CMTA 2023 ANNUAL CONFERENCE

FOR ALL TREASURY | FLAVORS OF DEBT | FINANCE INVESTMENTS

MARRIOTT SAN MATEO • SAN FRANCISCO AIRPORT • APRIL 26-28, 2023

Internal Controls

Common Pitfalls and Real-Life Solutions

California Municipal Treasurers Association

Get to Know Me—Instructor Background

Katherine Krisch, CPA
Partner
Maze & Associates
katherinek@mazeassociates.com

Donald Hester
Cybersecurity Manager
City of Livermore
dehester@LivermoreCA.gov

Table of Contents

Today's Objectives

By the end of this session, you should be able to:

- Name the five components of the Internal Control Integrated Framework;
- Identify some internal control deficiencies seen in your organization
- Respond to these deficiencies by ideas you have learned in this class

Background Information

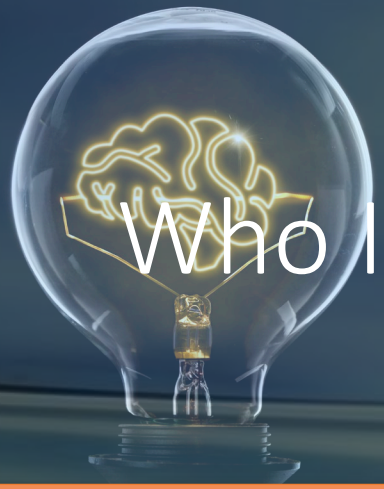
What is internal control

What is **it**?

- A system consists of people, policies and procedures that allow the organization to function

What is **"good" internal control**?

- Allows to achieve 3 objectives:
  - Operation (safeguarding assets, operating effectively and efficiently)
  - Information (providing reliable information)
  - Compliance (complying with all applicable constraints)



Who Is Responsible for Internal Control (IC)?

Management	Governing Body	Internal Auditor	Audit Committee
• Design, Implementation, and maintenance of effective IC	• Overseeing management's performance	• Assisting management in meeting its internal control responsibility	• Assisting the governing body in meeting its IC responsibility

CalCPA

IIA Yearly Report

- 2023 North American Pulse of Internal Audit: Benchmarks for Internal Audit Leaders
- > 550 internal audit leaders
- Rated high/very high as a primary driver of risk:
  - Cybersecurity (78%)
  - IT (57%)

The Five Components

of the Integrated Framework of Internal Control

Effective Internal Control

Favorable *control environment*

Periodic *risk assessment*

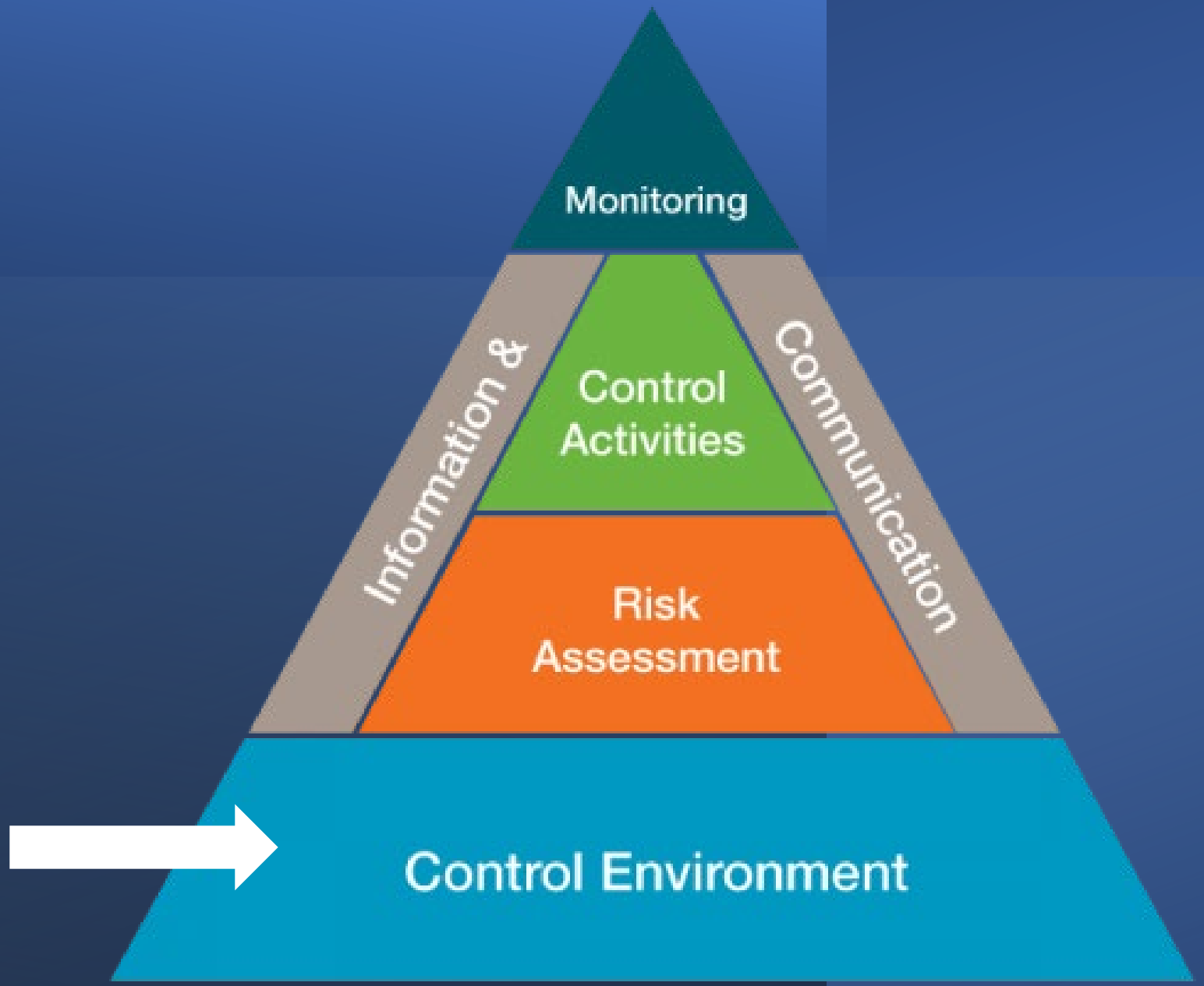
Effective *control activities*

(design, implementation and maintenance)

Effective *information and communication*

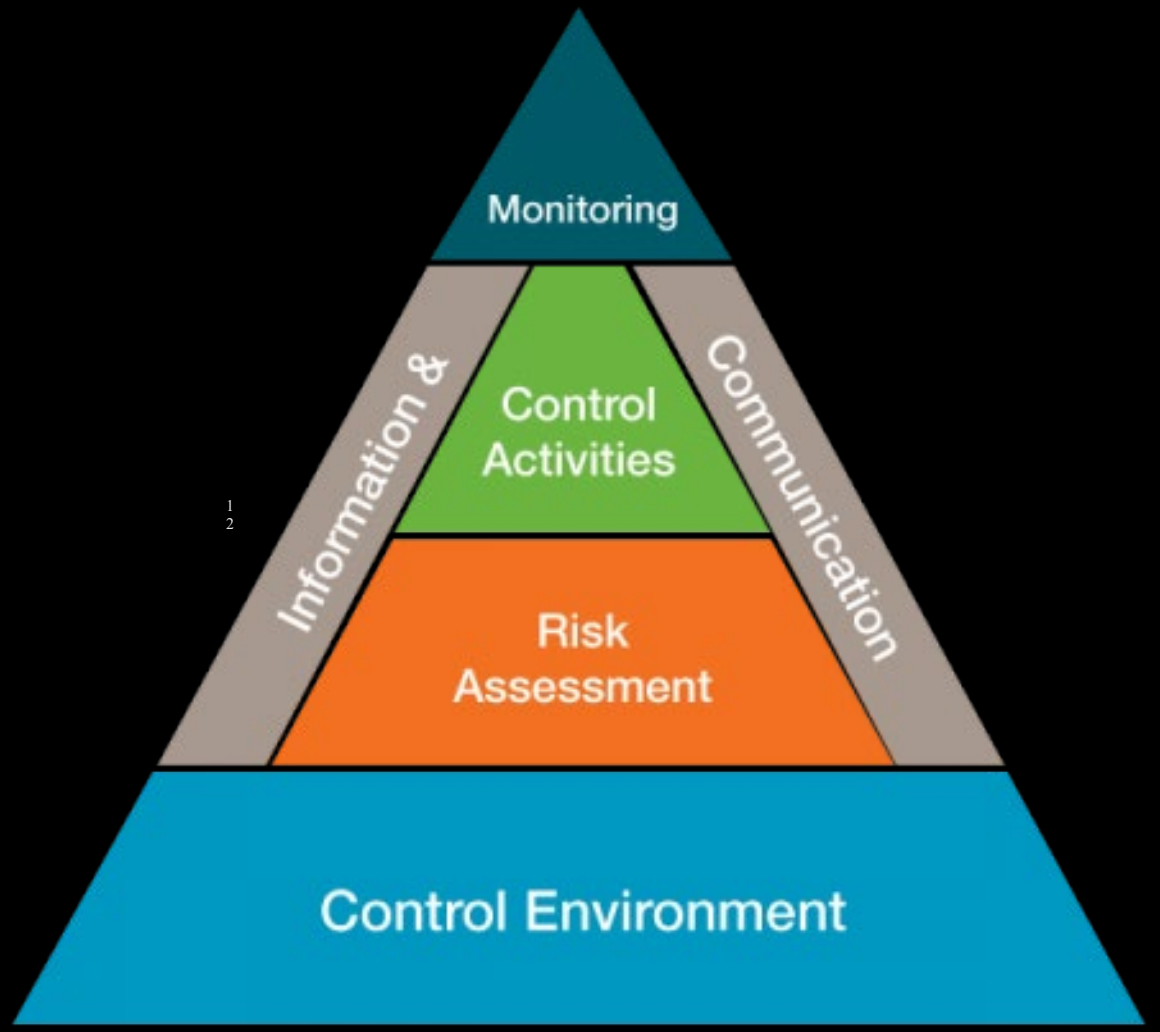
Ongoing *monitoring*

Control Environment



Control Environment

- Infrastructure
- Standards
- Process and structures



An Entity Should……

Demonstrates integrity and ethical values

Has a governing board that takes the role of overseeing management performance actively and seriously

