IT audit universe, where to start:  
business, IT, or IT control framework?**

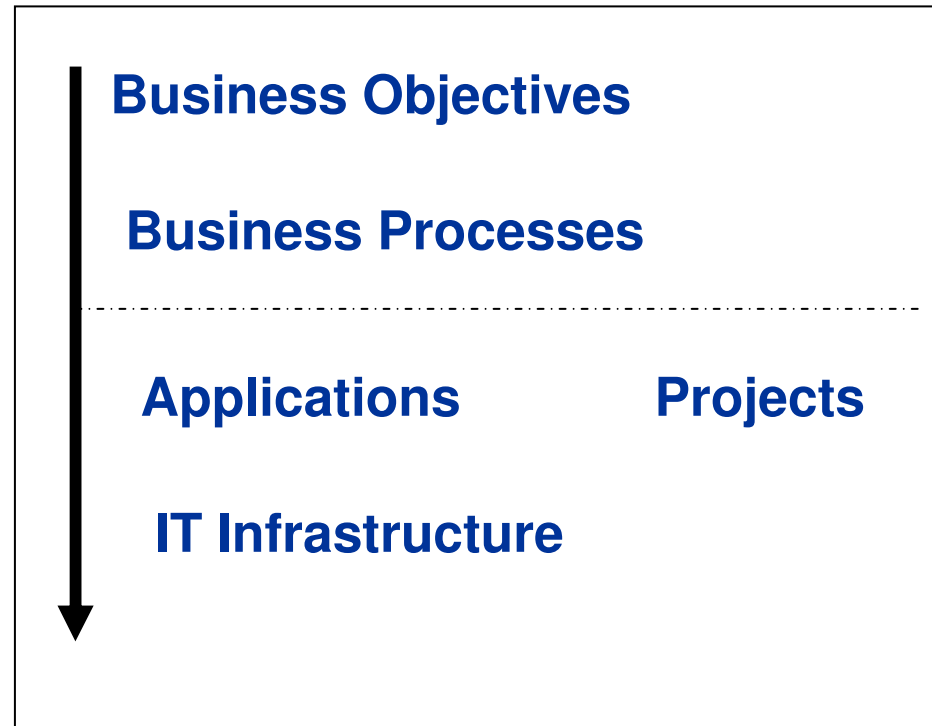
- ◆ **IT only exists to support and further business objectives.**





- ◆ Identify the organization's strategy and business objectives
- ◆ Identify how organization structures its business operations
- ◆ Understand the high risk profile for the organization
- ◆ Understand the regulation and compliance requirements
- ◆ Understand the IT support model
  - The degree of system and geographic centralization
  - The degree of outsourcing
  - The degree of customization
  - The degree of reliance on technology

- ◆ Dissect the business fundamentals
- ◆ Identify key business areas
- ◆ Identify application systems that support the above business areas
- ◆ Identify critical infrastructure that supports the above applications
- ◆ Identify major projects and initiatives
- ◆ Determine realistic audit subjects

