Global Information Security Society
for Professionals of Pakistan

Certified Information System Auditor

Information Systems Operations and Business Resilience

This course is worth 27 percent of the CISA examination
(about 41 questions)




Instructor Introduction

Muhammad Saquib Malik

EMBA (LUMS) – In progress
MS Information Security
Certified Information Security Manager (CISM)
Certified Information Security Auditor (CISA)
Project Management Professional (PMP)
Certificate of Cloud Security Knowledge (CCSK)
Certificate of Cloud Auditing Knowledge (CCAK)
Privacy and Data Protection Foundation (GDPR)
IRCA Certified ISO 27001 Lead Auditor (ISMS)
Certified Information Technology Infrastructure Library (ITIL)
Certified EC-Council Instructor (CEI)
Certified Ethical Hacker (CEH)
Certified Hacking Forensics Investigator (CHFI)
Certified Secure Computer User (CSCU)
Certified Administrator for IBM Qradar

Part A: Information Systems Operations

- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-user Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release and Patch Management
- IT Service Level Management.
- Database Management

Part B: Business Resilience

- Business Impact Analysis
- System Resiliency
- Data Backup, Storage and Restoration
- Business Continuity Plan
- Disaster Recovery Plans

Part A: Information Systems Operations

Overview

Ensure understanding and provide assurance that the processes for information systems operations, maintenance, and service management meet the organization's strategy and objectives.

Information System Management

Adequate allocation of resources

Authorizing and monitoring resource usage

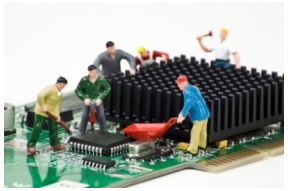
Ensuring compliance with understanding

Information System Operations

Scheduling

Authorizing changes

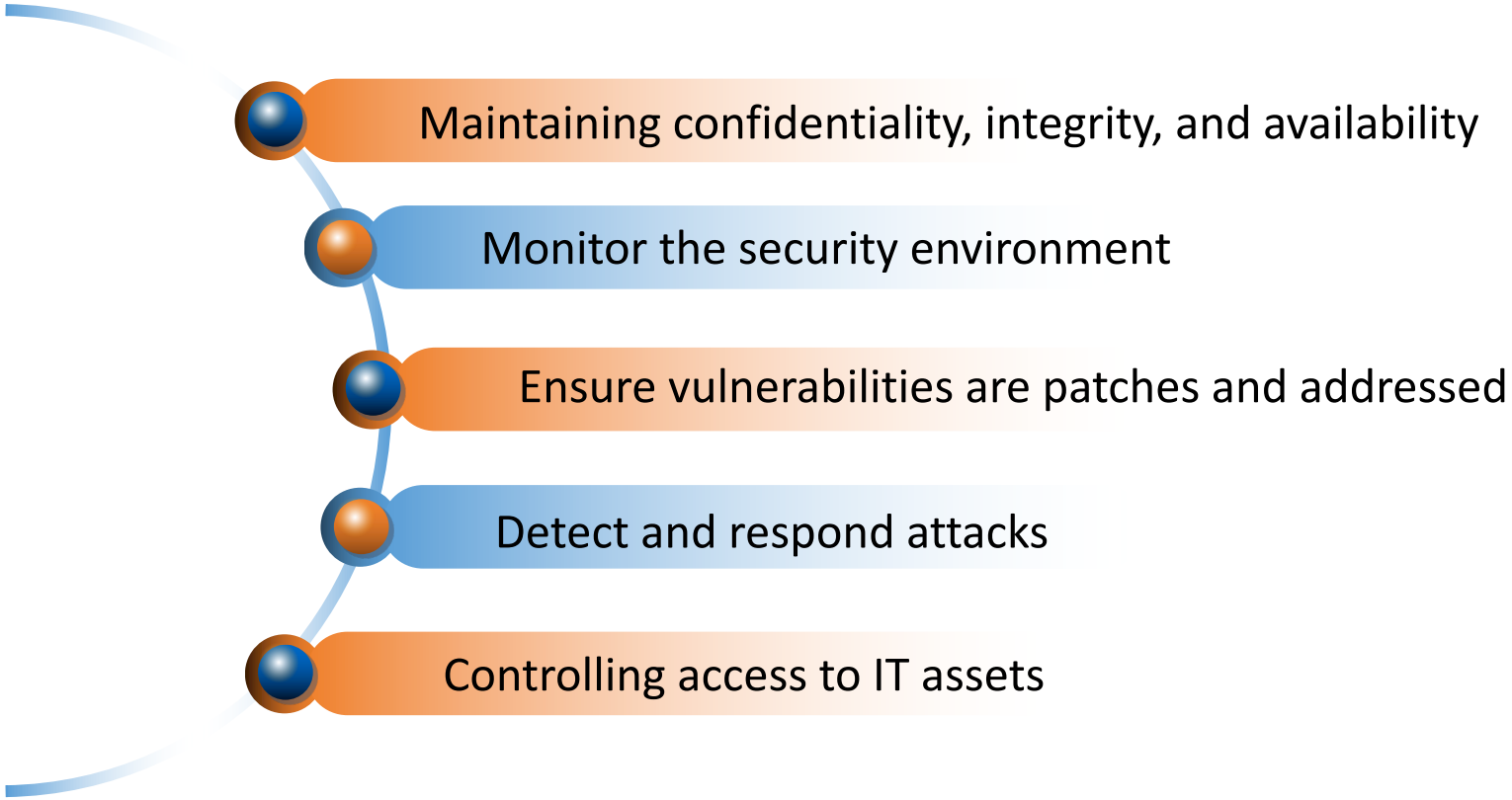
Monitoring system performance / reviewing logs



Maintaining equipment's

Handling incidents and recovery

Information Security



IT Service Levels

Service Level Agreement (SLAs)

- Create expectations and requirement for service levels
- Ensure clients understand what it promised
- Make service delivery level measurable
- Set forth rules of changes to, and operation of, system

Measure Service Levels

Exception reports
May indicate systemic problems

System and Application logs
Appropriate data access

Operator Problem Reports
Appropriate operator actions

Operations Work Schedules
Adequate staffing

Monitoring Service Level for Third Party Providers

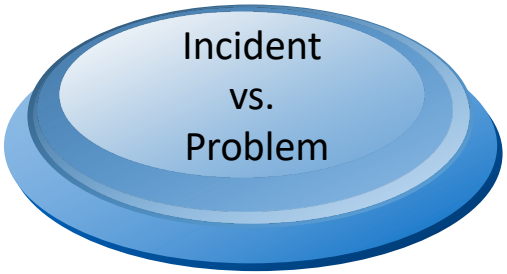
Ensure service providers meet SLAs.