Clearly assigns and document authorities and responsibilities

Has a process to attract, develop, and retain talents

Has measures, incentives and rewards to drive accountability for performance

Challenges Nowadays

Skilled staff shortage (50%)

- Loss of institutional and technical knowledge
- Difficulty in maintaining proper segregation of duties

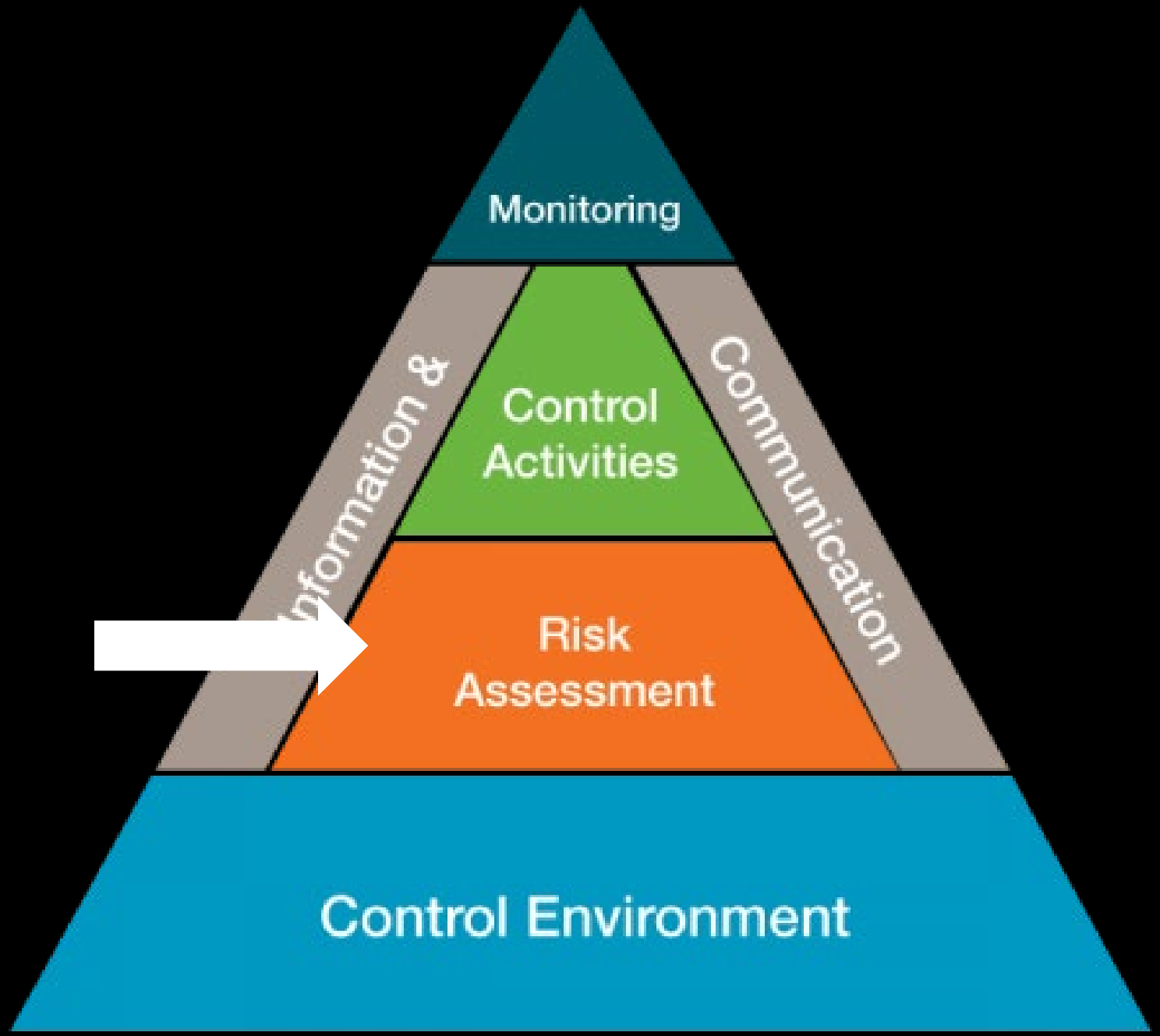
Technological advances (41%)

- Policies and procedures are not updated to reflect changes in technology
- Insufficient skilled staff to keep up with the changes in technology
- Not keeping pace with the technology because “that’s the way we have always done it”

Possible Responses

Frequent	Individualize	Rethink
Frequent risk assessment	Individualize staff development plans	Rethink staff retention strategies

Risk Assessment



Risk Assessment

- Risk = Anything that could negatively affect the achievement of the corporate objectives
- Four steps:
  - Identify
  - Estimate
  - Assess
  - Decide

Risk Assessment Best Practice

Done periodically

Sample risk assessment questions:

- What are the weak spots?
- What could go wrong?
- What if a team member is unable to work for a period? Is there cross-training?
- How do the latest changes (e.g. legislation, organizational, accounting…etc.) affect my organization?
- Does the organization have a succession plan and disaster recovery plan?

Challenges Nowadays

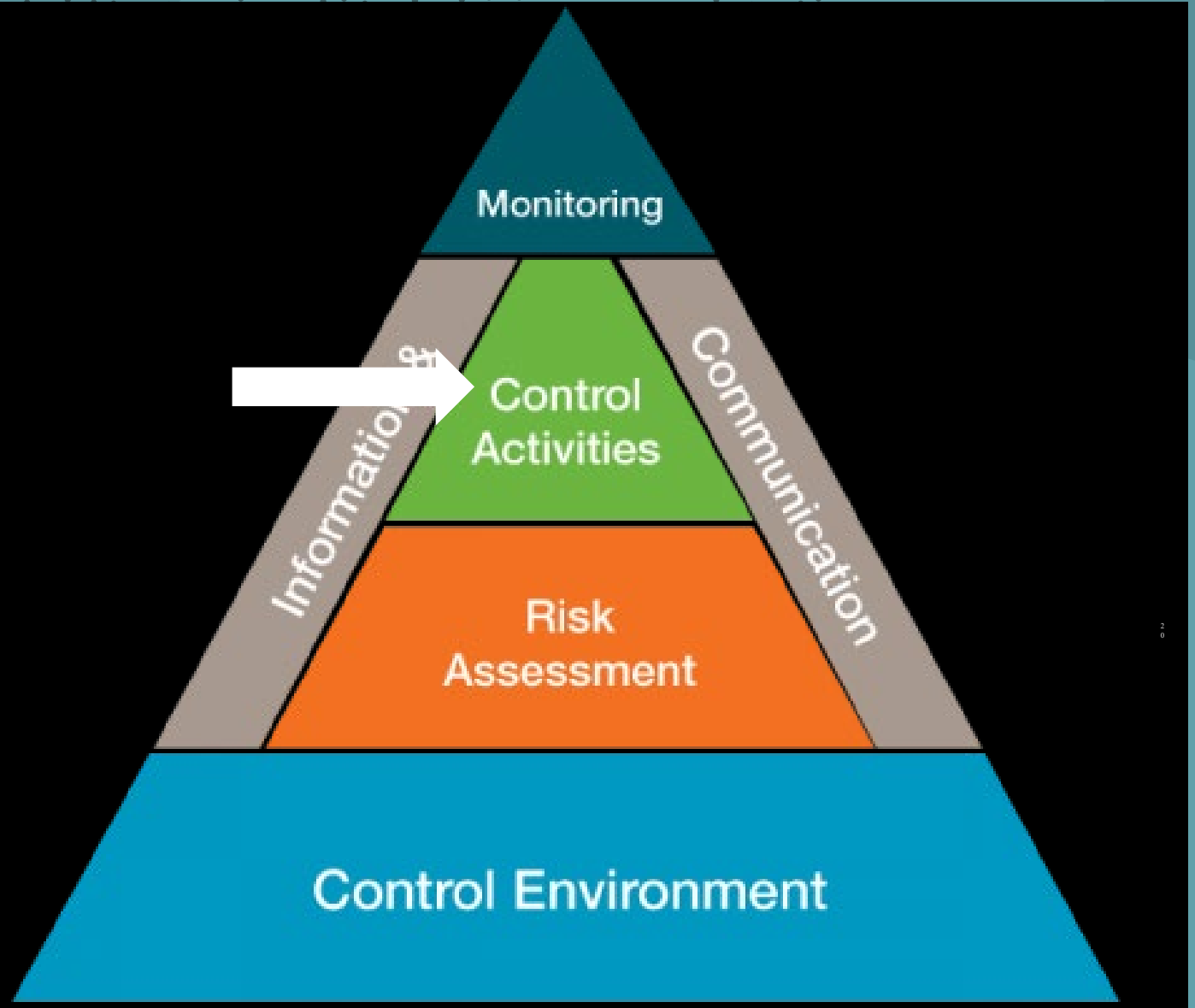
Risk assessment is not done

- Duty should be assigned
- Should be done more frequently, especially when major changes happen
- Meet with the IT professional regularly to identify new risks

Lack of SKE (Skill, Knowledge and Experience)

- People responsible for risk assessment should have the SKE
- Risk assessment procedures should be documented