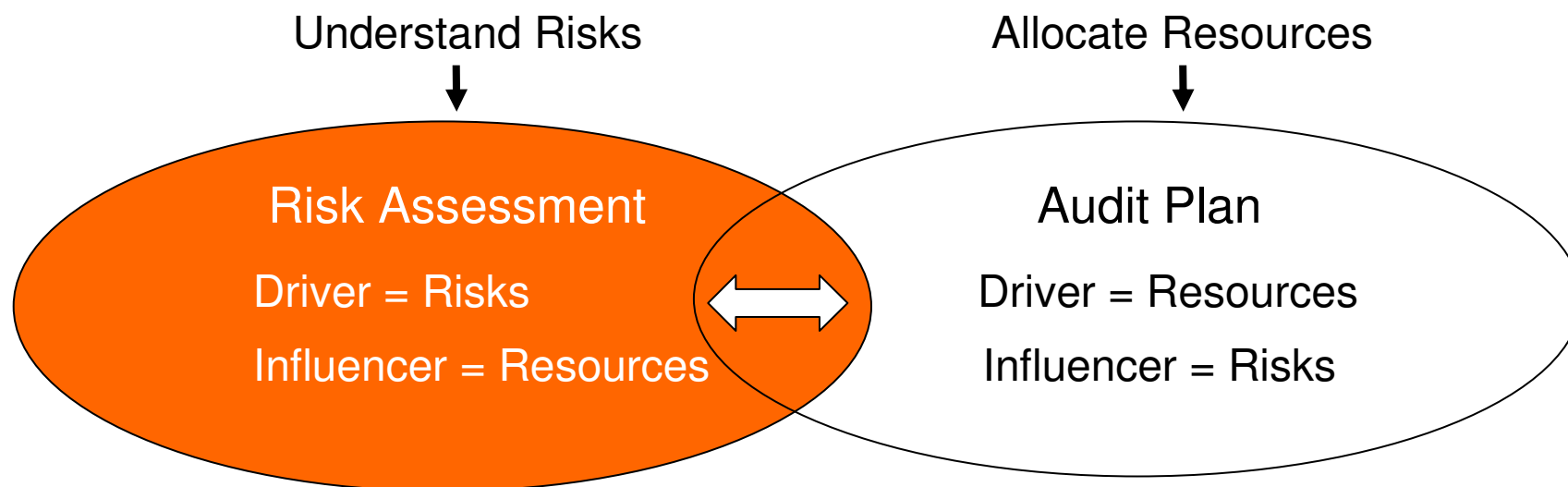


- ◆ Defining the IT audit universe should consider elements under all three IT layers
  - Technical layer - applications, IT infrastructure
  - IT managements
  - IT controls - general controls and application controls

**Now we have defined the IT audit universe.  
We may not have enough resources to audit all subjects in it.  
What to do next?**

- ◆ The IIA Standard 2010 Planning - The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.
- ◆ There is no such thing as "IT Risk." Examples of risks are
  - Strategic
  - Financial
  - Reputation
  - Legal and Regulatory
  - Operational
- ◆ Many risk ranking approaches. The IIA's IPPF glossary says - Risk is measured in terms of impact and likelihood.
- ◆ Prioritize audit subjects based on the risk ranking

## ◆ Objectives of risk assessment and audit plan



### Key Activities:

- Obtain Explicit Input from Stakeholders
- Identify Relevant Risks
- Assess Risks
- Prioritize Risks