Right to audit third parties or SSAE16 / SAAE3402 reports

Review operational reports and exceptional reports

Review change logs

Incident Management vs. Problem Management



An incident is a non-standard operation that has the potential to disrupt business mission

Incident management is the process of continuing operations or resolving an interruption

A problem is an underlying root cause of a series of incidents or major incident

Problem management is based on root cause analysis and fixing the core issue.

Maintenance of an Error Log

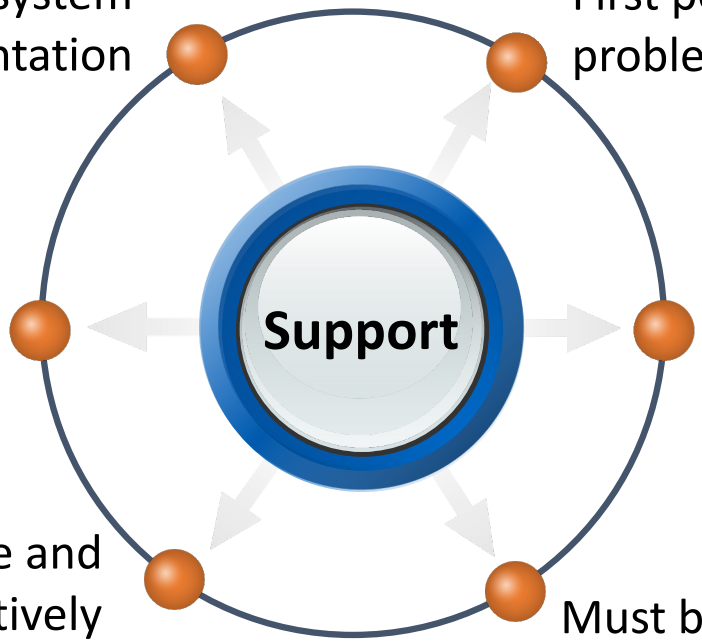
Errors and exceptions should be logged in order to track their resolution

Log entries should be complete with all detail needed to investigate the error

Management should ensure that the errors are addressed and resolved in a timely manner