Control Activities

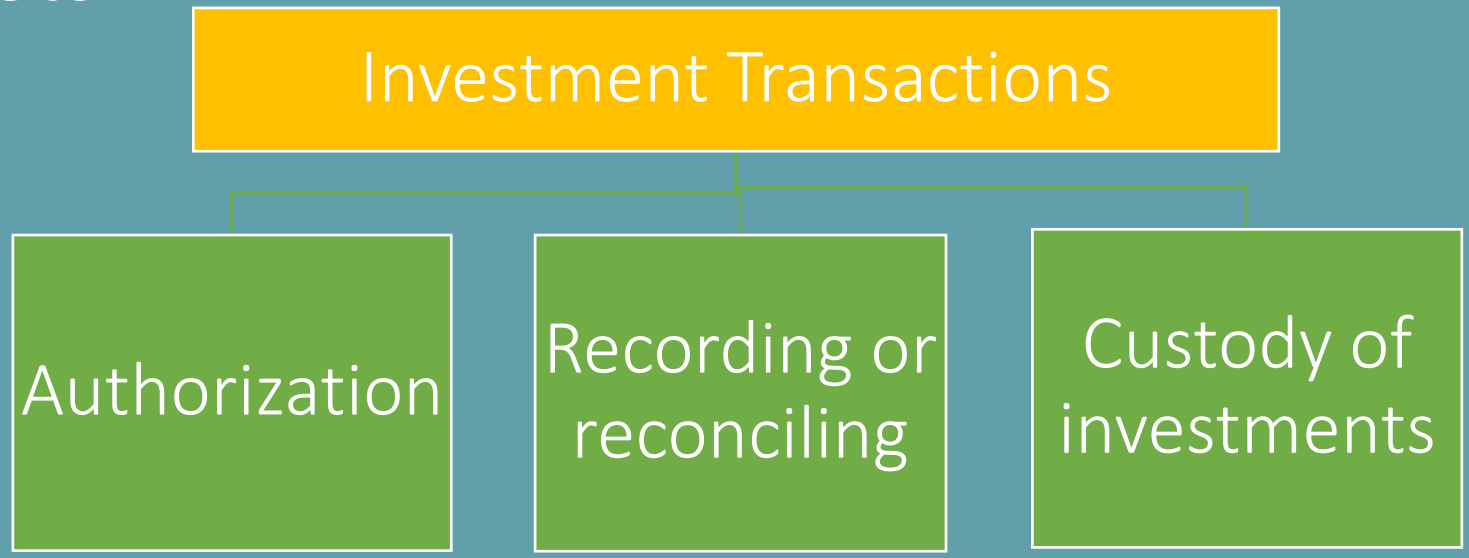


Control Activities

Control activities = actions established through policies and procedures, which help ensure that management's directives to mitigate risks to the achievement of objectives are carried out

Segregation of Duties

- Should segregate:
  - Authorization
  - Recording/reconciliation
  - Custody of assets



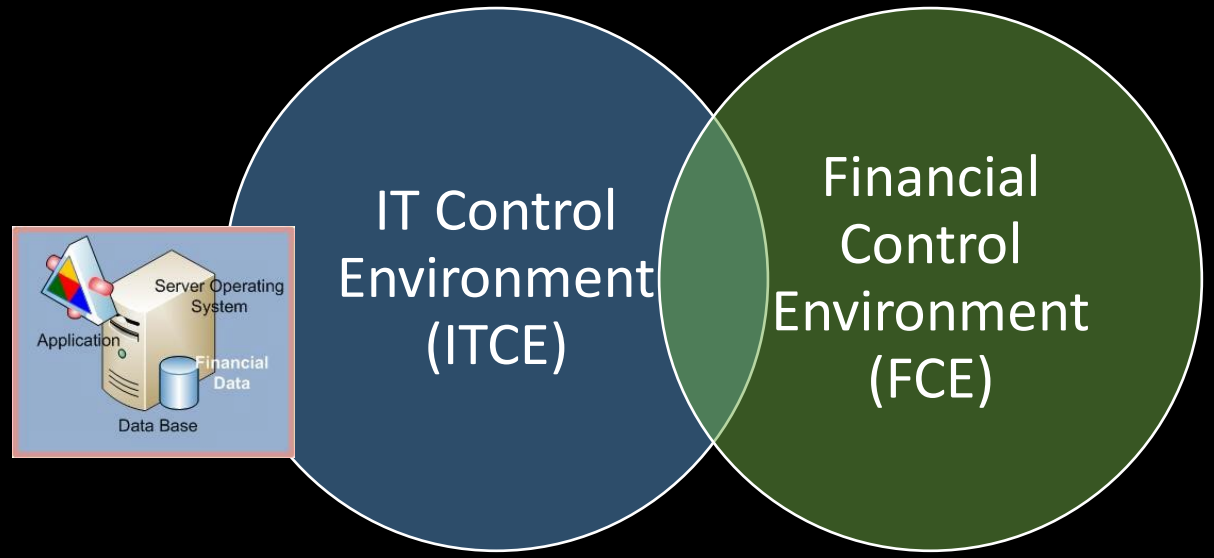
Other Control Activities

Proper procedures and appropriate authorizations documented in a meaningful manner

Financial data is regularly analyzed by someone with SKE

Maintain physical controls over assets and records

The IT & Financial Control Environment Overlap



Control Environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization.

Controls over information processing

- Information produced by the system should be reliable
- Integrity of the system
- Control procedures should be in place to restrict
  - (1) the access to the program data, and
  - (2) the ability to make modifications to the data

Benefits vs. Cost

Benefits > Cost of control activities

For smaller governments, an **appropriate** second person may be a member of the governing body

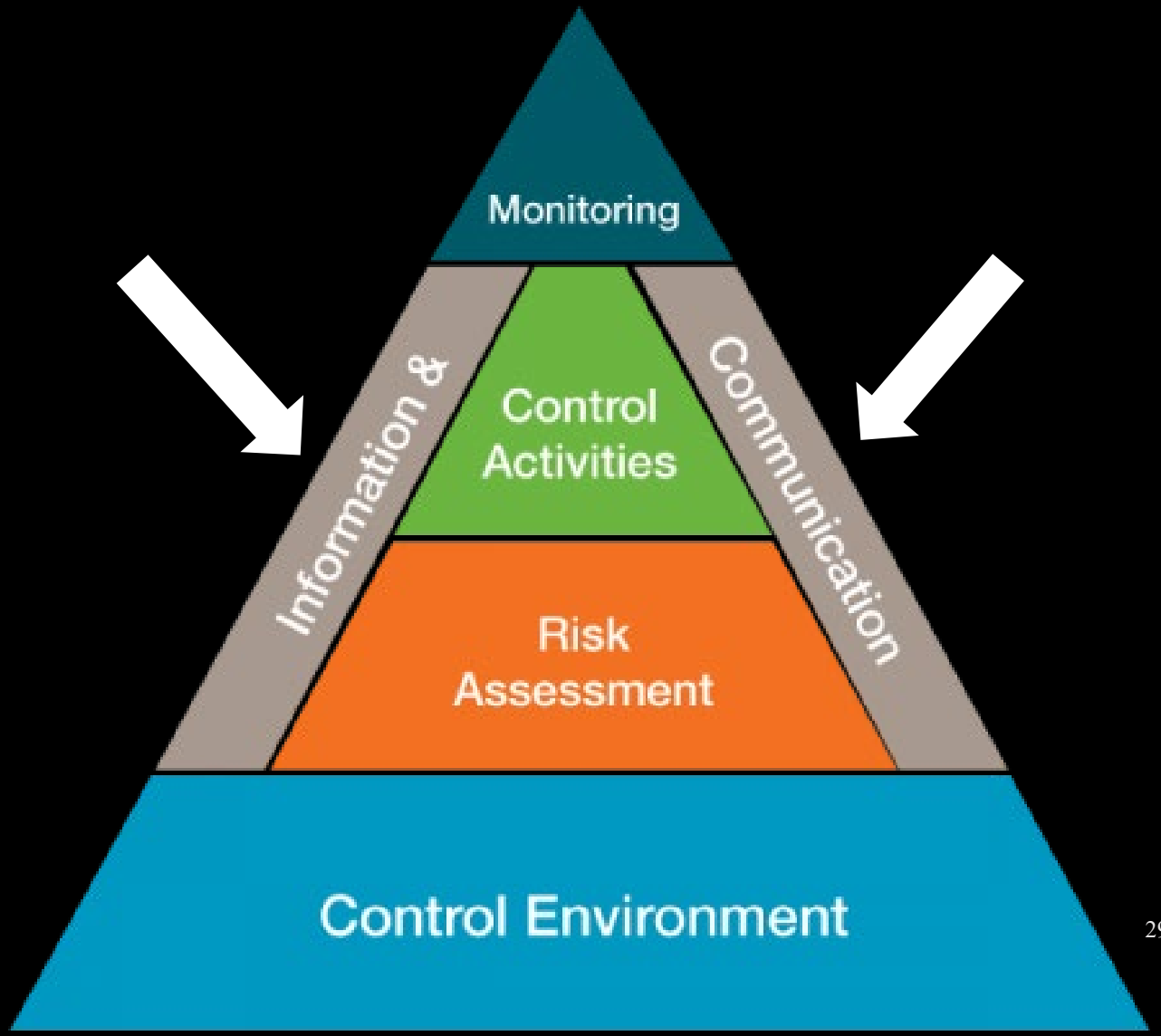
Challenges Nowadays

- Desk procedures are not documented
  - Loss of knowledge during staff turnover
- Control activities are compliance driven instead of effectiveness led
- Difficulty in updating control activities after transformational changes, due to:
  - Lack of technical knowledge
  - Lack of focus on internal control