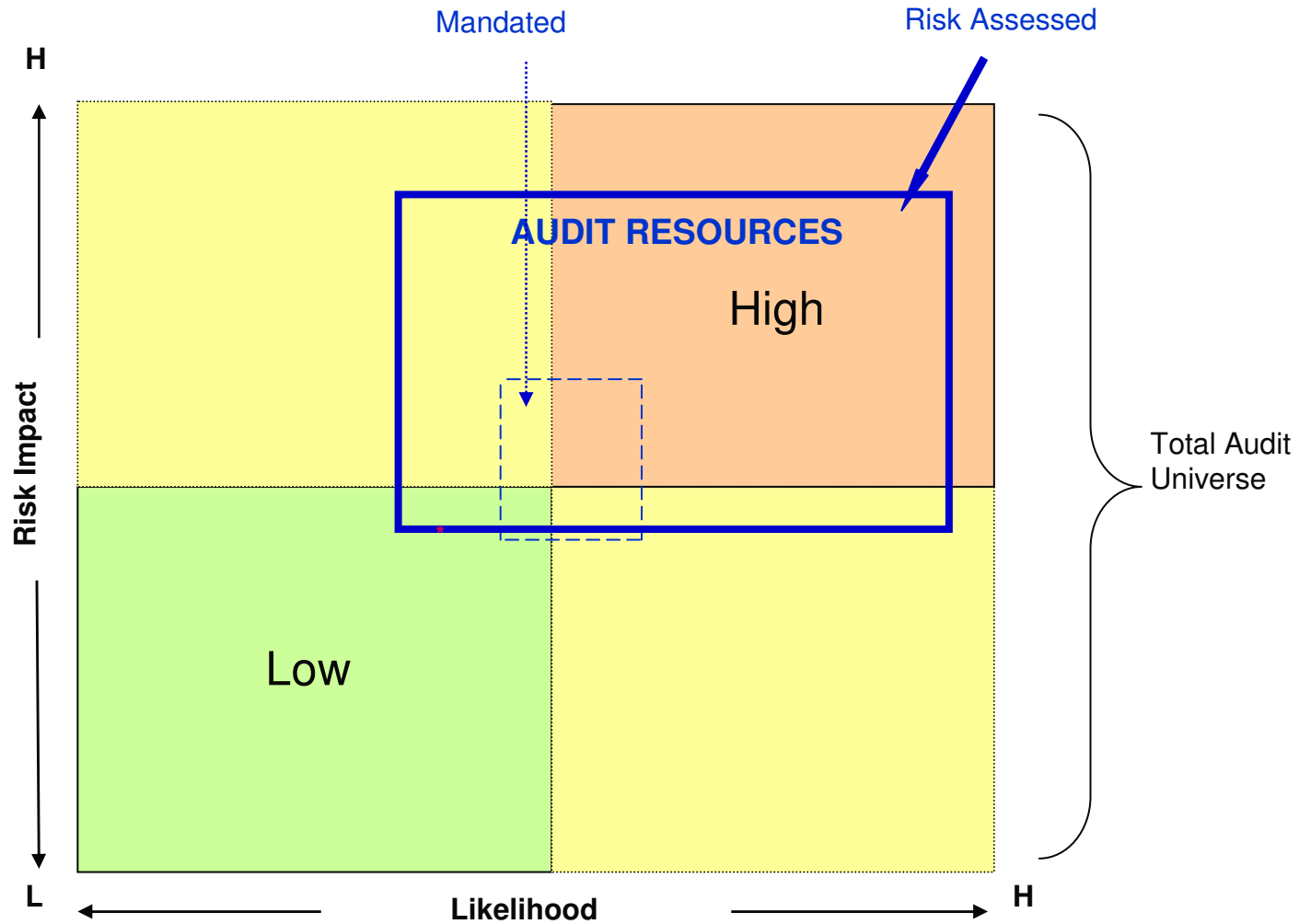
### Key Activities:

- Understand Universe of Potential Audit Subjects
- Allocate and Rationalize Resources
- Reconcile and Finalize Audit Plan

Source: Ernst & Young

- ◆ Focus on high risk audit subjects
- ◆ Audit frequency
  - Established in an initial risk assessment and is proportional to the risk level
  - No predefined audit frequency; The audit plan is based on a continuous risk assessment
- ◆ Consider mandated audit areas
- ◆ Consider management's requests for consulting services
- ◆ Integrate the IT audit plan with non-IT audit activities

# Validate the IT Audit Plan



## Steps to develop the IT Audit Plan:

- ◆ Understand the organization and how IT supports it
- ◆ Understand the IT environment and define IT audit universe
- ◆ Prioritize audit subjects through risk assessment
- ◆ Develop the IT audit plan

## An example - The Company



- ◆ US \$7 billion in total assets
- ◆ Based in the United States
- ◆ Thirty production facilities in seven countries, including Belgium, China, Qatar, Saudi Arabia, Singapore, South Korea, and the United States
- ◆ Six research, technology, and quality control centers co-located in each production facility
- ◆ Five thousand employees worldwide
- ◆ Five major competitors
- ◆ Holds nearly 3,000 domestic and international patents and patent applications
- ◆ Three major business units for manufacturing operations along product lines, centralized headquarters, and support service organizations
- ◆ Three major capital projects to build and expand manufacturing capacity

## An example - The Company's IT Environment

Centralized IT organization consists of four basic divisions:

- ◆ Global infrastructure
  - Telecommunications, Voice communications, Networks, Remote connectivity, Desktop and Internet, Information life cycle management, Servers
- ◆ Enterprise applications: one major ERP application used throughout the company
- ◆ Manufacturing systems
- ◆ Strategy and risk management