Once resolved the log entry should be marked as complete

Help Desk



Maintain system documentation

First point of contact for users with problems or concerns

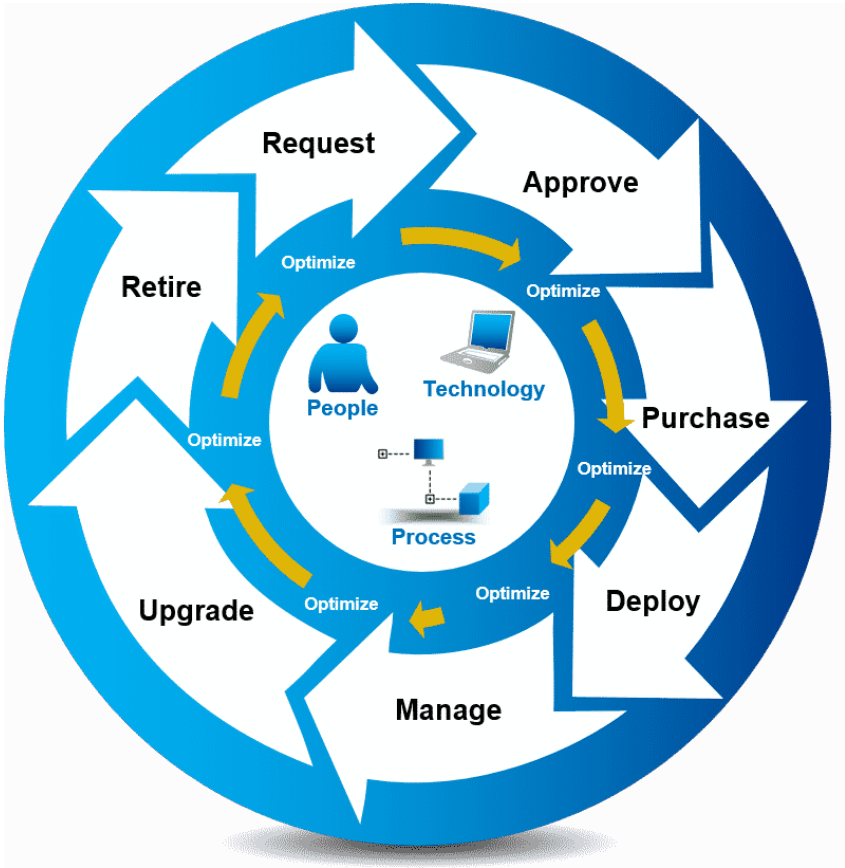
Produce logs on requirement

Often the first to be aware of an outage or exception condition

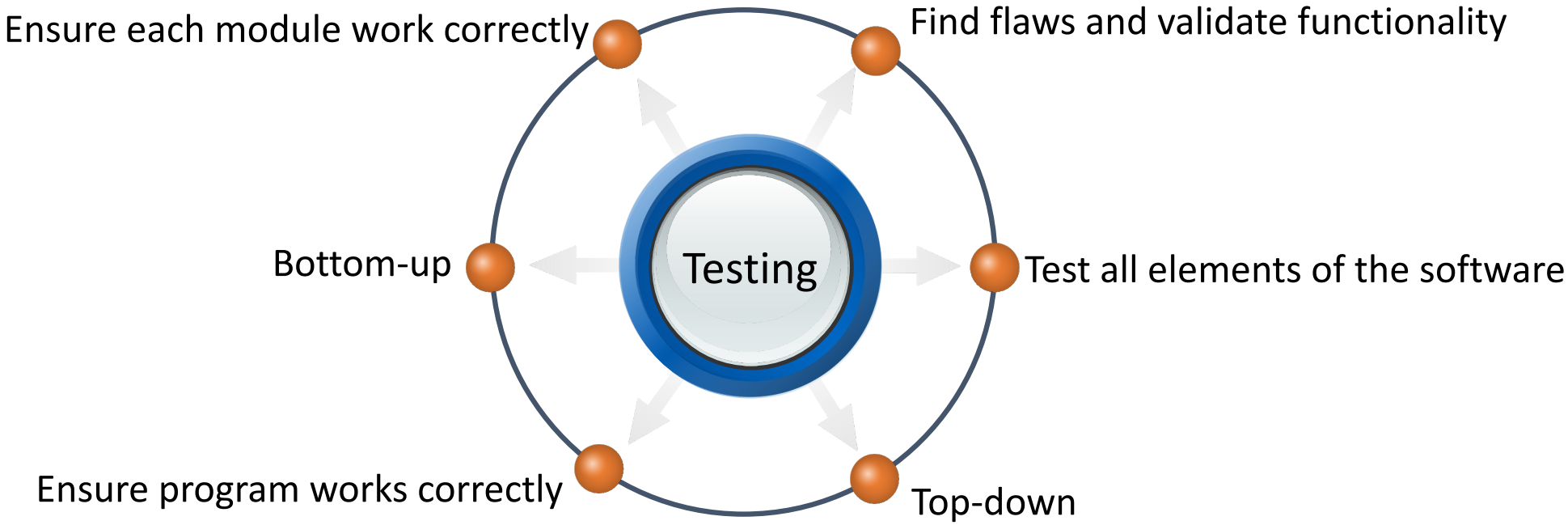
Should communicate and escalate incidents effectively according to incident management process

Must be aware of security concerns

IT Asset Management



Testing Software and Systems



An Asset

Something of tangible or intangible value that is worth protecting.

People

Information

Infrastructure

Finance

Reputation

Asset Inventory

- Specific identification of asset
- Relative value of asset
- Loss implications and recovery priority
- Location
- Security/risk classification
- Asset group
- Owner/custodian

Auditing Information Systems Hardware

- Capacity management
- System Monitoring
- Hardware Maintenance
- Hardware Acquisition

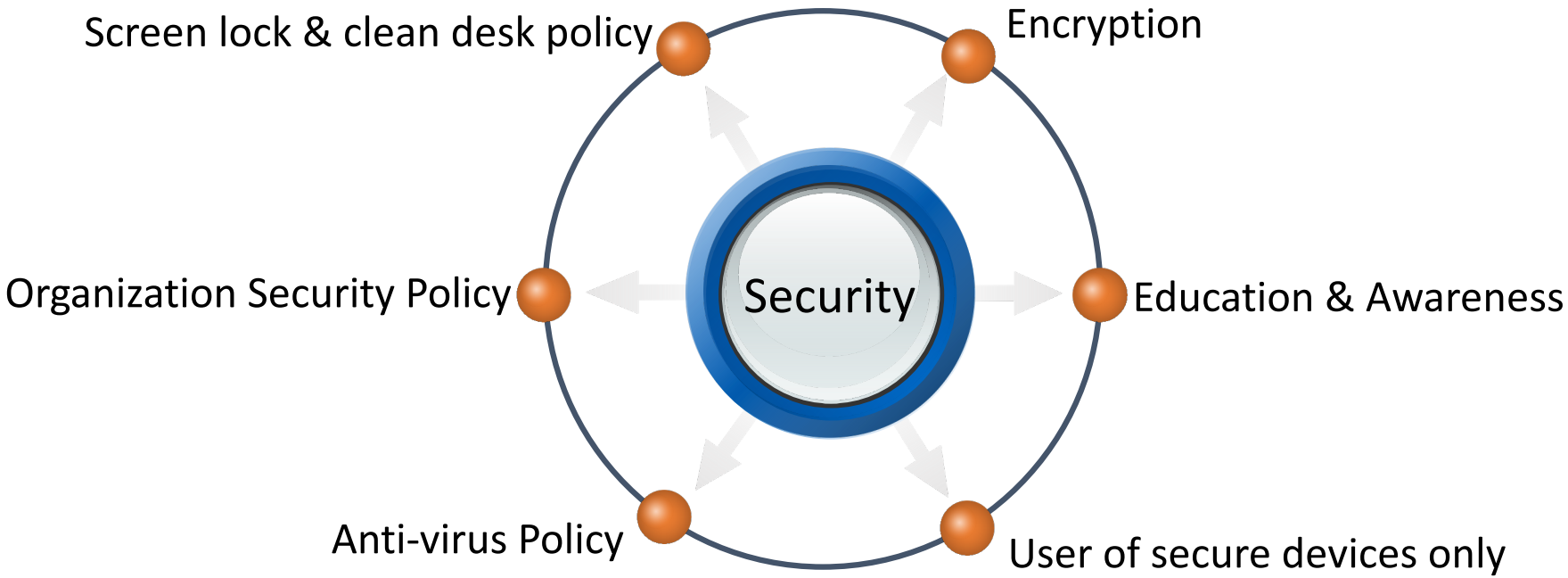
Risk with USB Flash Drive, Storage Drives