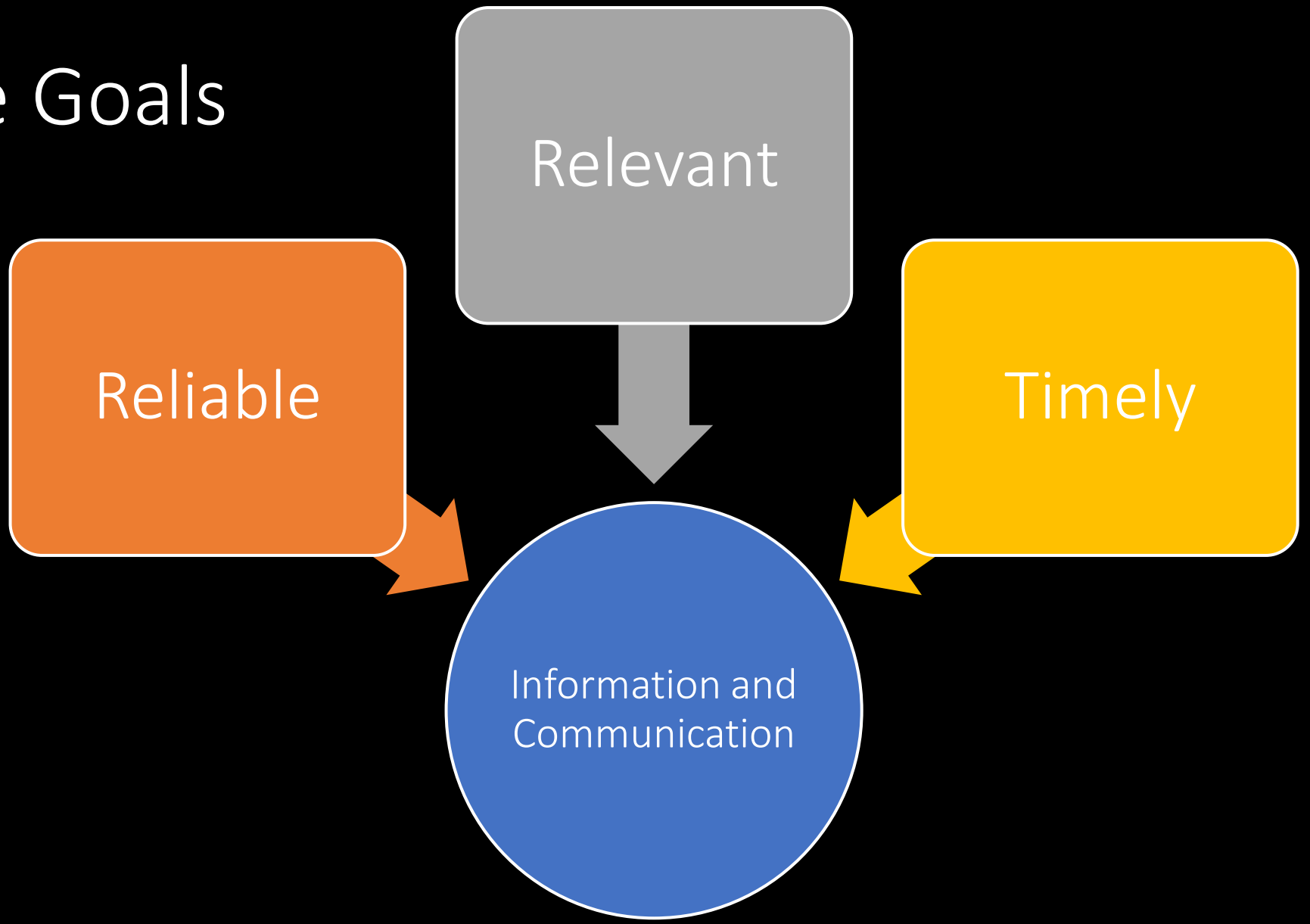
Challenges Nowadays -- Employees may be accessing systems from networks outside of the organization

- Ensure proper IT and cybersecurity measures are in place
  - Evaluate policies and controls for access and authorizations. Remote access to servers should be established via secure connections (e.g. virtual private network “VPN”).
  - Communicate to staff clearly the policies about using devices owned by your organization.
  - Consider implementing security measures such as automatic locking of devices after a period of inactivity to prevent access without re-entering credentials, two-factor authentication for log-ins…..etc.
  - Cloud based systems can easily allow people to access the system from any device from any location. Consider a Policy on BYOD bring-your-own-device for employee-owned devices.

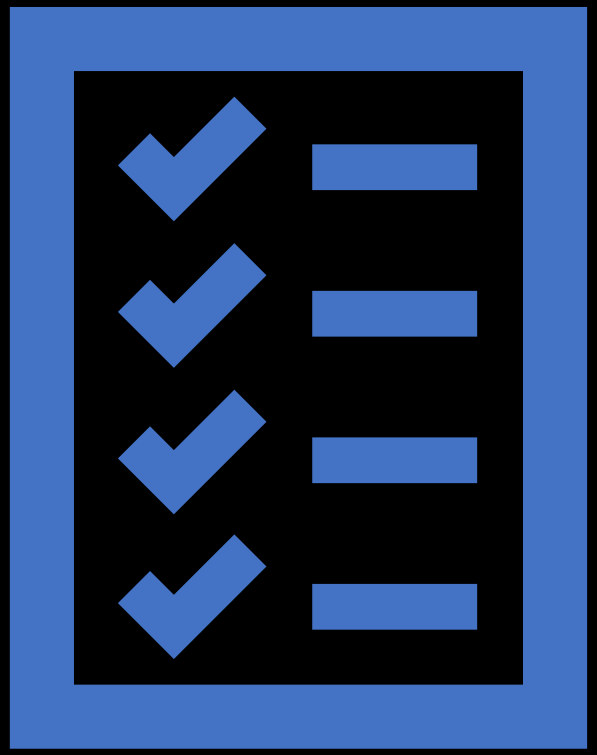
Information and Communication



Three Goals



Does your organization……



- Record transactions accurately?
- Resolve errors timely?
- Leave an audit trail when making corrections to financial records?
- Allow management overrides in financial system?
- Ensures accurate data transfer between systems?
- Has procedures to capture other information timely and accurately?
- Produces accurate and timely financial reports?
- Have available to the stakeholders relevant and reliable information in a timely manner?
- Have means for external parties to provide feedback?
- Have regular inter- and intra-departmental meetings to encourage communication?

Challenges Nowadays:

Remote/Hybrid Work Environment

- Public Wi-Fi may be used however it is not safe
  - People have access to that network and, without a firewall between you and them, nefarious personnel can hack away at your computer from across the room.
  - Any interested observers on either the current network or any other public networks your data hits between you and your workplace can monitor your traffic.

Challenges Nowadays:

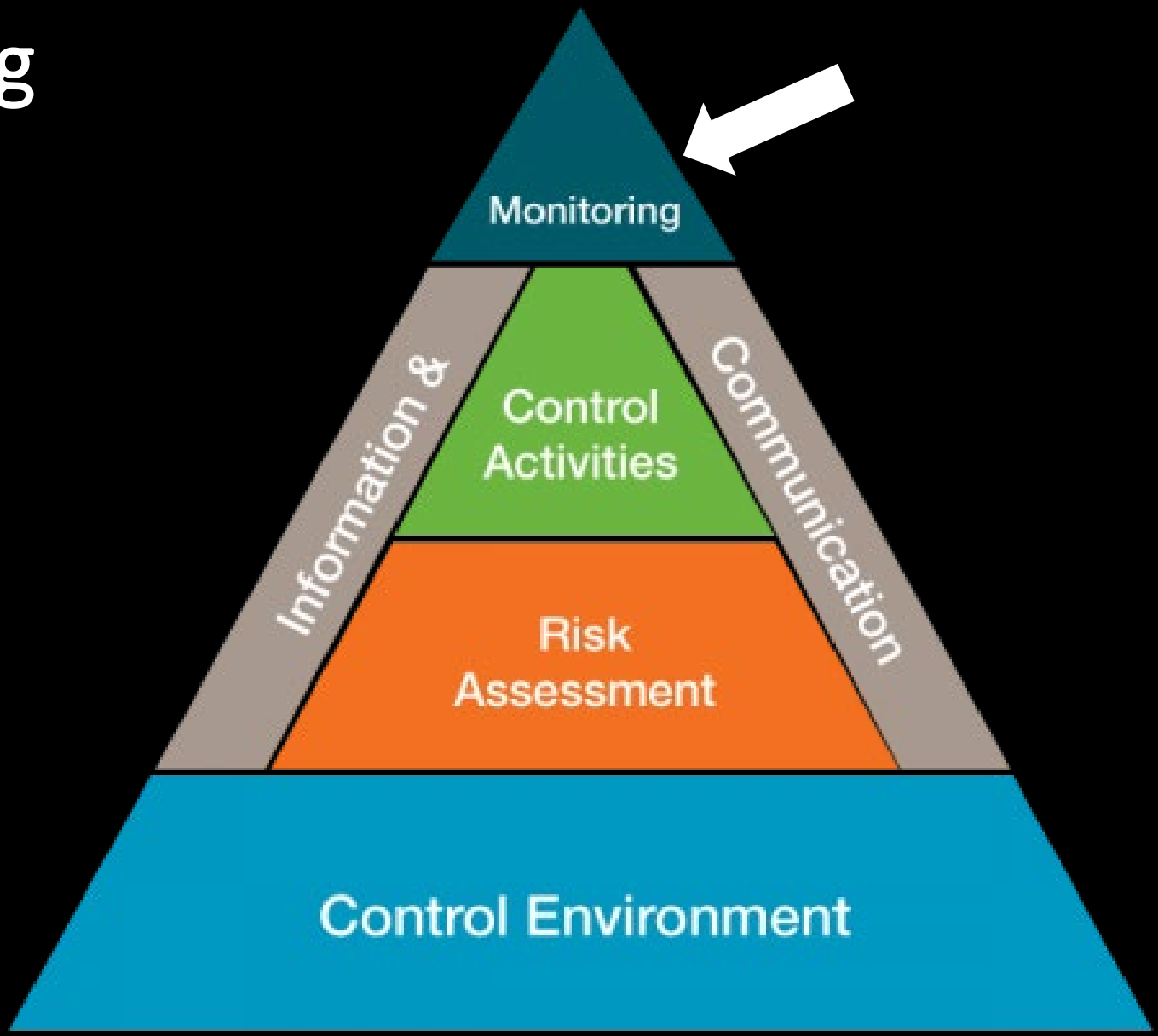
Remote/Hybrid Work Environment

- Consider using:
  - Personal hotspots from a dedicated device or cellphone, does eliminate getting hacked by people on the same public Wi-Fi.
  - Use a VPN for public Wi-Fi
  - Use Phishing-resistant Multi-factor Authentication (MFA)
  - Provide awareness training.

Protect Information

- Educate your employees to:
  - Regular Cybersecurity Awareness Training
  - Keep work data on work computers
  - Screen Blocker
  - Encrypt sensitive data in emails and on the device
  - Use a USB data blocker when charging up at a public phone charging station

Monitoring


Monitoring
Information &
Control
Activities
Communication
Risk
Assessment
Control Environment

Monitoring

A process that is used by management to assess the effective operation of internal controls over time

Should be done on an on-going basis and taking remedial actions when necessary

Should Have Procedures to Ensure……

Control procedures are

1. In place,
2. Have been performed, and
3. Are effective

Control deficiencies

1. Have been communicated to appropriate parties, and
2. Mitigated by corrective actions

Challenges Nowadays

Outdated policies or procedures that do not correspond with the current environment

- ❖Frequent conversations with staff to ensure changes to processes do not render controls ineffective.
- ❖Identified gaps in internal controls should be addressed proactively.
- ❖Once changes to control procedures are made, solicit feedbacks in order to the effectiveness of the new procedures.

