IT Control Environment & Financial Reporting

Donald E. Hester, Maze & Associates
Ron Puccinelli, City of Fairfield

Donald E. Hester

CISA, CISSP, CRISC, CAP

Director, Maze & Associates

DonaldH@MazeAssociates.com

www.LearnSecurity.org

Ron Puccinelli

CIO

City of Fairfield

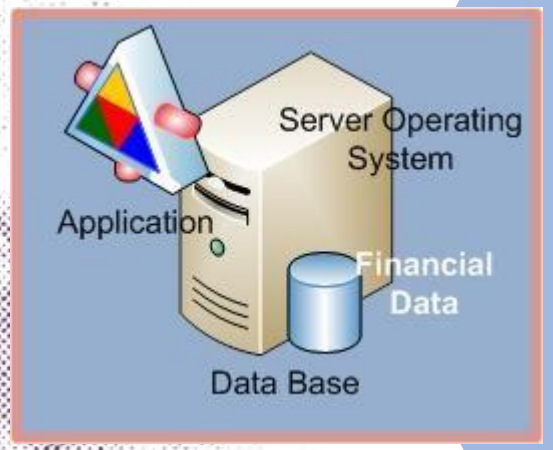
rpuccinelli@fairfield.ca.gov

Common Questions

From the audit field. - What questions do you have?

- What is the IT Control Environment?
- How do we demonstrate due diligence?
- Who should setup users in the financial application, IT or finance staff?
- How do we know IT is doing the right thing?
- How does a cloud financial application effect the control environment?
- Are we PCI Compliant?
- Others
  - Should IT Report to Finance Director?
  - Do we have enough IT staff?

The IT and Financial Control Environment



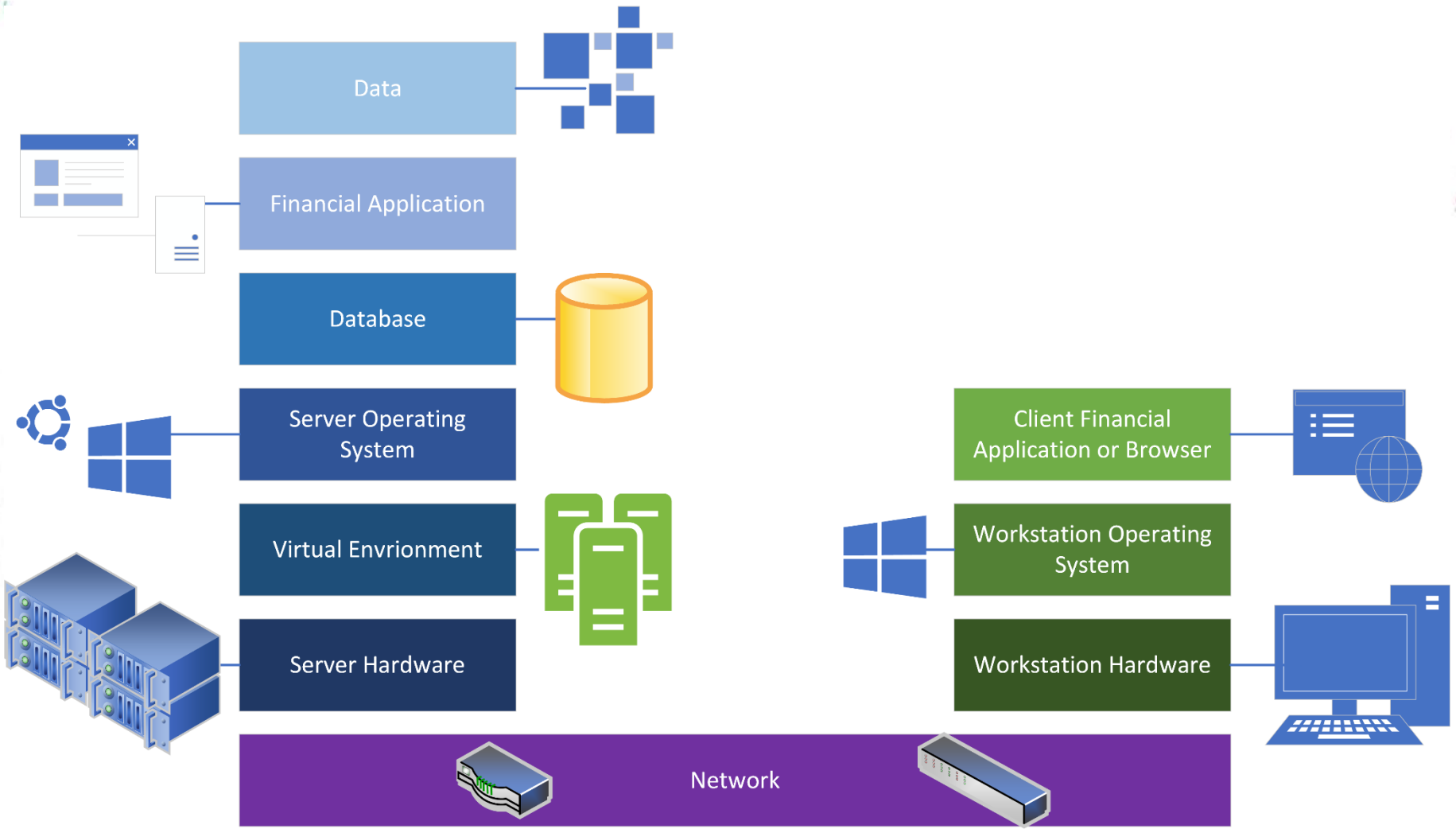
IT Control Environment (ITCE)

Financial Control Environment (FCE)