Data / Device Theft

System corruption

Data Compromise

Implementing Security

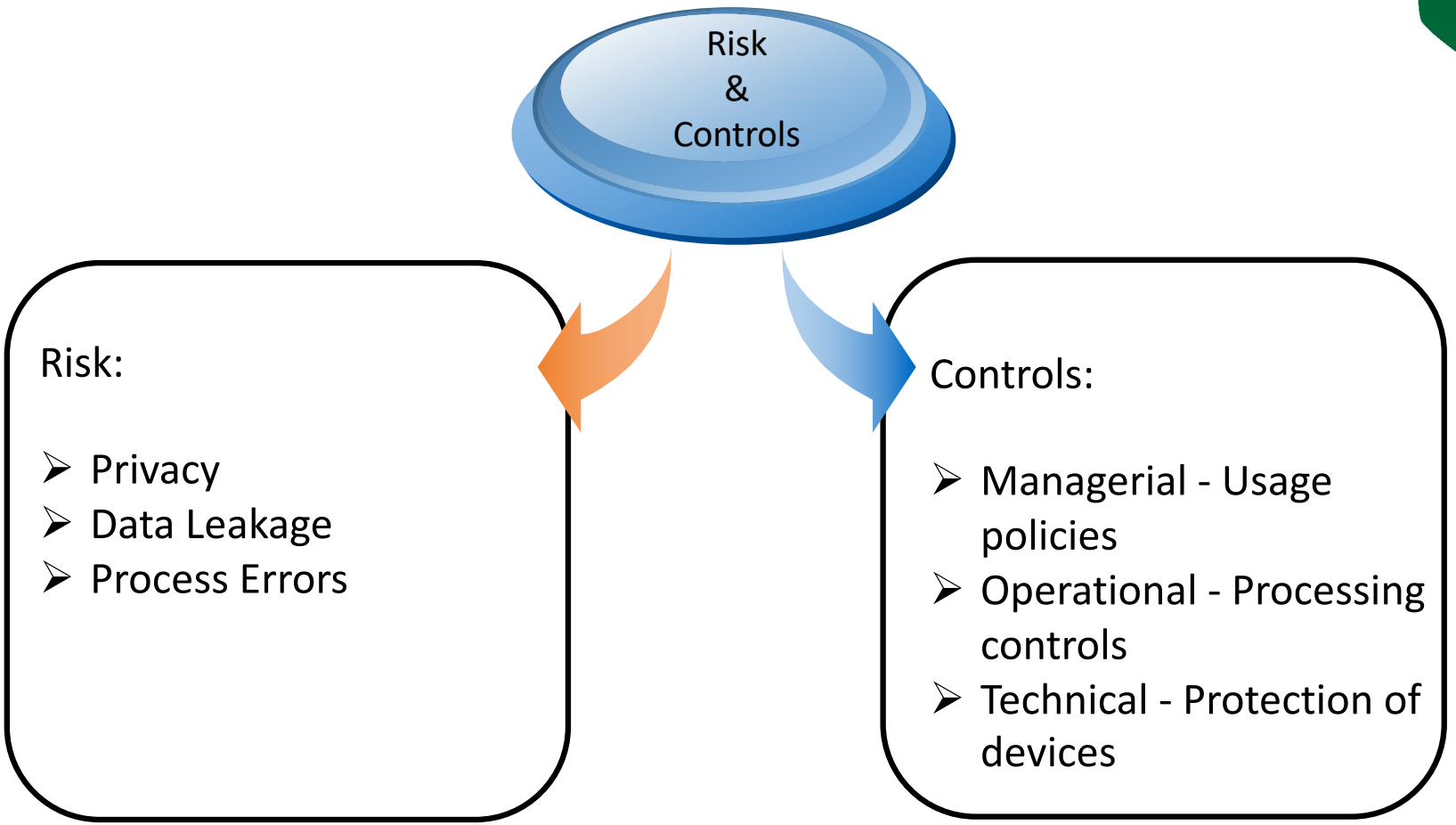


RFID & Uses

Radio Frequency Identification

- Radio waves to identify tagged objects
- Limited range
  - Passive tags
  - Active tags

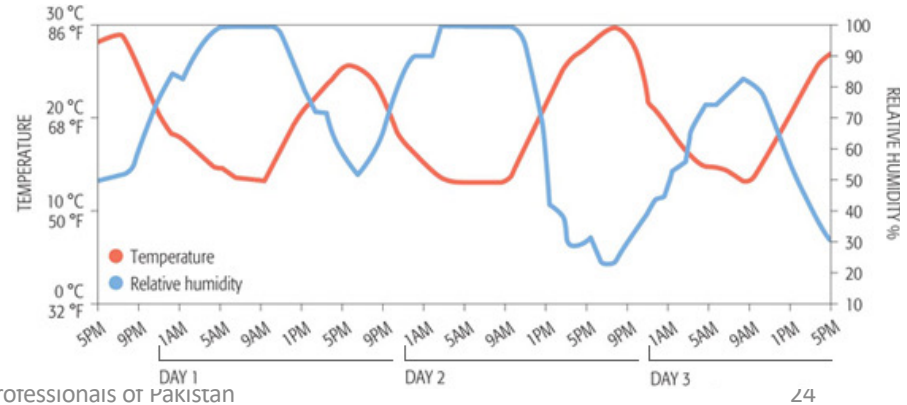
RFID Risk & Controls



Information System Hardware

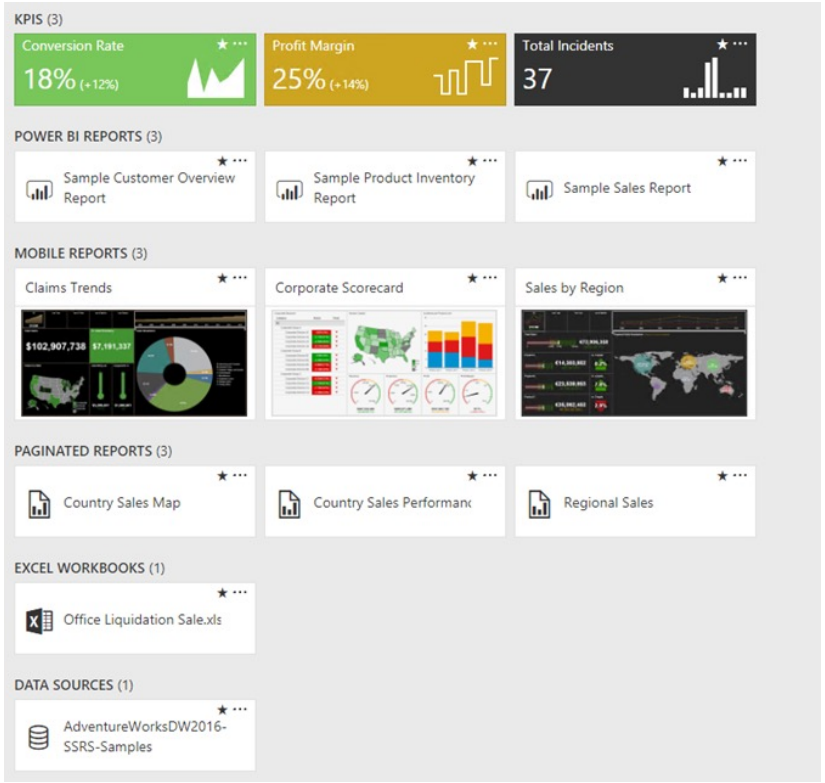
Maintenance of hardware and physical operating environment