Audit findings go unresolved due to priority change

- ❖Evaluate the current internal control environment and re-prioritize tasks.
- ❖Speak to the auditor to find feasible alternatives to mitigate the control deficiencies.

Challenges Nowadays

Complexity and continuous rapid change of technology

Lack of staff time to periodically review controls

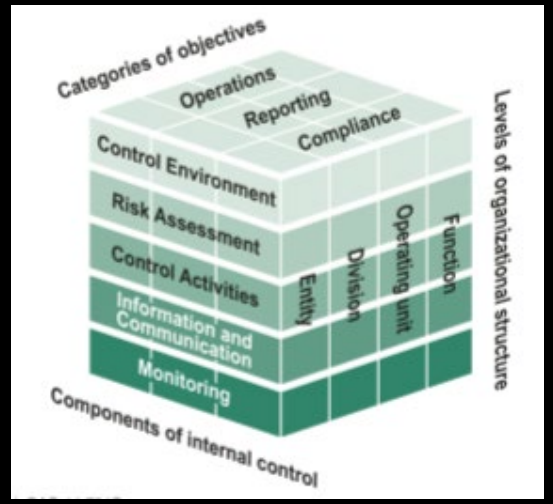
No staff ability to assess or create technical controls

Consider smart systems to monitor for anomalous activity (Artificial Intelligence)

Consider adding cybersecurity to Internal Audit function

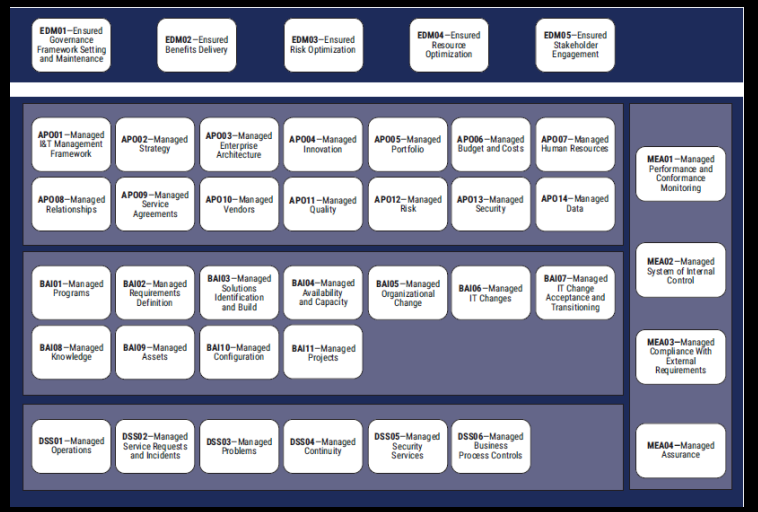
Case Study Complex IT Control Environment

Governance of IT and Internal Controls



COSO Framework

Internal Control Guidelines



COBIT 2019

It's all about the mission

Internal Controls

Cyber Risk Management

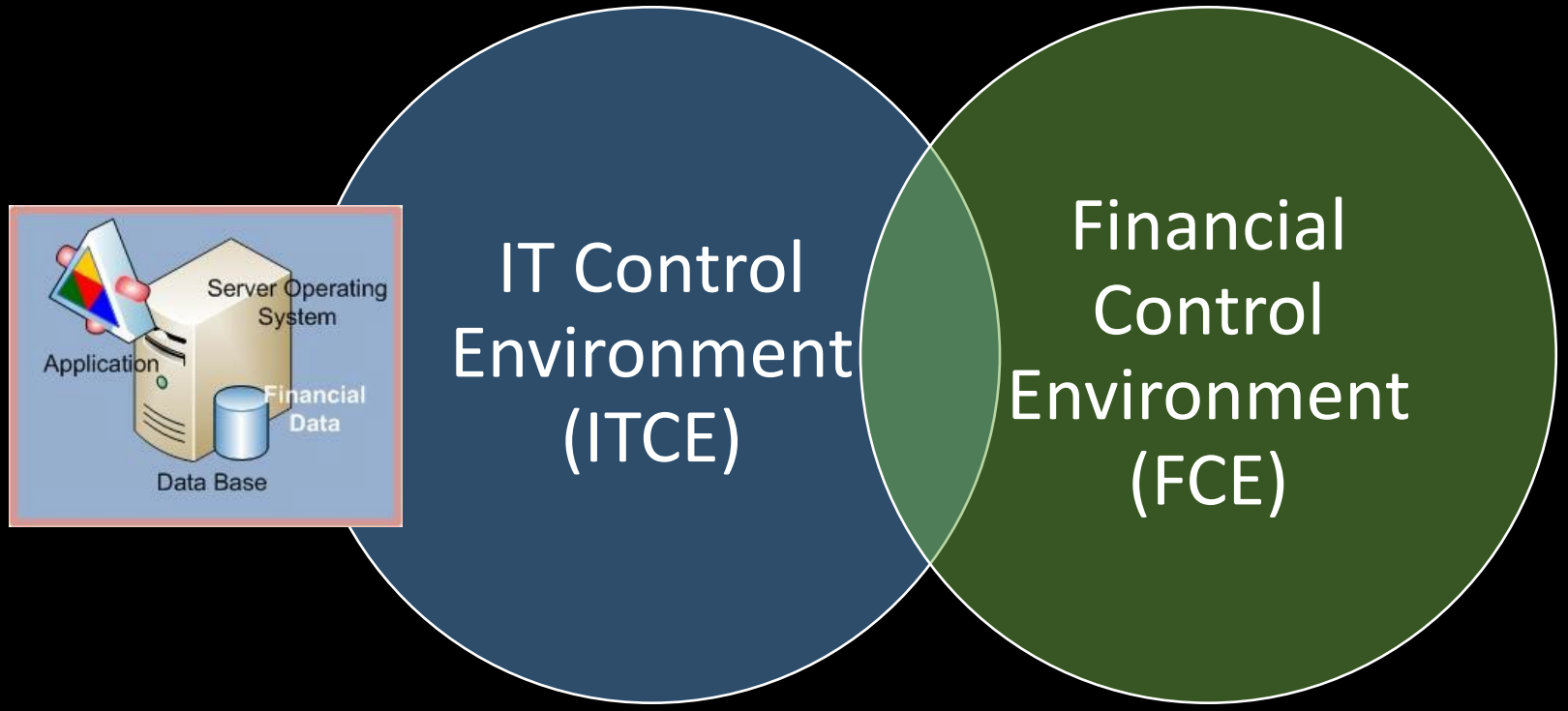
"The Information Technology (IT) department should periodically identify and communicate risks for which employees should be particularly vigilant."

Follow Industry Standards

"Application Controls and General IT Controls, which relate to the overall effectiveness of IT controls to ensure the proper operation of the local government's information systems."

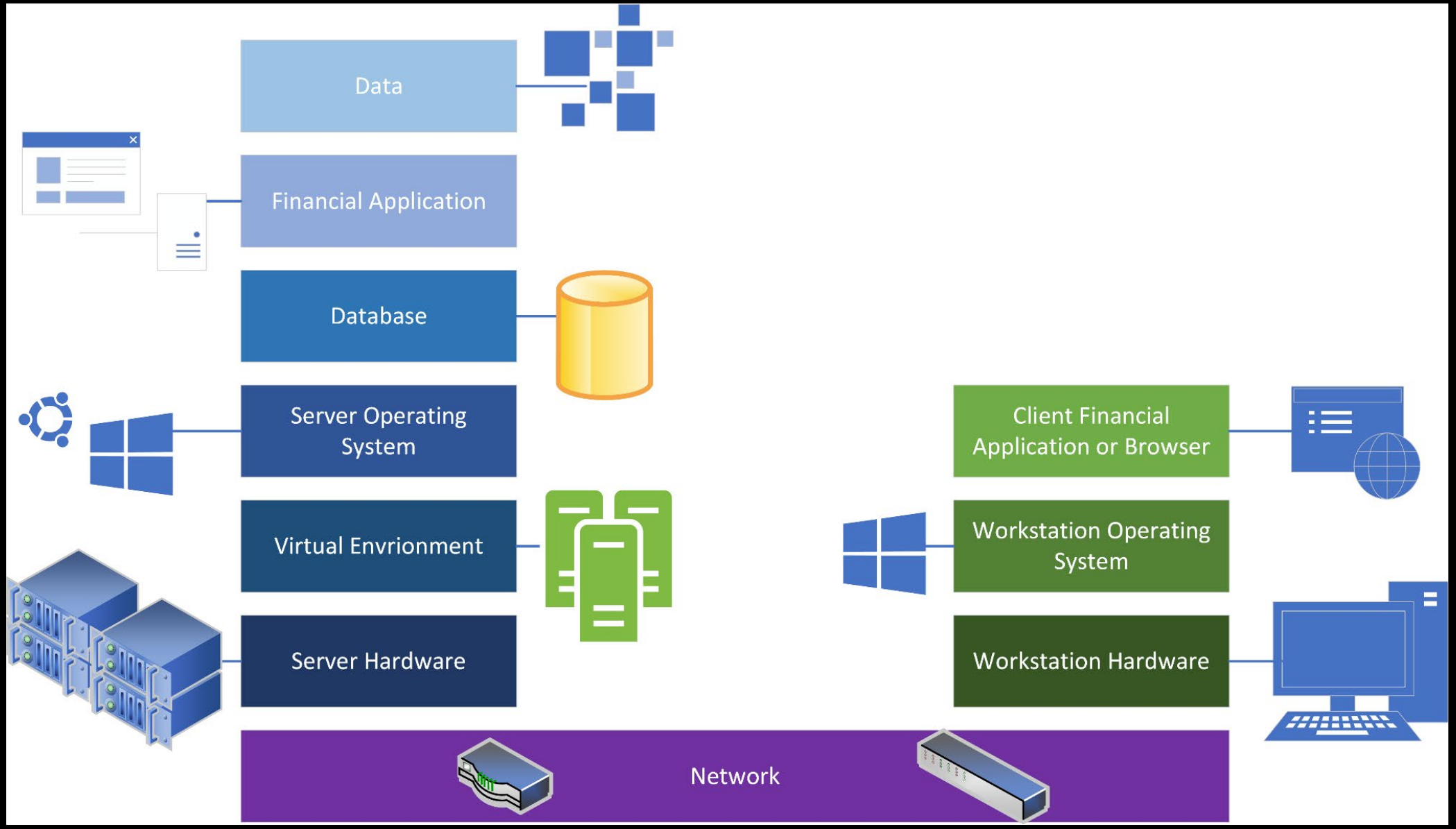
Internal Control Guidelines

The IT & Financial Control Environment



Control Environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization.