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

IT Control Environment

Preview



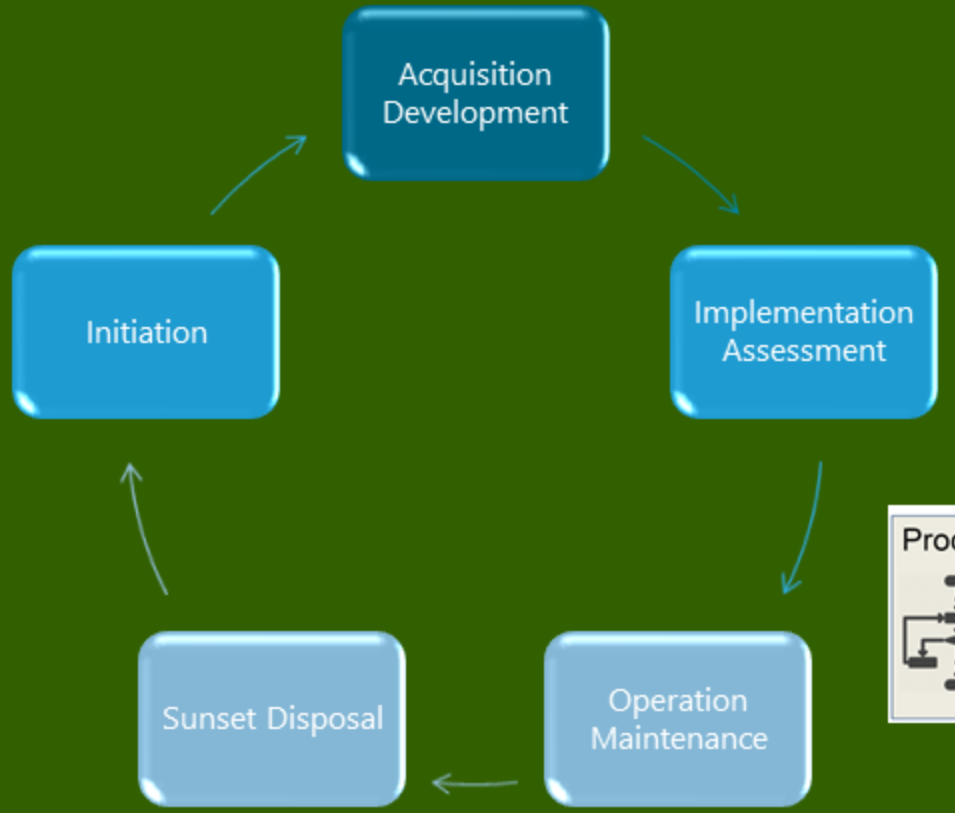
Most business processes rely upon information technology at some point

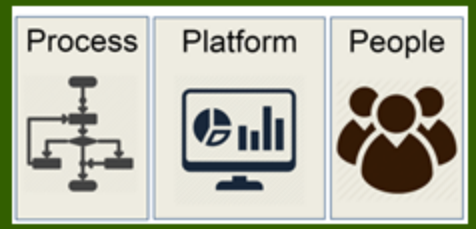
IT Governance is Critical to Demonstrate Due Diligence

IT Governance

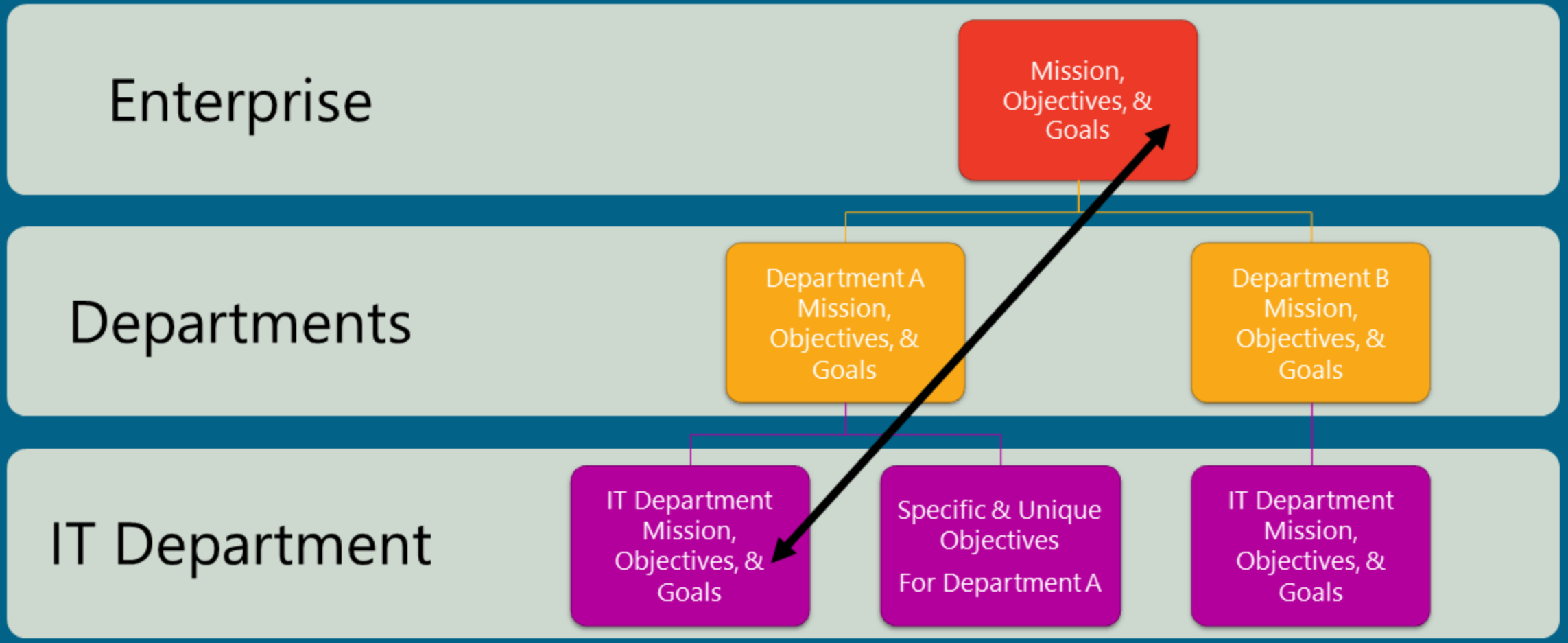
- Governance Framework
- Benefits Delivery
- Risk Mitigation
- Resource Optimization
- Transparency

IT Management





Cascading Alignment



What process do you use to provision user accounts on the financial application?

What process do you use to provision user accounts on the financial application?

Who provisions the accounts?

A user with administrative or root privileges on the financial application could:

- Make changes to account permissions
- Create fake accounts
- Change security parameters
- Delete event/audit logs
- Create or modify vendors
- Can do any function
- Hide their actions

Account Provisioning

Can you spot the weakness of this process?

Provisioning

Provisioning
- New user account
- Set Permissions
- Change of Permissions

By
- Finance Dept.