- Temperature
- Humidity
- Vendor maintenance
  - Reputable vendor



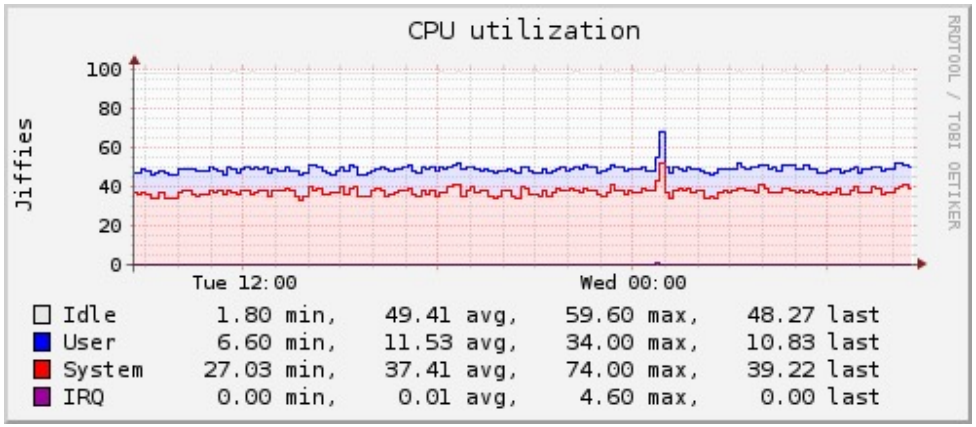
Hardware Monitoring

- Availability reports
- Hardware error and malfunction reports
- Equipment utilization reports
- Asset management and inventory



Capacity Management

- CPU utilization
- Network utilization
- Number of users
- Time to deploy new technologies
- Response time for user requests



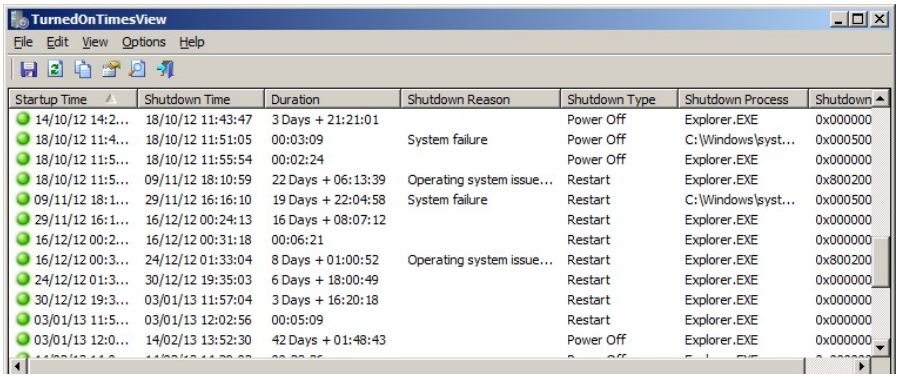
Information System Architecture & Software

Hardware

Software

Logging

- Transaction Logs
- Job reports completion logs
- Network Monitoring
- SIEM Systems
- Incident logs
- Access logs



Risk with Privileged Processes

- Restrict privileged operations to authorized staff
  - Enforce least privilege

- Log all activity
  - To sensitive data/accounts
  - System configuration changes
  - Changes to user permissions
  - Uploads into production

The Data Life Cycle

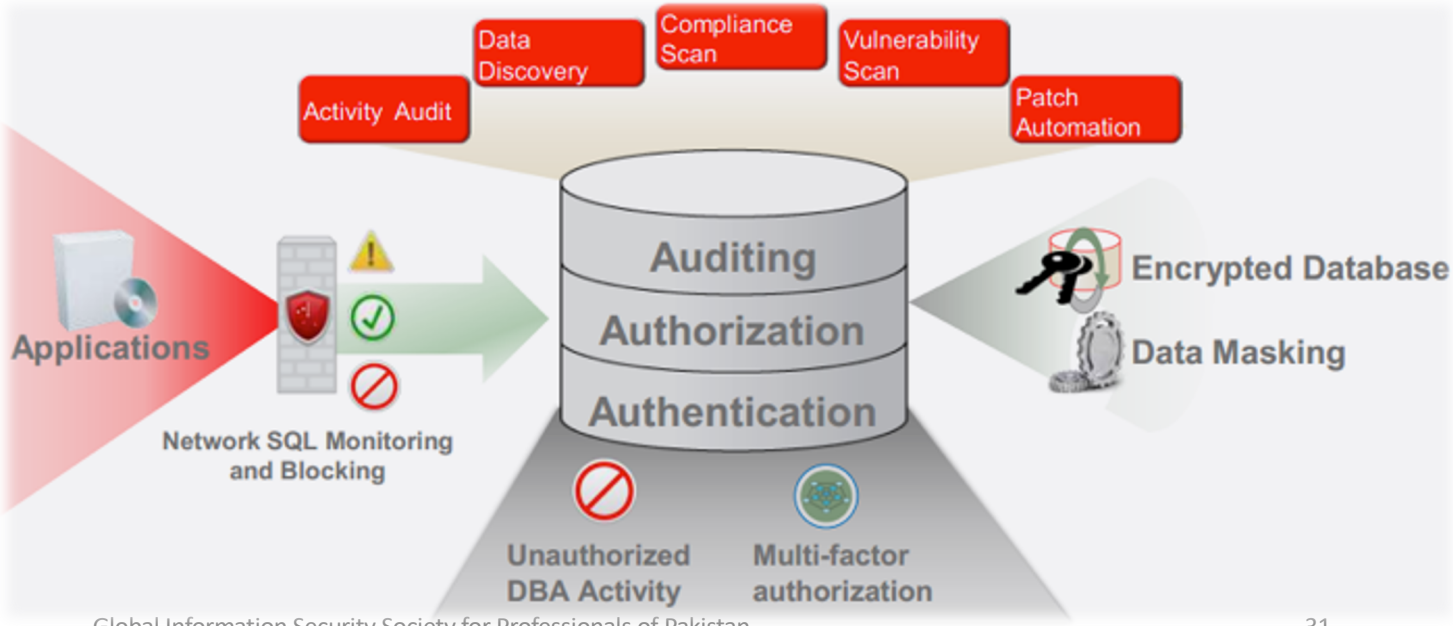
- Plan — identify and determine value of sensitive data - classify
- Design — standards for data format and usage
- Build/acquire — creation or acquisition of data
- Use/operate — store, share, process
- Monitor — maintain data integrity
- Dispose — archive or destroy data