Traditional IT Control Environment



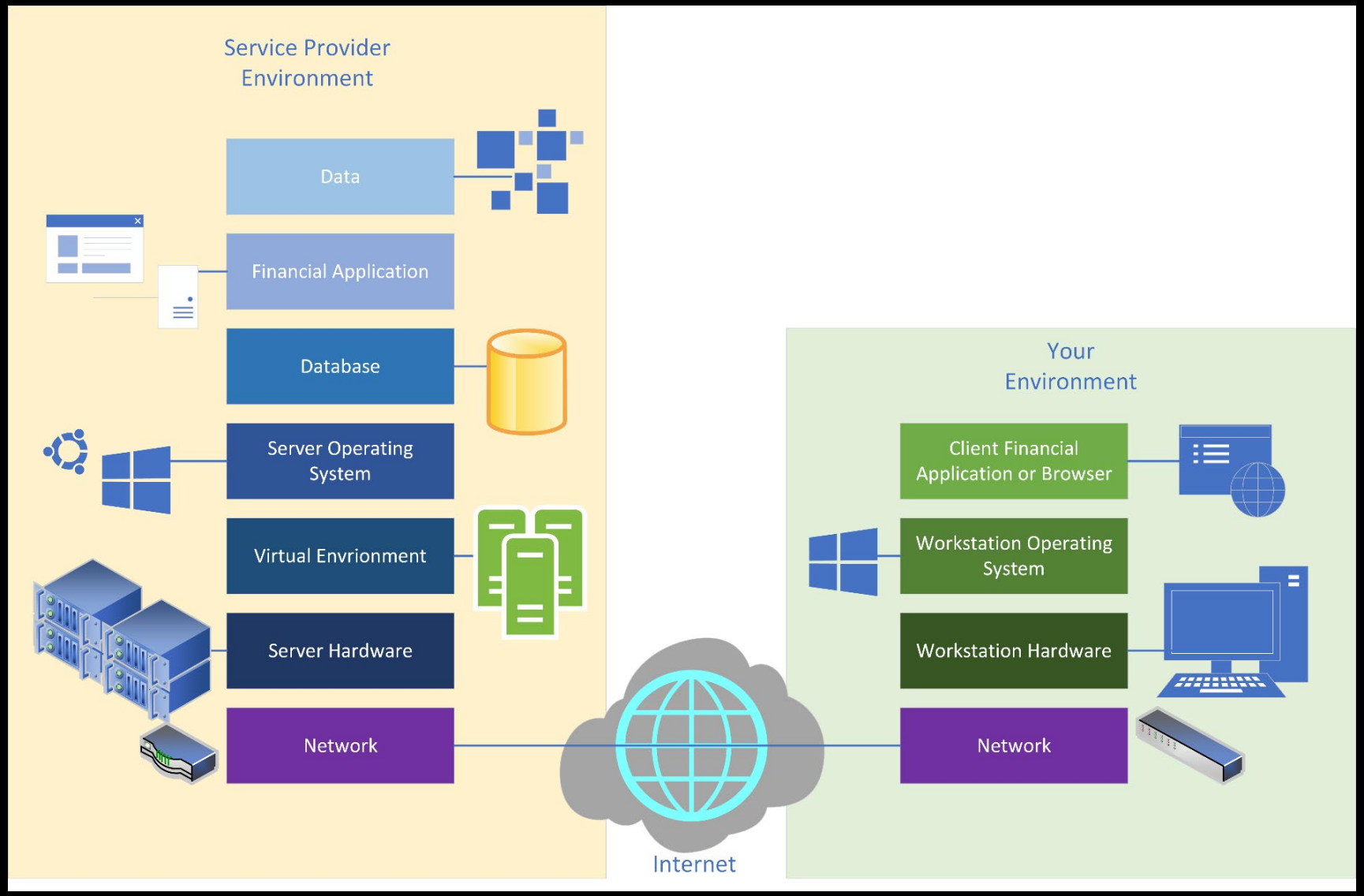
What about a Cloud Based ERP?

Who manages the control environment in the cloud?

How do you know who is responsible for what controls?

How do you verify the cloud service provider is secure?

Cloud IT Control Environment



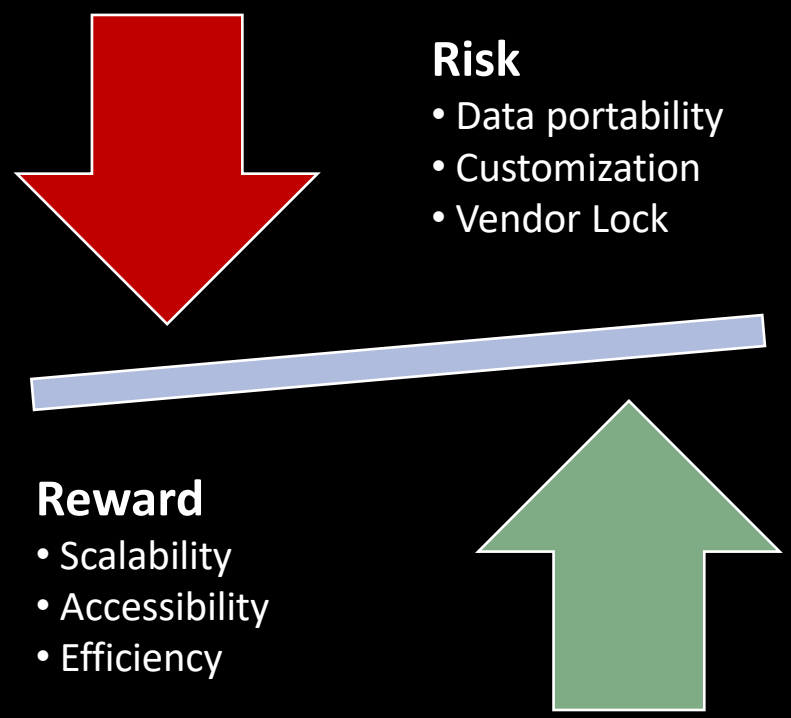
On Prem or Cloud

The on-premise solution is not necessarily the lowest risk option.

IT leaders must determine internal capabilities for staff skill sets, network availability, application security, and data protection.

Risk and Benefit

- Leveraging the Cloud is about risk and reward.
- Consider both sides and balance the opposing forces to successfully evaluate cloud-based ERP deployments.



Shared Responsibility

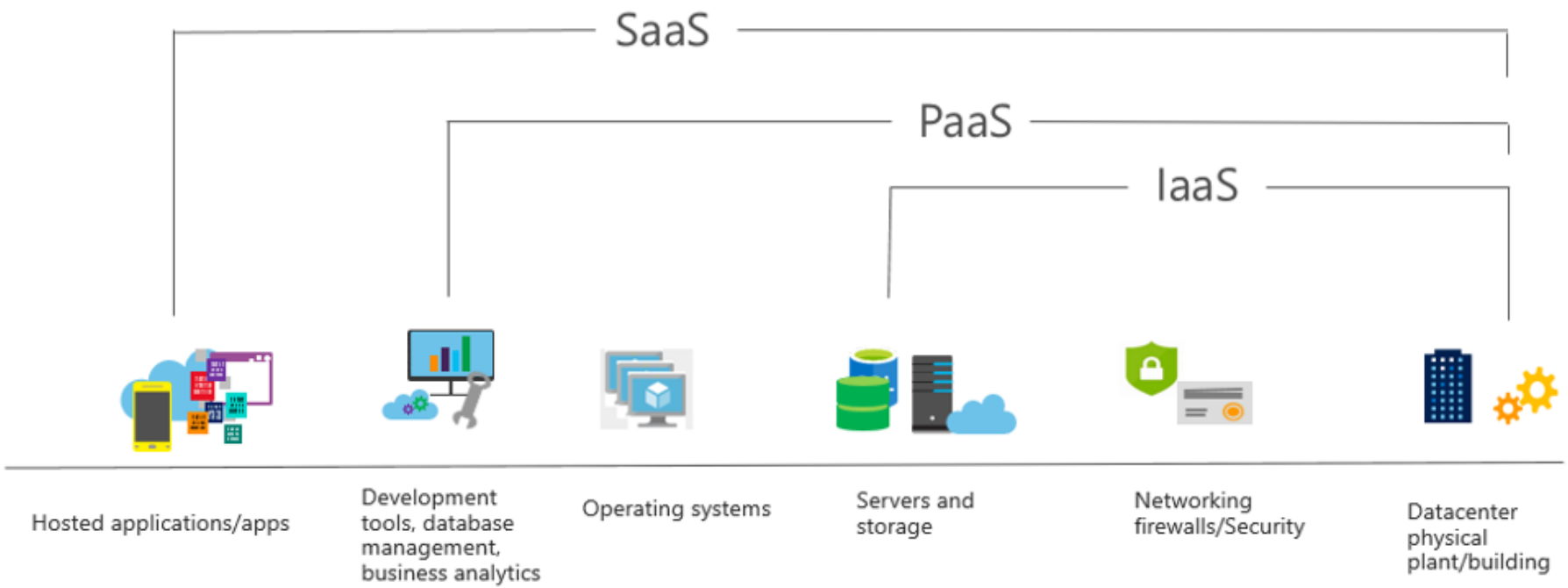
- The control environment is now shared
- Therefore, responsibility is shared
- Where is the line of demarcation?