No Separation of Duties
From IT Admin functions

Account Provisioning

Can you spot the weakness of this process?

Provisioning

Provisioning
- New user account
- Set Permissions
- Change of Permissions

By
- Finance Dept.

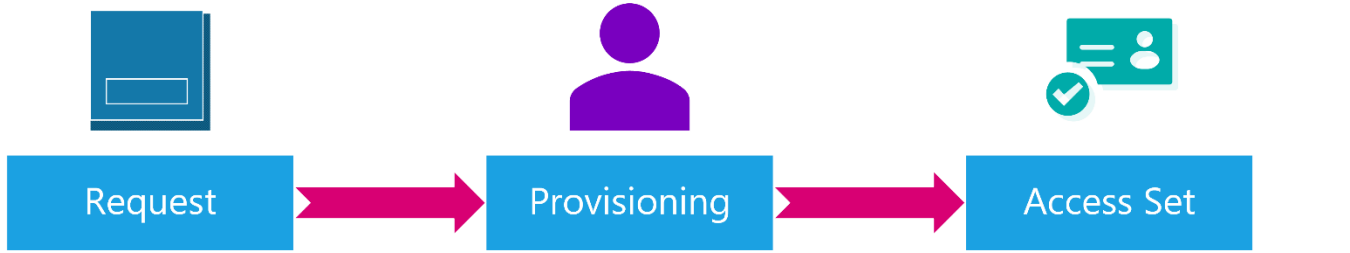
No Separation of Duties
From IT Admin functions

Pro
- Easy to implement

Con
- No separation of duties
- No review process
- Must rely heavily on FCE
- Person in finance is always on the suspect list

Account Provisioning

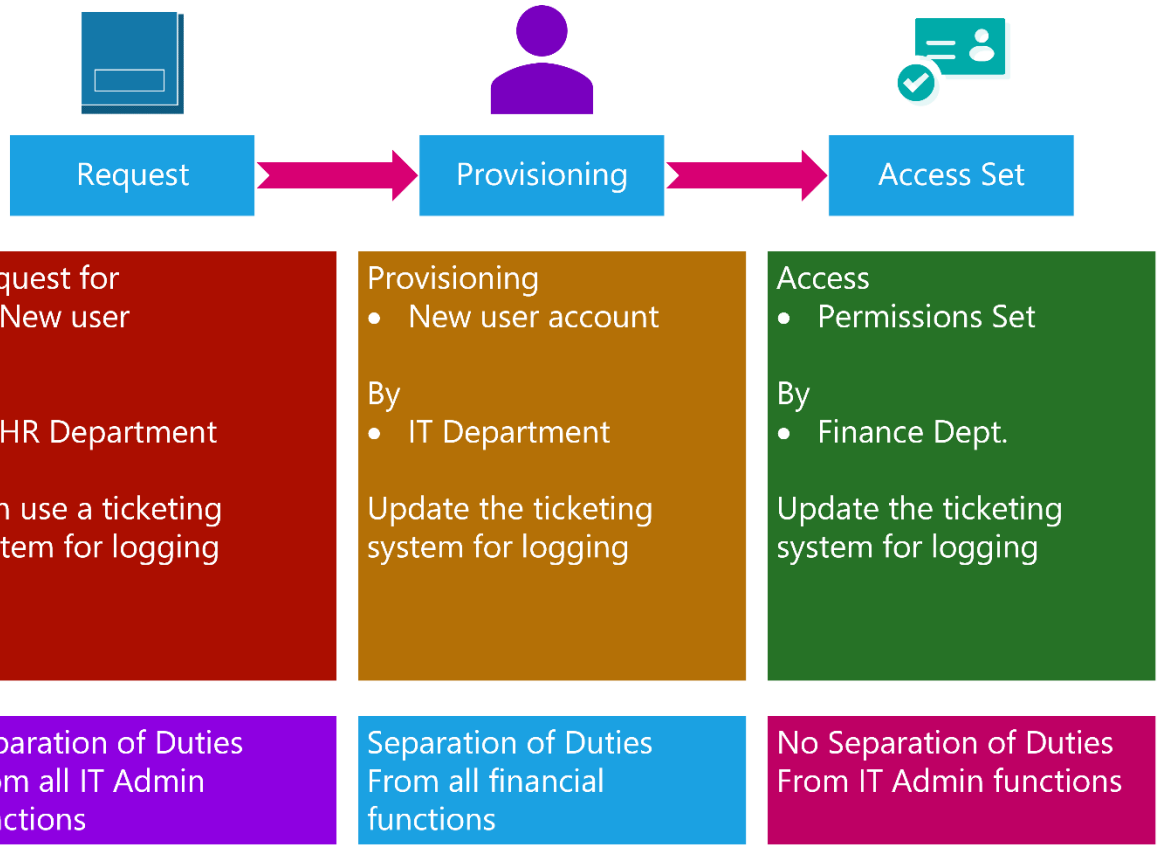
Can you spot the weakness of this process?



Request	Provisioning	Access
Request for • New user By • HR Department Can use a ticketing system for logging	Provisioning • New user account By • IT Department Update the ticketing system for logging	Access • Permissions Set By • Finance Dept. Update the ticketing system for logging
Separation of Duties From all IT Admin functions	Separation of Duties From all financial functions	No Separation of Duties From IT Admin functions

Account Provisioning

Can you spot the weakness of this process?



Pro

- It takes two people to create an account and provision
- Prevents someone in finance from creating a fake account
- IT can create an account but not grant permissions

Con

- Finance can still change permissions
- No review process
- Person in finance is on suspect list