Database & Security

Method to store and access data

- Hierarchical
- Network
- Relational

Protecting the gold of the kingdom



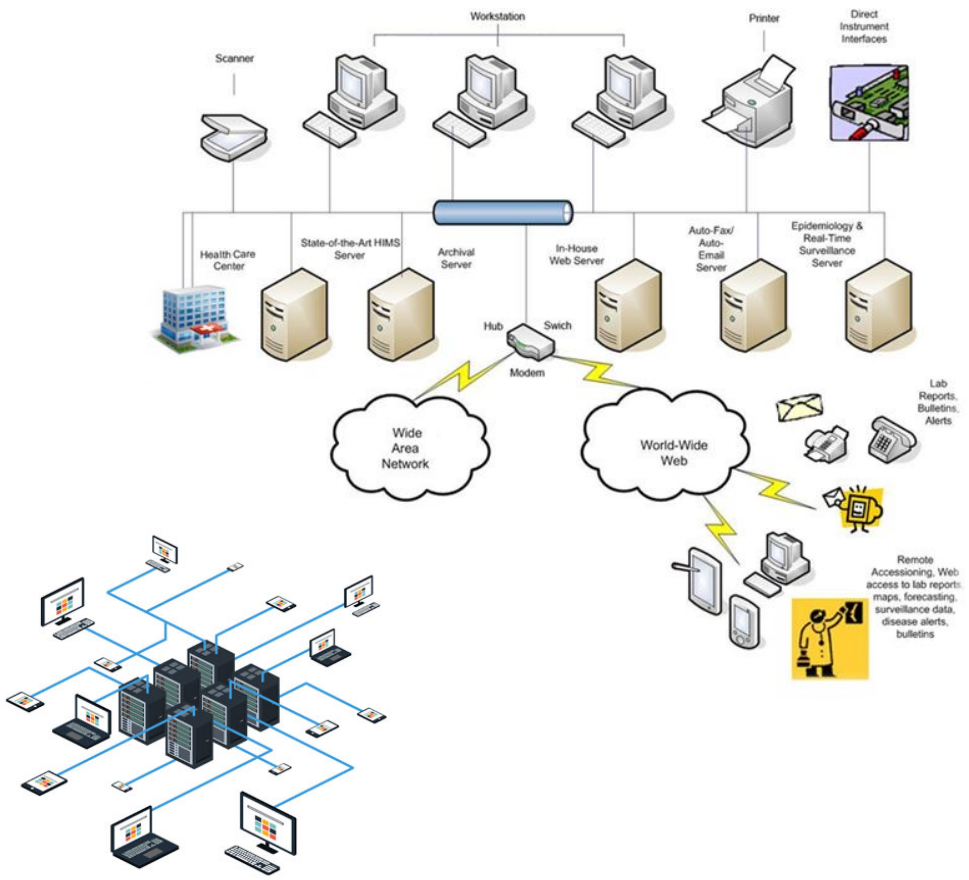
Software Issues

Licensing Escrow

Version Control Documentation

Protection of Source code

Information System Network Infrastructure

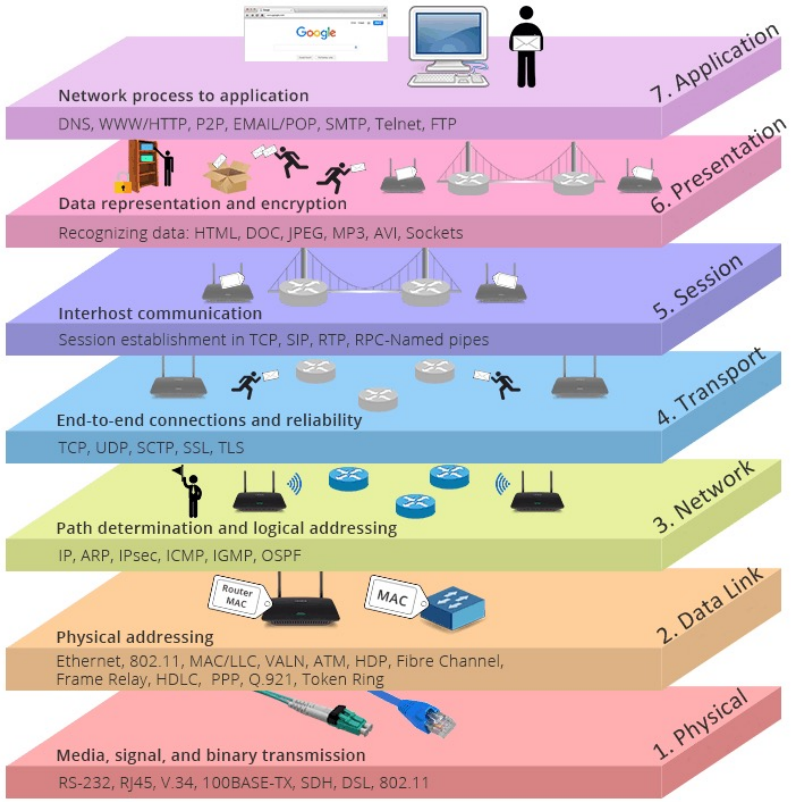


- Dedicated Network
- Circuit Switching
- Packet Switching
- Multi-tiered Networks