- Inside your organization:
- Cross-departmental team
- Finance, operations, and IT stakeholders
- Regular review process

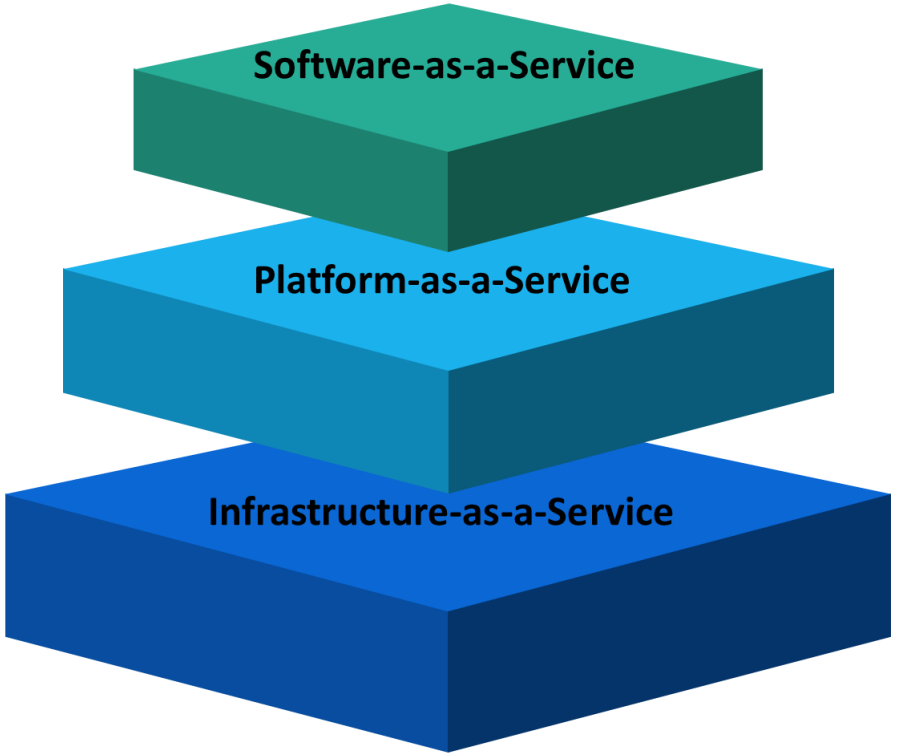
- Outside your organization:
- Define and establish responsibilities
- IaaS Provider
- SaaS Provider
- Consultants, Venders, Resellers, Integrators
- Additional service providers

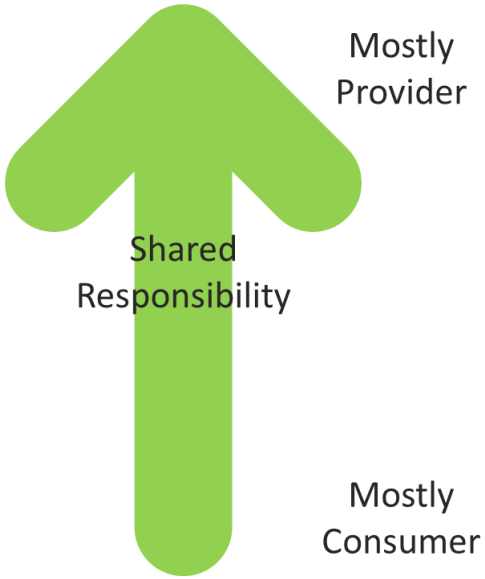
Different Cloud Services Different Risks