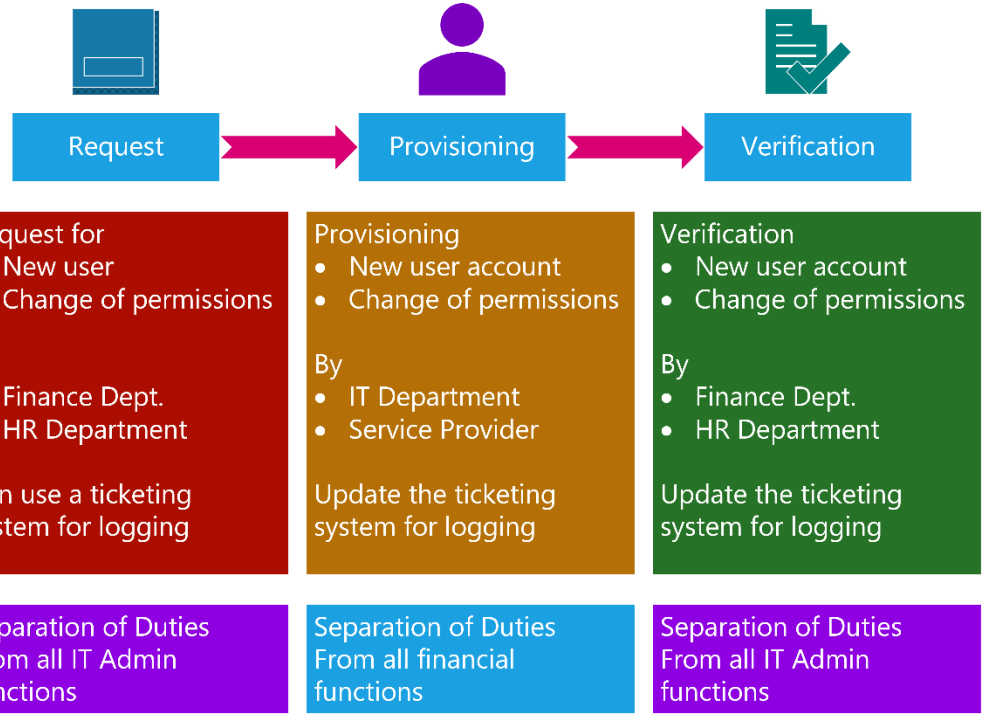
Account Provisioning

Can you spot the weakness of this process?

Request	Provisioning	Verification
Request for • New user • Change of permissions By • Finance Dept. • HR Department Can use a ticketing system for logging	Provisioning • New user account • Change of permissions By • IT Department • Service Provider Update the ticketing system for logging	Verification • New user account • Change of permissions By • Finance Dept. • HR Department Update the ticketing system for logging
Separation of Duties From all IT Admin functions	Separation of Duties From all financial functions	Separation of Duties From all IT Admin functions

Account Provisioning

Can you spot the weakness of this process?



Pro

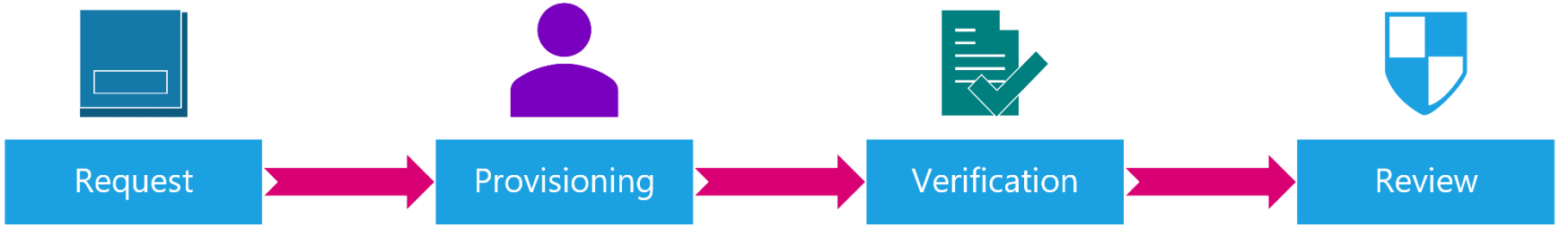
- Good separation of duties
- Review for known permission changes or added accounts

Con

- IT can create an account or change permissions without knowledge of finance
- No review process for unknown changes
- IT is on suspect list

Account Provisioning

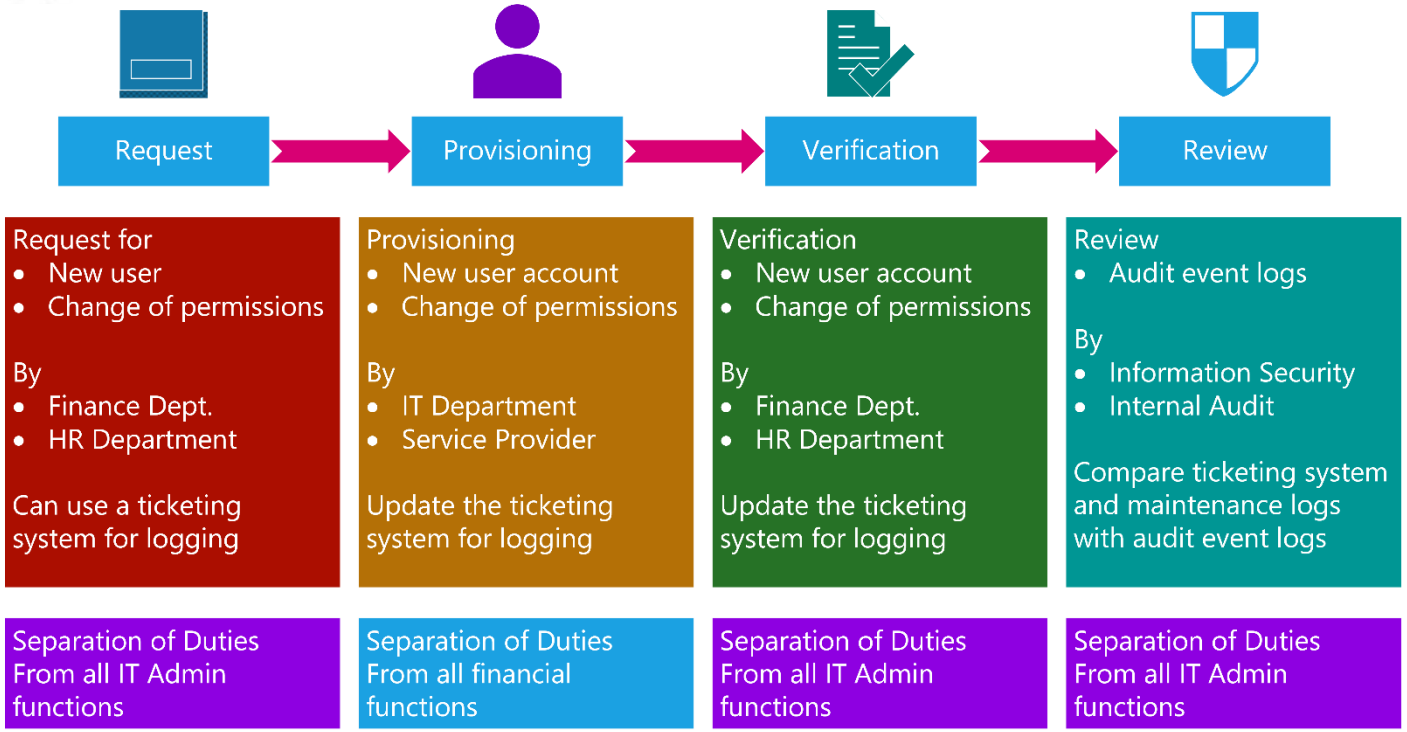
Can you spot a weakness in this process?