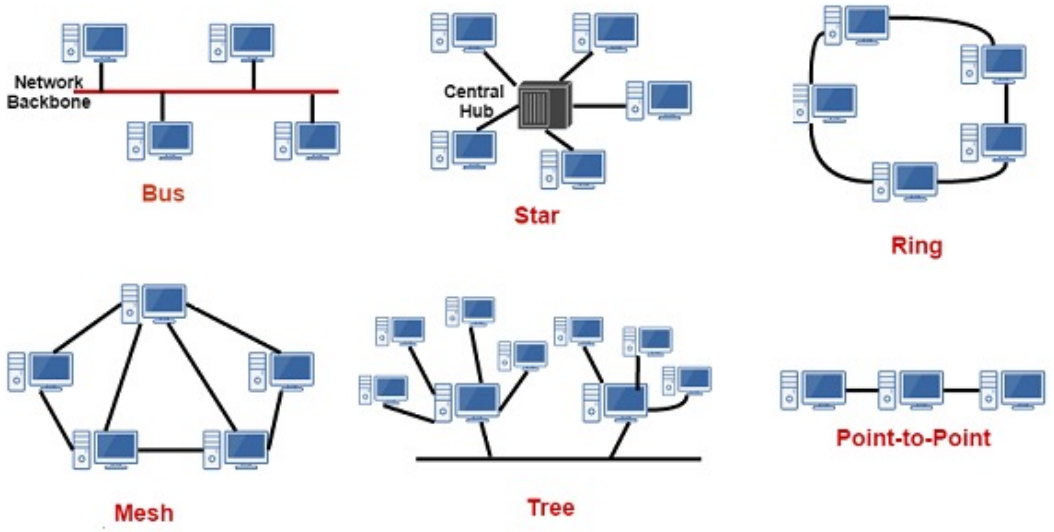
OSI (Open Systems Interconnection)

Developed by International Organization for Standardization (ISO)

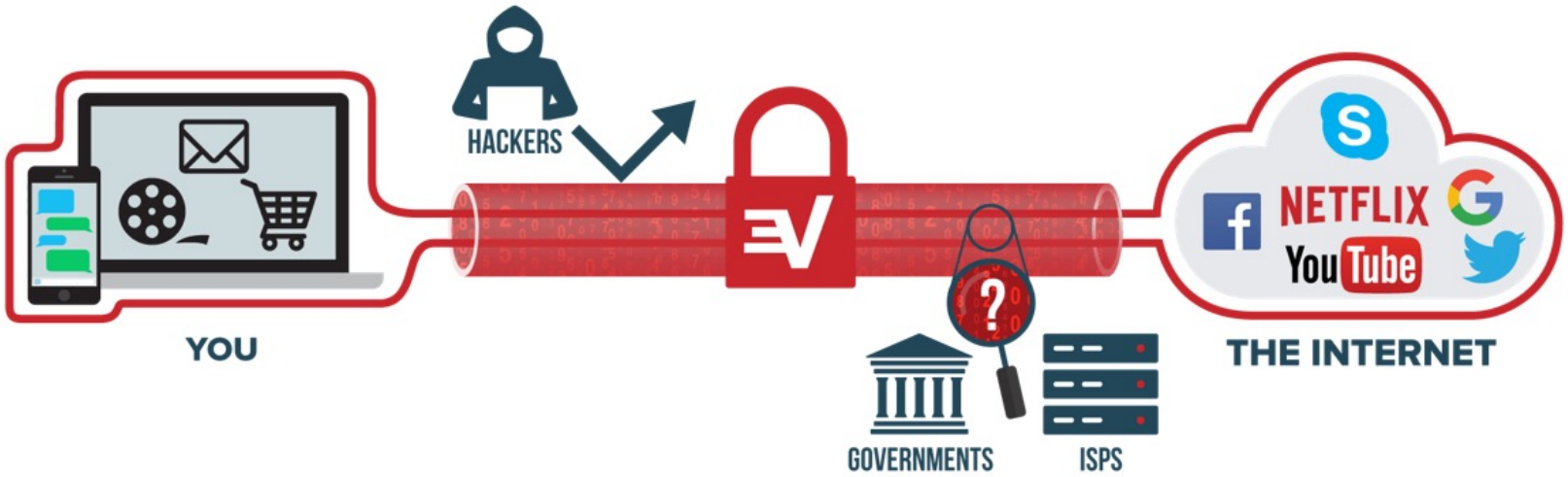
"All People Seem To Need Data Processing"



Network Media & Topologies



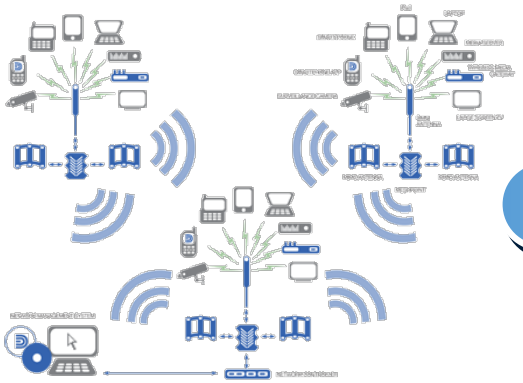
Virtual Private Networks (VPN)



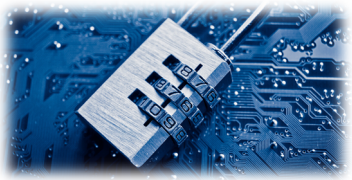
- Encrypted (usually) tunnels to carry traffic through an untrusted network
- Remote access — teleworkers, business partners
- IPSec

WLAN & Security

- Mobile phone
- IEEE 802.11
- Satellite
- WLANs
- Microwave
- IEEE802.16
- WIMAX
- Bluetooth