# An example - IT Audit Universe

<b>Business Unit</b>	<b>Audit Subject</b>
Corporate	Network administration and security
Corporate	Remote connectivity
Corporate	Windows server administration and security
Corporate	UNIX administration and security
Corporate	ERP application and general controls
Corporate	Sarbanes-Oxley sustainability review
Corporate	Corporate privacy compliance
Corporate	Database administration and security
Corporate	IT governance practices
Corporate	ITIL deployment practices
Corporate	Application program change control
Business Segment 1–3	Major capital investment projects (i.e., information protection and corporate compliance)
Facility 1–30	IT infrastructure
Facility 1–30	Human resources and payroll application
Facility 1–30	Process control systems

## An example - Risk Assessment

A three-point scale to assess likelihood, and impact is used as outlined in the following description:

<b>Likelihood Scale</b>		
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

<b>Impact Scale (Financial)</b>		
H	3	There is a potential for material impact on the organization's earnings, assets, reputation or stakeholders.
M	2	The potential impact 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.

# An example - Risk Assessment

Audit area	Financial Impact		Quality of Internal Controls		Changes in Audit Unit		Availability		Integrity		Confidentiality		Score & Risk level	
	L	I	L	I	L	I	L	I	L	I	L	I		
ERP Application & General Controls	3	3	2	2	3	3	3	2	3	2	3	2	31	H
Treasury EFT Systems	3	3	3	3	3	3	3	2	3	2	2	1	31	H
Facility 3 – HR/Payroll Application	3	3	3	2	3	3	2	2	2	3	2	3	31	H
Employee Benefits Apps (Outsourced)	2	3	2	2	3	3	3	2	2	3	3	3	31	H
Facility 3 – IT Infrastructure	2	2	3	2	3	3	3	3	3	2	2	2	30	H
Facility 3 – Process Control Systems	3	3	3	2	3	3	3	3	2	2	2	1	30	H
UNIX Administration and Security	2	2	3	2	3	3	3	2	3	2	2	1	28	M/H
Corp Privacy Compliance	3	1	3	3	3	3	2	1	2	1	3	3	28	M/H
Database Administration and Security	2	2	2	2	2	2	3	3	2	2	2	1	25	M
SOX Sustainability Review	2	2	2	2	2	2	1	1	2	2	1	2	21	M
Network Administration and Security	2	2	1	1	1	2	2	1	2	2	2	2	20	M
Facility 2 – Process Control Systems	2	2	2	2	2	2	2	2	1	1	1	1	20	M/L
ITIL Deployment Practices	1	1	1	3	2	1	3	1	1	3	2	1	20	M/L
Facility 2 – HR/Payroll Application	1	1	1	2	2	3	2	2	3	1	1	1	20	M/L
Facility 30 – HR/Payroll Application	1	1	1	2	2	2	2	2	2	2	1	2	20	L
Facility 1 – HR/Payroll Application	1	1	1	2	2	2	2	2	2	2	1	2	20	L

## An example - High Level Audit Plan

Engagement	Risk Level	Cycle	Audit Days Allocated
Pen Test Coordination	*	0	40
Procurement Application Follow-up	*	0	20
ERP Application & General Controls	H	1	100
Facility 3 – HR/Payroll Application	H	2	30
Employee Benefits Apps (Outsourced)	H	3	100
Facility 3 – IT Infrastructure	H	2	90
UNIX Administration and Security	M/H	1	90
Corp Privacy Compliance	M/H	3	40
Windows Server Admin and Security	M	3	90
Facility 1 – IT Infrastructure	M	3	90
Facility 1 – Process Control Systems	M	3	90
Environmental Reporting Systems	M	3	30
Major Capital Investment Projects	M	3	30
SOX Sustainiability	M/*	3	120
ITIL Deployment Practices	L/*	4	40
<b>Total</b>			<b>1000</b>
* = Management Request			

- ◆ IT only exists to support and further business objectives.
- ◆ To define IT audit universe, understand the business first
- ◆ To develop IT audit plan, assess business risk associated with IT

- ◆ The International Professional Practices Framework (IPPF)
- ◆ Developing the IT Audit Plan – Global Technology Audit Guide (GTAG) series.
- ◆ The GAIT Methodology – Guide to the Assessment of IT Risks

Visit [www.theiia.org/technology](http://www.theiia.org/technology)

---

Questions?

Contact [Lily.Bi@theiia.org](mailto:Lily.Bi@theiia.org)