Request	Provisioning	Verification	Review
Request for • New user • Change of permissions By • Finance Dept. • HR Department Can use a ticketing system for logging	Provisioning • New user account • Change of permissions By • IT Department • Service Provider Update the ticketing system for logging	Verification • New user account • Change of permissions By • Finance Dept. • HR Department Update the ticketing system for logging	Review • Audit event logs By • Information Security • Internal Audit Compare ticketing system and maintenance logs with audit event logs
Separation of Duties From all IT Admin functions	Separation of Duties From all financial functions	Separation of Duties From all IT Admin functions	Separation of Duties From all IT Admin functions

Account Provisioning

Can you spot a weakness in this process?



Pro

- Good separation of duties
- Review for known permission changes or added accounts
- Unknown changes caught
- No one is a suspect

Con

- Difficult to implement

How do you know what IT staff or service provider has done on the financial application?

IT Administrator or service provider can:

- Duplicate the financial app
- Write directly to the raw DB
- Make changes to account permissions
- Create fake accounts
- Change security parameters
- Delete event/audit logs
- Create or modify vendors
- Can do any function
- Hide their actions
- Introduce malware

Transparency with IT

Trust but Verify

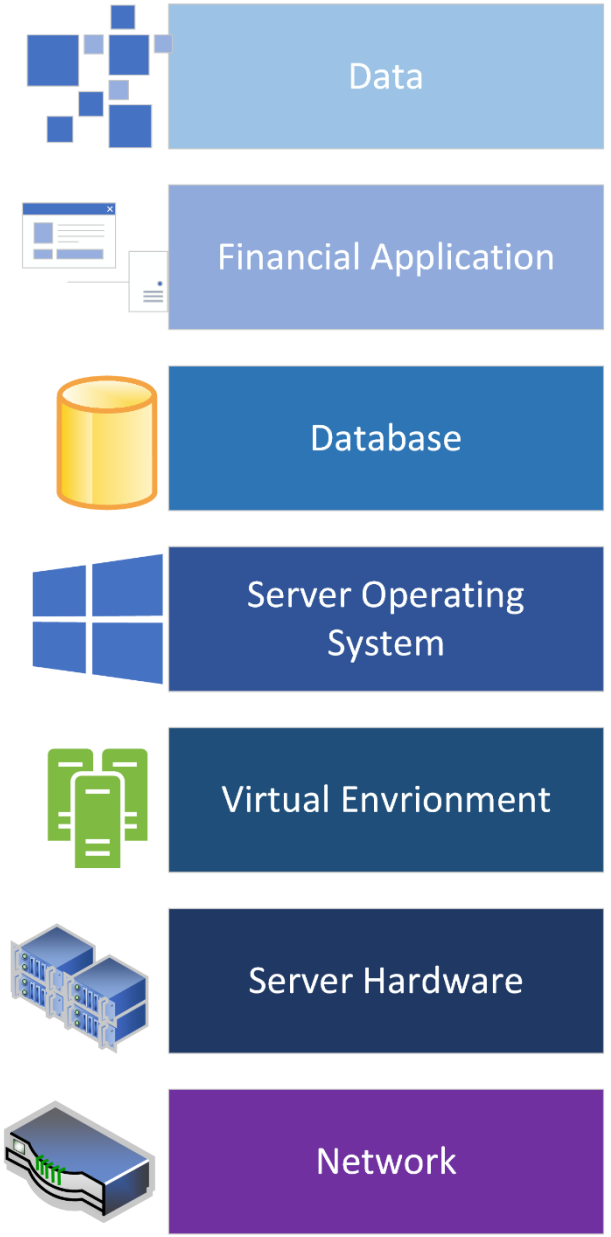
Access to data can be denied
Data can be corrupted
Data can be disclosed

Information can be extracted or inserted directly into a data base. (e.g. Add vendors)

A clone of the Financial application can be made easily in virtual environments. (e.g. Nefarious acts covered up)

Eavesdropping on network traffic. (Capture passwords, print jobs etc.)

Logs on Financial application are not enough.
Logs are needed at all levels and separated from IT admins.
Who reviews the logs? How often? Do you know what you are looking at?



Transparency with IT (Cont.)