- WEP
- WPA
- WPA2
- Rouge Wireless AP
- Unsecured WAPs

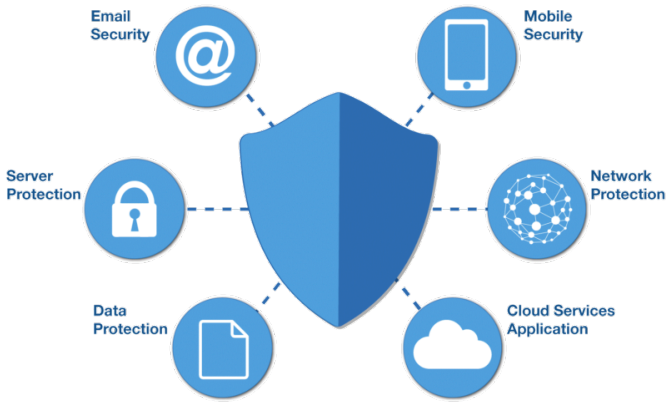


Network Security

Monitoring

Availability - Fault Tolerance

Configuration Management



Auditing Infrastructure and Operations

Auditing Network

Configured Properly

Capacity Planning

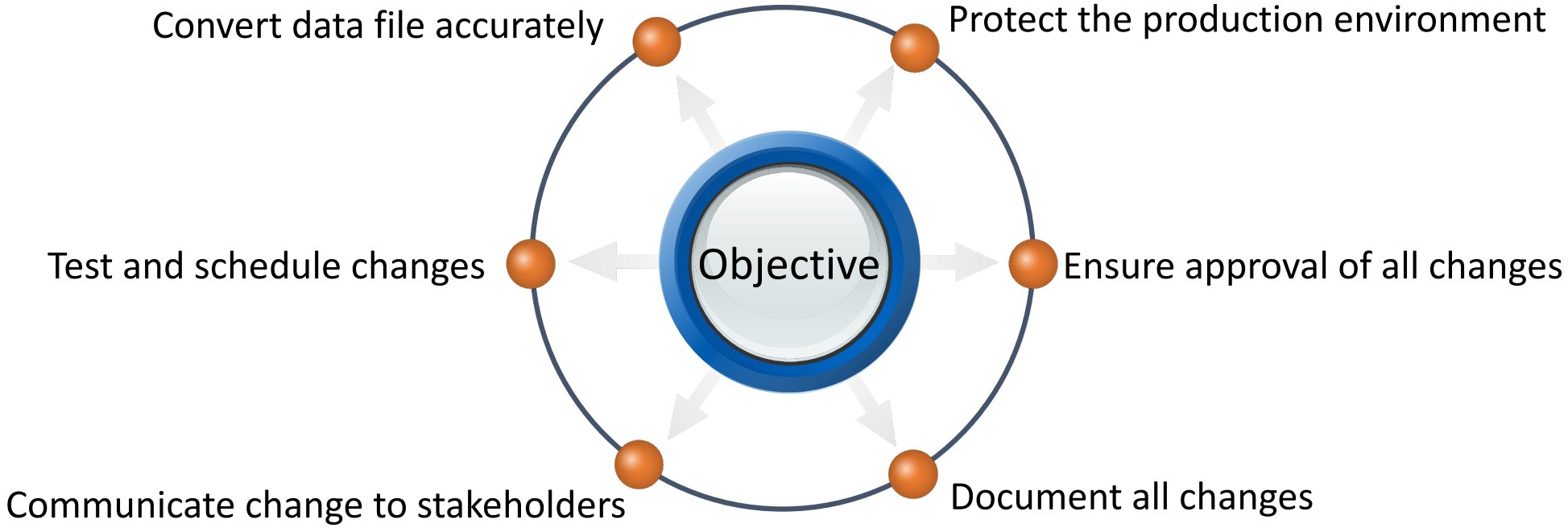
Trained Staff

Change Controls

Controlling changes to IT systems and application through a defined process.

- Request Change
- Authorize Change
- Test Change
- Implement
- Communicate to Users

Change Control Objective



Change Risk

Interruption of business

Bypassing of security controls

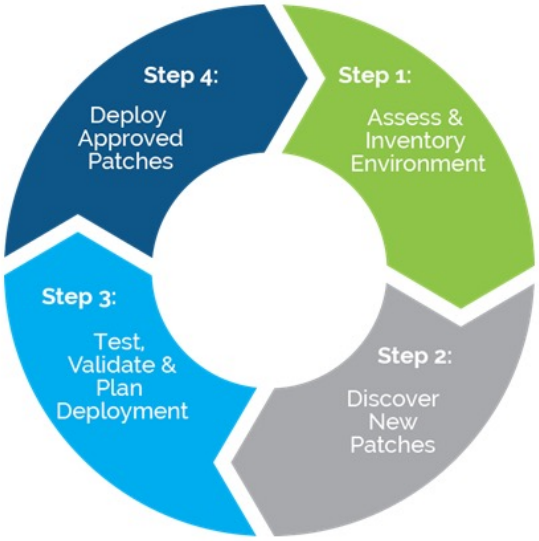
Drop in service quality

Patch Management

Apply upgrades and fixes to systems

Improve software

Address security risks



Patch Management (Part of Change Control Process)

- Be aware of available patches
- Determine which patches are appropriate
- Ensure correct installation
- Document Changes
- Backup Systems
- Test Thoroughly

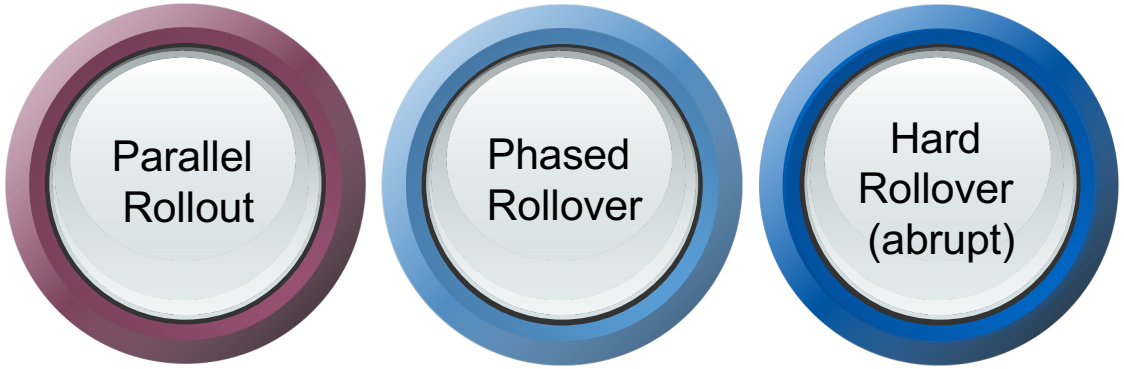
Release Management

A collection of authorized changes to software

Why?

For Enhancements
For Fixes

Rollout of Changes



Frequency of releases


THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
DANKSCHEEN
BIYAN
SHUKRIA
TINGKI
YAQHANYELAY
TASHAKKUR ATU
SUKSAMA
EKHMET
GRAZIE
MEHRBANI
PALDIES
MAAKE
KOMAPSUMNIDA
GOZAIMASHITA
EFCHARISTO
JUSPAXAR
BOLZÏN
MERCI