Shared Responsibility

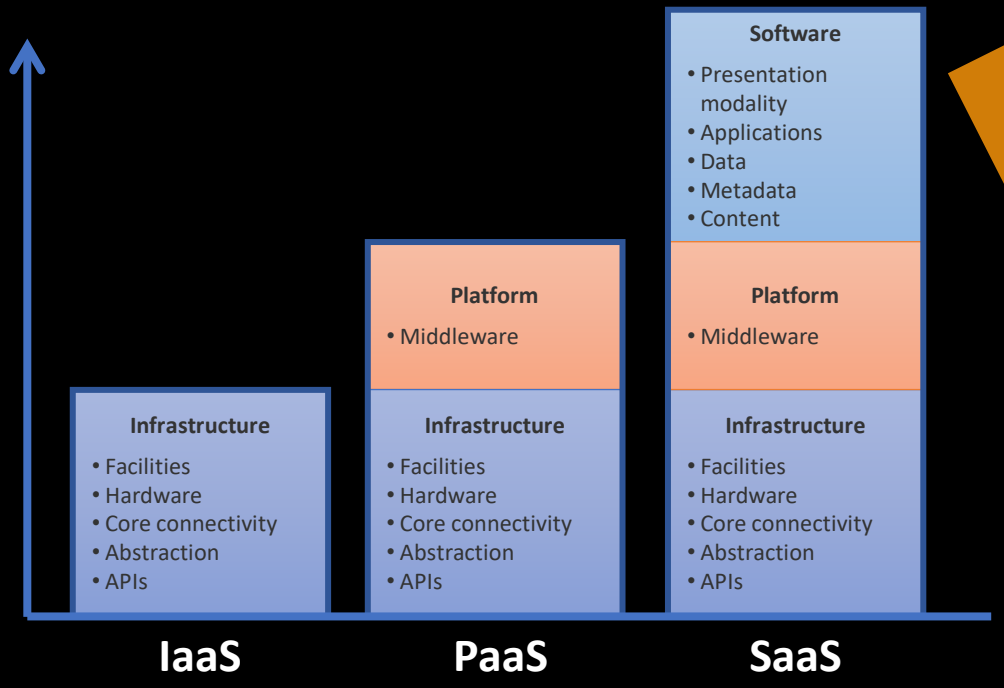


Cloud Service Models



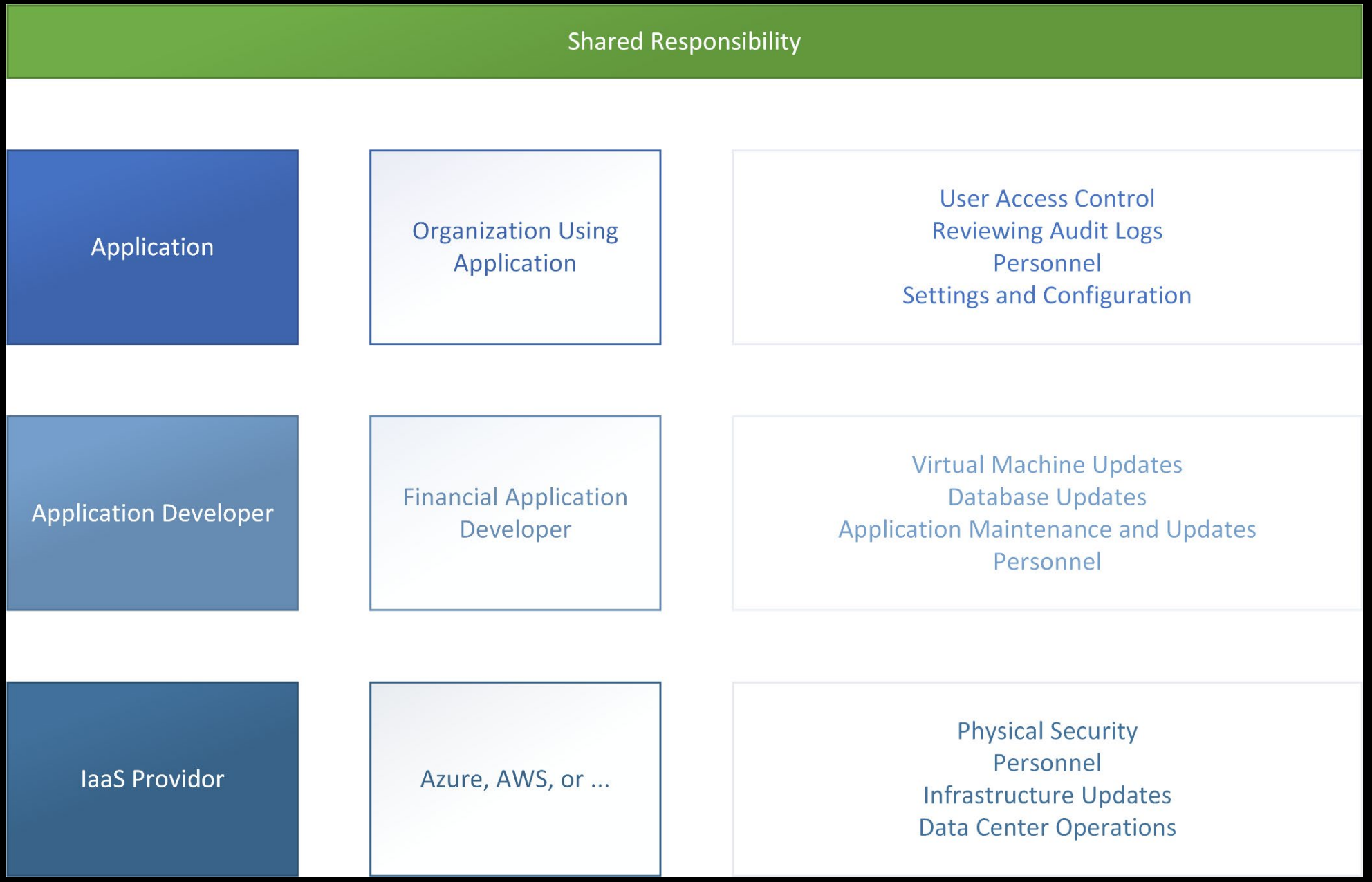


White Label

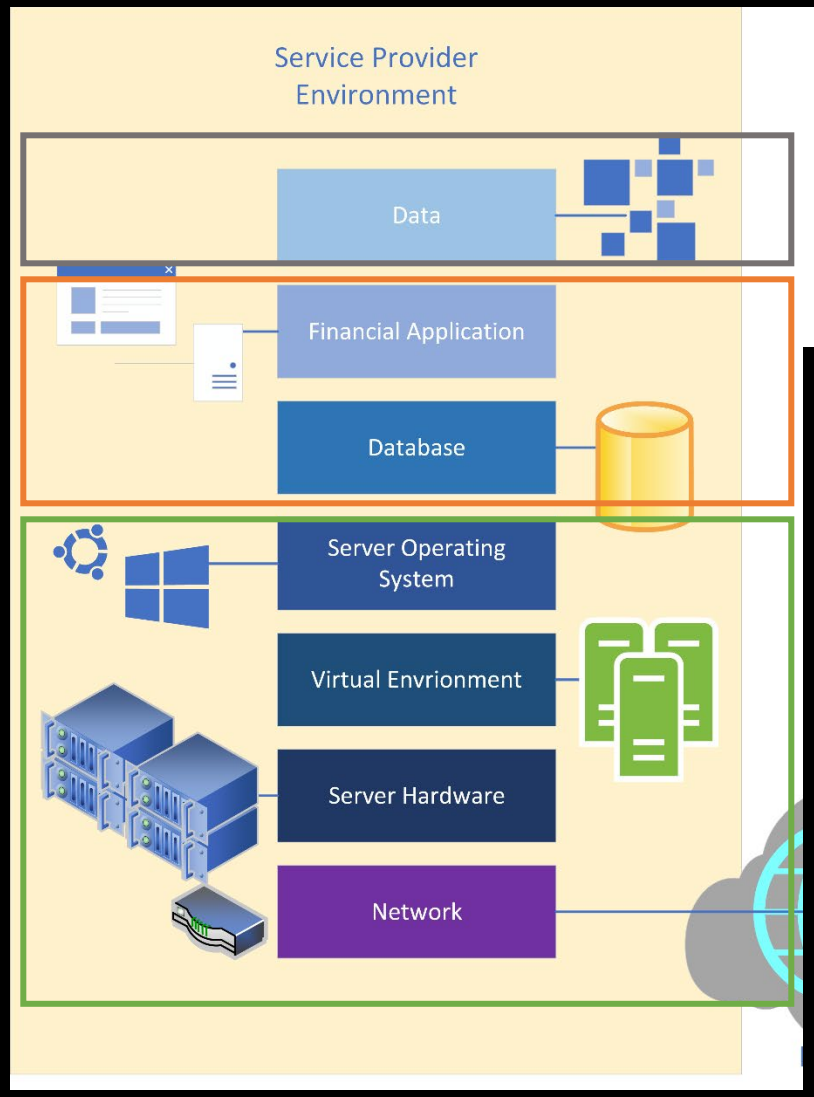


White Label and Proprietary Cloud models require detailed due diligence. Ensure that the solution is appropriate not just as the Software tier, but also at the Platform and Infrastructure tier.

White Label cloud providers mimic SaaS, but require IaaS-style due diligence


Shared Responsibility
Application
Organization Using Application
User Access Control
Reviewing Audit Logs
Personnel
Settings and Configuration
Application Developer
Financial Application Developer
Virtual Machine Updates
Database Updates
Application Maintenance and Updates
Personnel
IaaS Providor
Azure, AWS, or ...
Physical Security
Personnel
Infrastructure Updates
Data Center Operations

Cloud IT Control Environment



Your responsibility

Developers' responsibility

Cloud Providers responsibility

Critical Controls

- Third Party Service Provider Risk Assessment
- Annual Risk Assessment
- Additional Compensating Controls
- Service Level Agreement
- Breach Notification
- Timely Breach Notification

- Access Control
- Session Locks
- Session Termination
- Audit/Event Logs
- Business Continuity
- Authentication

Critical Controls

- Transborder Data Flow and Storage
- eDiscovery, Litigation Hold, Forensics
- Data Retention
- Data Export
- Geofencing
- Audit Review
- Disengagement Process

What to do?

- Careful planning before engagement
- Understand the technical aspects of the solution
- Make sure it will meet your needs (security and privacy)
- Maintain accountability
  - Define data location restrictions
  - Ensure laws and regulations are met
  - Make sure they can support electronic discovery and forensics
- Follow NIST and Cloud Security Alliance guidance

City of Livermore Technology Purchase Addendum

Cybersecurity Cloud Service Risk Matrix	
Complete this section if any part of this is solution is hosted in the Cloud or a Third-party hosted solution. The vendor, IT, or Cybersecurity can assist you in filling this portion out.	
Yes ☐ No ☐	Will this service process, store, or transmit City data? • If no, no further action is needed. • If yes complete the questions below.
Complete below only if you selected yes above	
What is the service model as defined by NIST SP 800-145? ☐ Software as a Service (SaaS) ☐ Platform as a Service (PaaS) ☐ Infrastructure as a Service (IaaS)	
What is the deployment model as defined by NIST SP 800-145? ☐ Private cloud ☐ Community cloud ☐ Public cloud ☐ Hybrid cloud	
Will any of the follow data types be process, store, or transmit by this service? ☐ Protected Health Information (PHI) ☐ Personal Identifying Information (PII) ☐ Criminal Justice Information (CJIS) ☐ Payment Card Information (PCI) ☐ Other data with compliance requirements ☐ N/A	
Yes ☐ No ☐	Will the cloud service provider notify the organization of any breach of the organization's data within 24 hours?
Yes ☐ No ☐	Does the cloud service solution provide for legal controls such as eDiscovery, litigation hold, and forensics?
Yes ☐ No ☐	Can the cloud service provider provide us records within 48 hours for public records requests?
Yes ☐ No ☐	Can the cloud service solution meet our records retention policies?
Yes ☐ No ☐	Does the cloud service provider have regular independent audits (e.g. SAS 70, SSAE 16/18, SOC Type II, ISAE)?
Yes ☐ No ☐	Will the cloud service provider guarantee secure removal of City data from their systems upon request of the City?
Yes ☐ No ☐	Does the cloud service provider perform regular backups of City data?
Yes ☐ No ☐	Does the City have access to backups performed by the cloud service provider?
Yes ☐ No ☐	Does the cloud service provider have written provisions for disengagement (contract termination) and data migration?
Yes ☐ No ☐	Will any City data be given or sold to third parties?
Yes ☐ No ☐	Is the cloud solution FedRAMP or StateRAMP approved? https://www.fedramp.gov/ | https://stateramp.org/
Yes ☐ No ☐	Does the cloud service solution provide access logging capabilities?
Yes ☐ No ☐	Does the City have access to access logs?
Yes ☐ No ☐	Does the cloud service provider offer a service level agreement (i.e. uptime guarantee)?
Yes ☐ No ☐	Is any City data processed, stored, or transmitted outside of the United States?
Yes ☐ No ☐	Does the cloud service provider have cybersecurity insurance?

City of Livermore Technology Purchase Addendum

Service Level

What service level does the cloud solution provider offer for uptime? (i.e. 99.9995%)	
Does the uptime meet the Division/Department/City needs?	Yes ☐ No ☐

The table below shows the equivalent time for percentage of uptime:

Availability Measure	Downtime Per Year	Downtime Per Week
90% (one nine)	36.5 days	16.8 hours
99% (two nines)	3.65 days	1.68 hours
99.9% (three nines)	8.76 hours	10.1 minutes
99.99% (four nines)	52.6 minutes	1.01 minutes
99.995% (four and a half nines)	26.28 minutes	30.24 seconds
99.999% (five nines)	5.25 minutes	6.05 seconds
99.9999% (six nines)	31.5 seconds	604.8 ms

Additional Third Parties

A cloud solution can be made up of multiple cloud service providers. For example, a cloud solution of an online application can have one cloud service provider who developed an application used by the City and that solution can be hosted on another cloud solution. Some cloud service providers develop their solution on the platform or infrastructure of a second cloud service provider.

Is the cloud service provider outsourcing to another cloud service provider for a portion of the complete solution?	Yes ☐ No ☐
List all other cloud service providers?	

Impact Assessment

What is the impact to the City/Department/Division in the event:

That City data hosted by the cloud provider is disclosed? (Loss of data confidentiality)	☐ Low ☐ Moderate ☐ High
That City data hosted by the cloud provider is altered (made inaccurate) without our knowledge? (Loss of data integrity)	☐ Low ☐ Moderate ☐ High
That City data hosted by the cloud provider is lost (no longer accessible)? (Loss of data access)	☐ Low ☐ Moderate ☐ High

Note: The Cybersecurity Division will need to see the independent audit/assessment initially and annually thereafter.

I am happy to provide you with a copy of the form. Just send me an email.

Designing an IT control

- Know your control objective
- Design the control to meet the objective
- Automate if you can
- Test the control

- Example: Who should setup access in the ERP (Financial Application)?
  - https://www.learnsecurity.org/single-post/2019/01/15/who-should-setup-access-in-the-erp-financial-application

Reminder: Effective Internal Control

Favorable *control environment*

Periodic *risk assessment*

Effective *control activities*

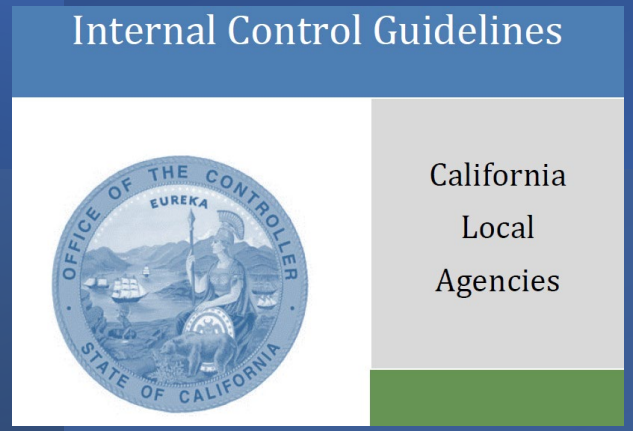
Effective *information and communication*

Ongoing *monitoring*

ADDITIONAL RESOURCES

SCO's Internal Control Guidelines

"…to assist local agencies in establishing a system of internal control to safeguard assets and prevent and detect financial errors and fraud."



Provides guidance

Suggestions NOT requirements

http://www.sco.ca.gov/Files-AUD/2015_internal_control_guidelines.pdf

Thank You!

Image Sources

- https://blog.volkovlaw.com/wp-content/uploads/2018/03/ic_Fotor.jpg
- https://www.sco.ca.gov/pubs_guides.html