Trust but Verify

Financial controls still play a part

Limit access to check stock

Positive Pay

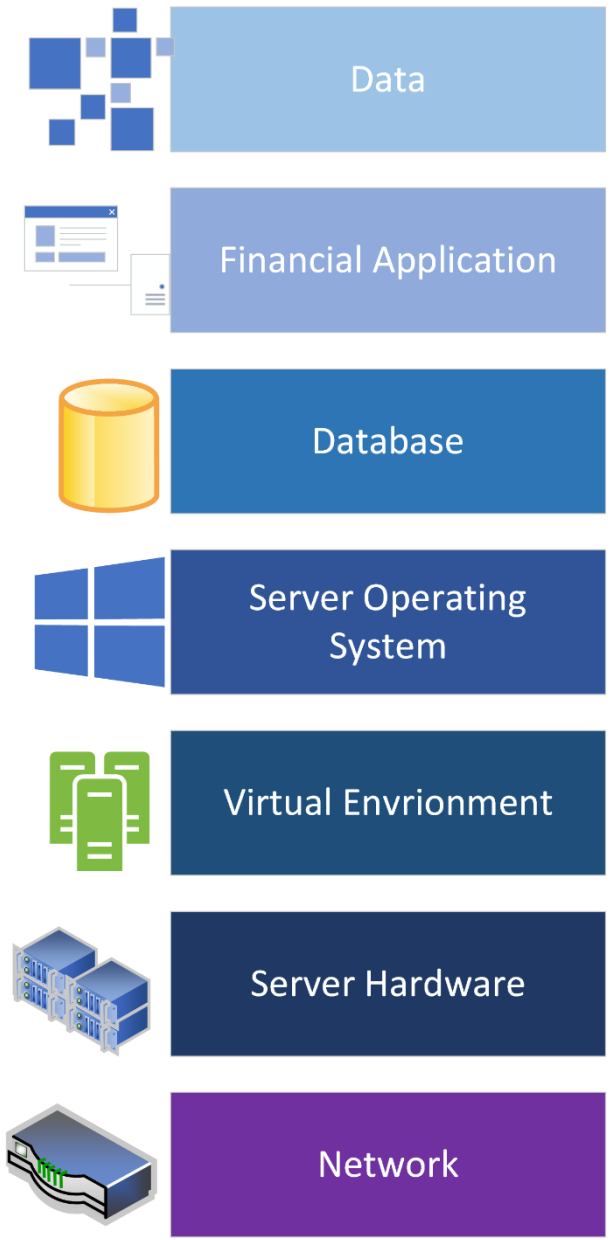
Two step approval for wire transfers

Timely reconciliations

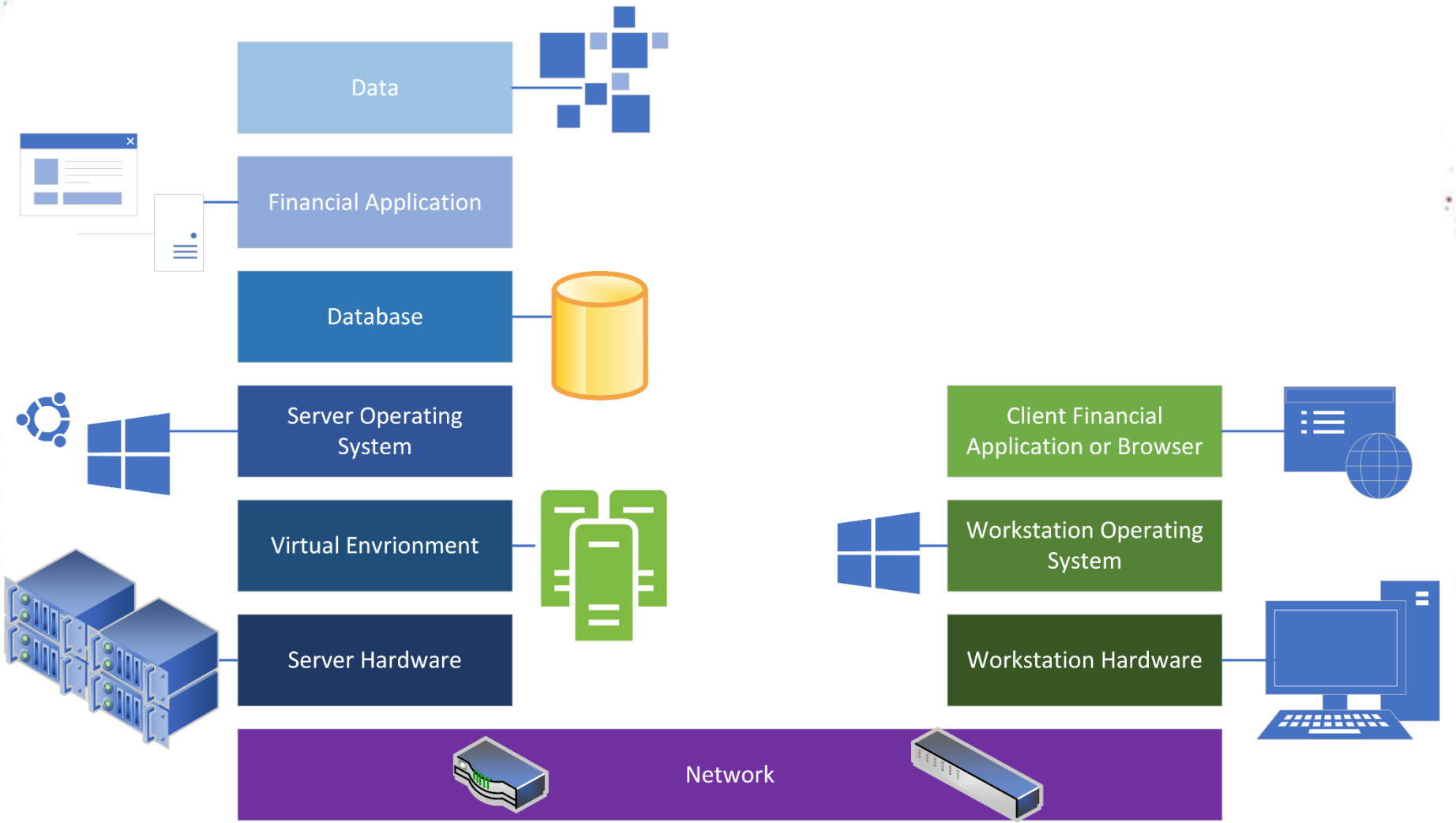
Review user accounts and permissions regularly

Review audit logs

Independent audit/assessment of IT control environments



IT Control Environment



Critical IT Controls

Criticality depends on how much you rely on information technology for control.

- Most business processes rely upon information technology at some point
- Do you rely on IT controls?
  - Access control (user accounts)?
  - Backups?
  - Calculations?
  - Error Handling?
  - Information Input Validation?

- Common Controls
  - Access Control
  - Business Continuity
  - Audit and Accountability
  - Identification and Authentication
  - System Development
  - Communication Protection
  - System and Information Integrity
- Compliance Requirements
  - PCI DSS

What about Cloud based financial systems?

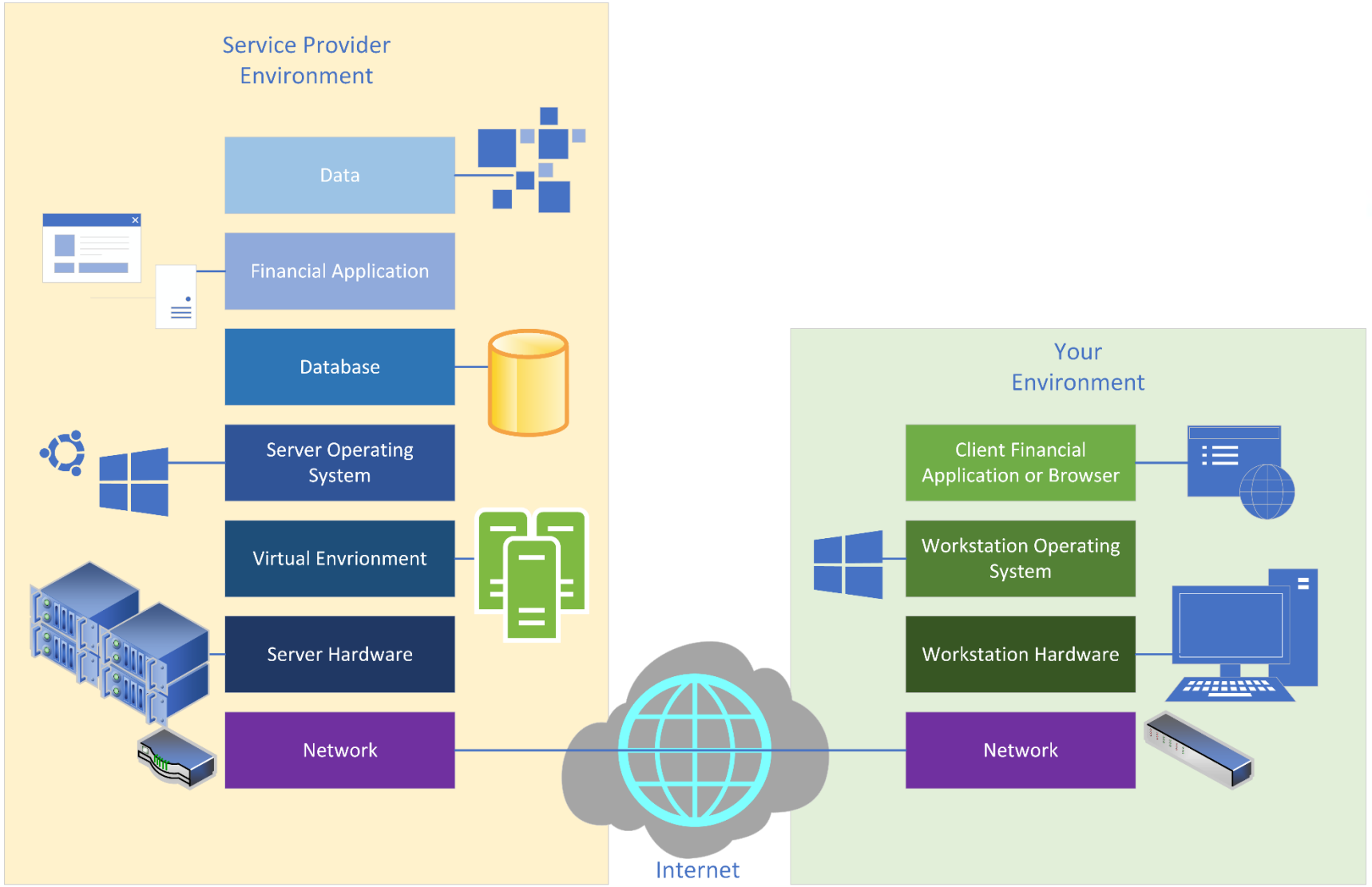
Cloud Service Provider

Financial application hosted offsite

- What controls do you need to worry about?
- You have all the same risks
- The difference is who is managing the IT control environment
- You have the service provider and your IT staff
- Both control part of the IT Control environment
- Complexity varies depending on the solution
- Hybrid solutions (often used for disaster recovery)
- Cloud service provider may be using another 3rd party

Cloud Service Provider

Financial application hosted offsite



Critical IT Controls For Cloud Services

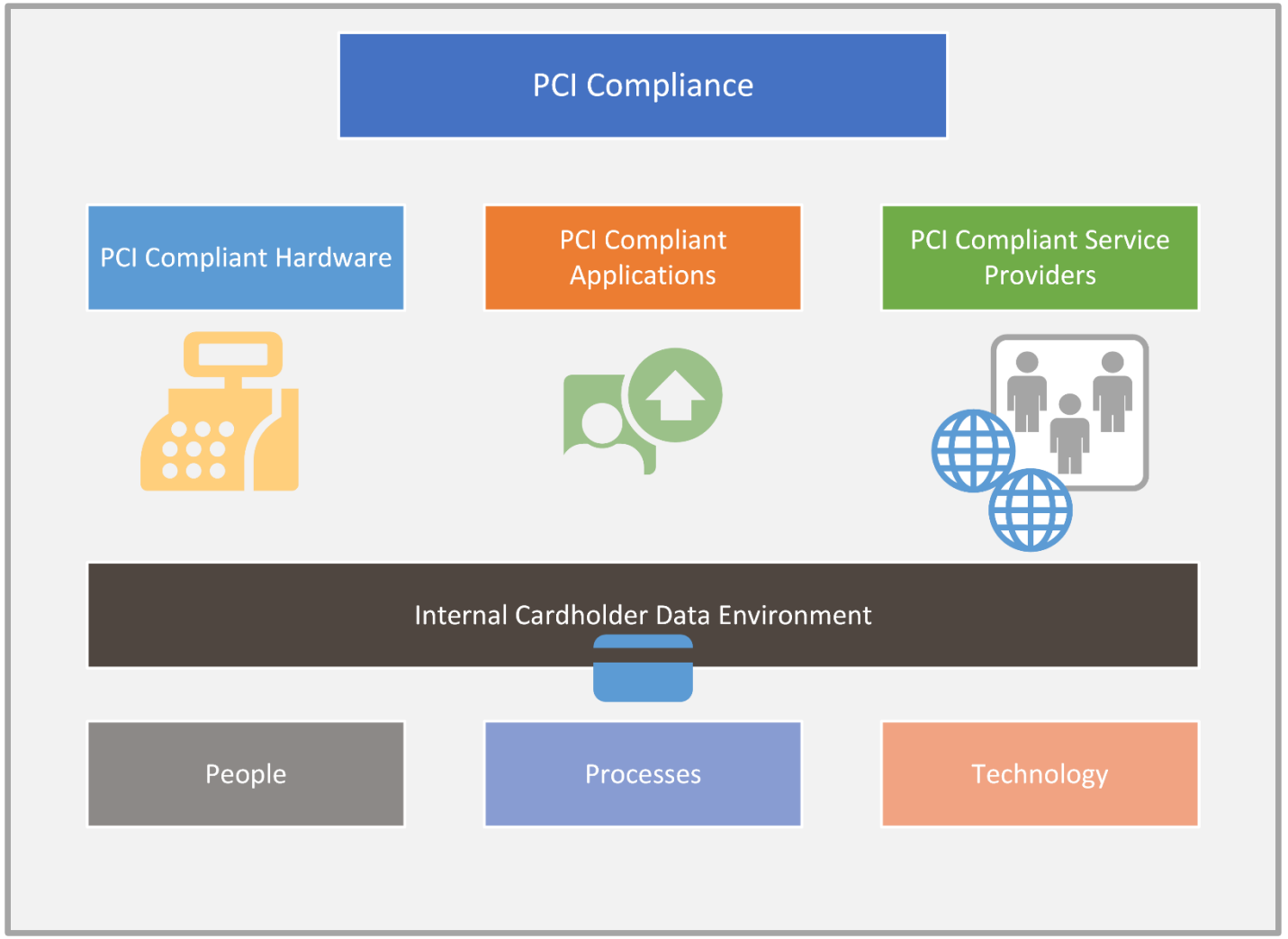
Criticality depends on how much you rely on information technology for control.

- Third Party Service Provider Risk Assessment
- Annual Risk Assessment
- Additional Compensating Controls
- Service Level Agreement
- Breach Notification
- Timely Breach Notification
- Transborder Data Flow and Storage
- eDiscovery, Litigation Hold, Forensics
- Audit Review (i.e. SSAE16)
- Disengagement Process

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

Are you PCI Compliant?

PCI Compliance is complex for Local Governments



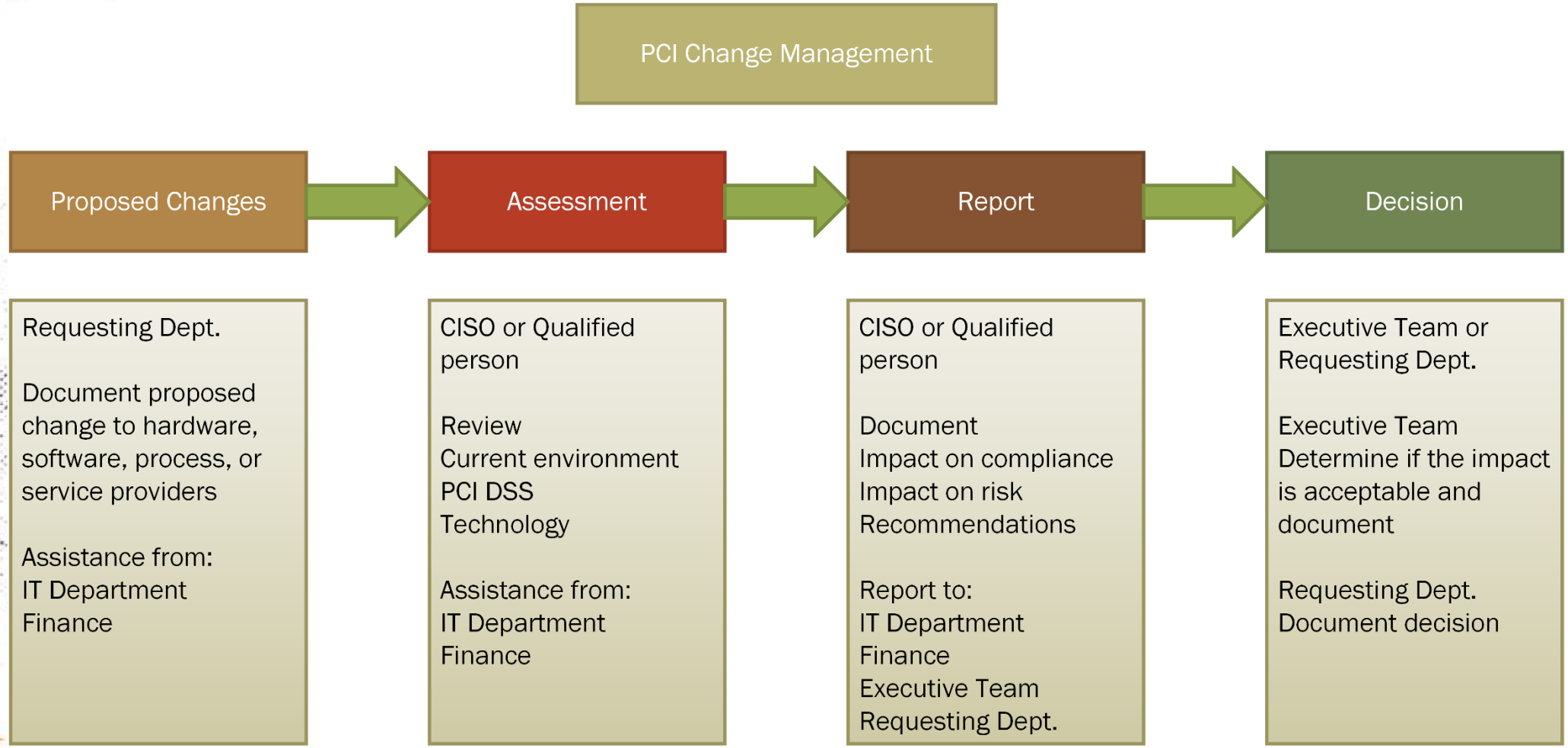
Common PCI Issues

From the Audit Field

- City staff thinks they are compliant because the app or hardware they use is PCI compliant
  - PCI Compliance requires compliant hardware, apps, service providers as well as internal processes and technology
- The left had does not know what the right hand is doing
  - Different departments choose payment acceptance hardware, software, and services without an assessment of the overall impact to the City
- Different compliant hardware solutions have different impacts on compliance
  - One hardware solution could limit the CDE, reduce risk, and cost of compliance
  - Another hardware solution may increase the CDE, increase risk, and cost of compliance
- Finance staff is not aware of all the way the City accepts payments
- Cashiers
  - Cashiers are not trained annually
  - Cashiers do not have consistent payment acceptance processes
- Physical Security

PCI Compliance Management

From the Audit Field



IT Control Environment & Financial Reporting

Questions?