

IT & IS audit practice areas

By

CA. S. Deephika ACA, DISA, PGP- BABI, CCRA, LIE

Information technology CPE on IT areas

for

SIRC of Institute of Chartered Accountants of India

08th September, 2021

The background is a dark gray with several concentric circles of varying line weights, some solid and some dashed, creating a subtle pattern. A small white triangle points downwards on the left side of the image.

There is no single universal definition of IT audit

Agenda

Overview of IT areas

Specific area of IT audit

Objectives of the engagement

Methodology for execution

Disclaimer

- This is not exhaustive list of areas

Reference framework



ICAI's Technical guide on Information system audit



Manual for Information technology audit from the office of comptroller and auditor general



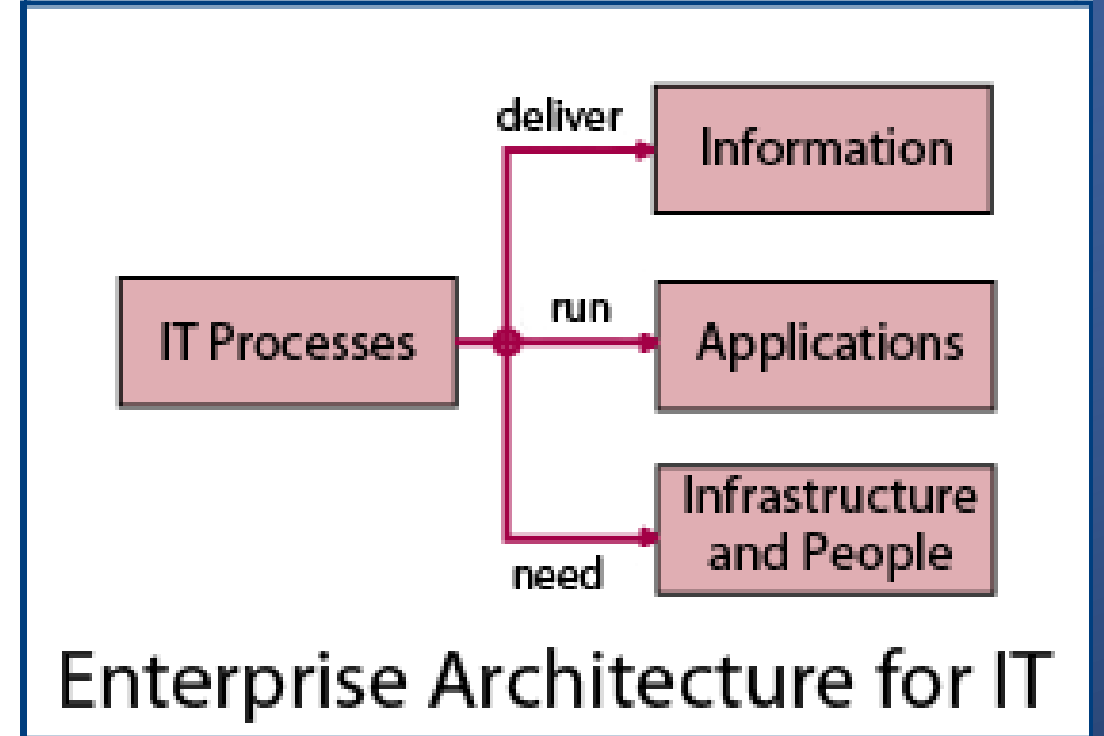
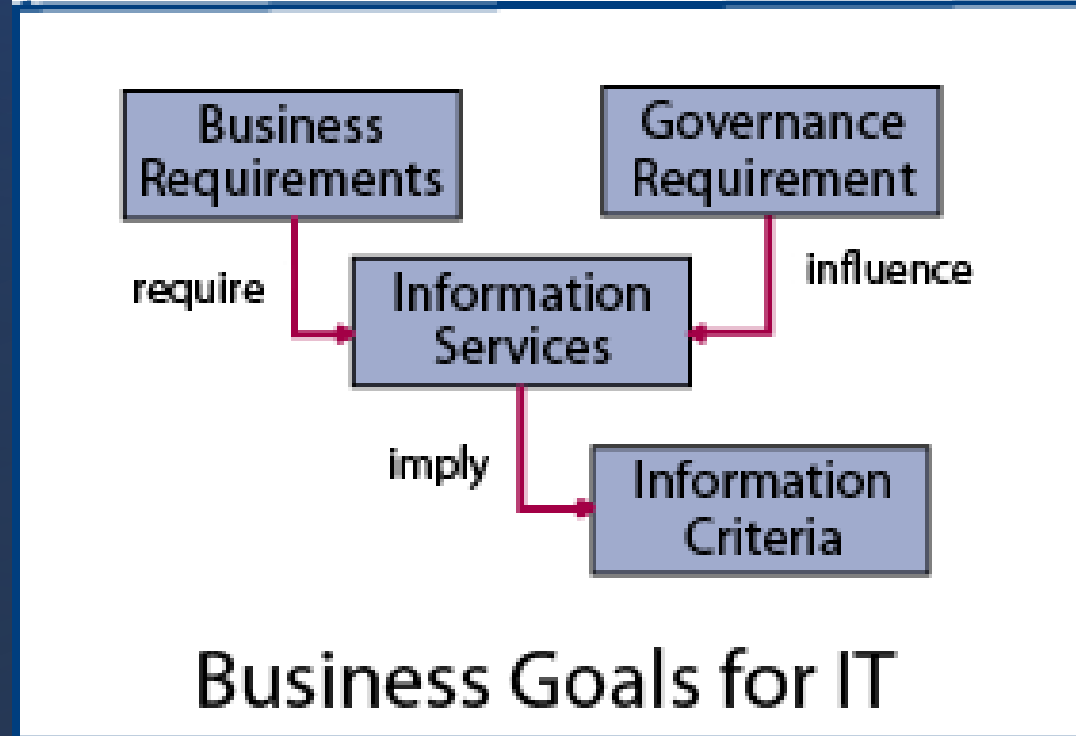
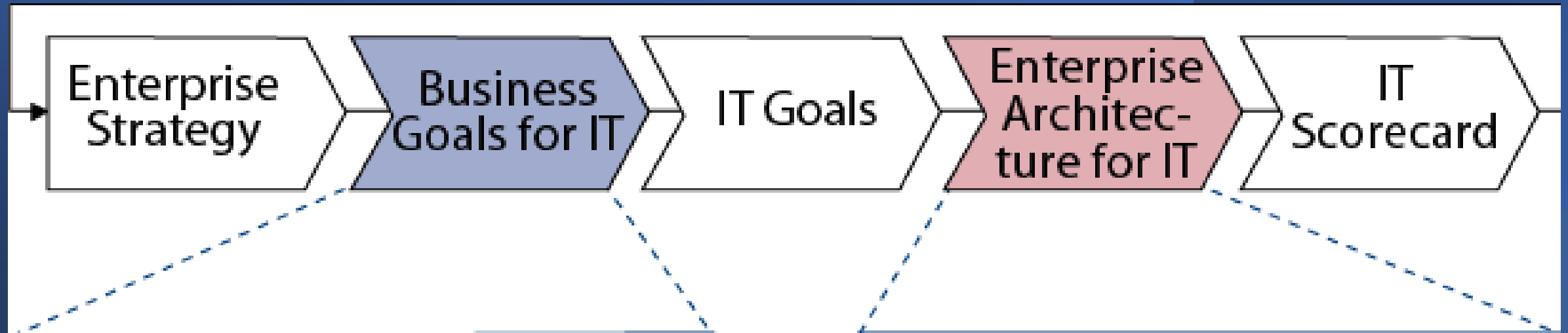
Information Technology audit framework from ISACA

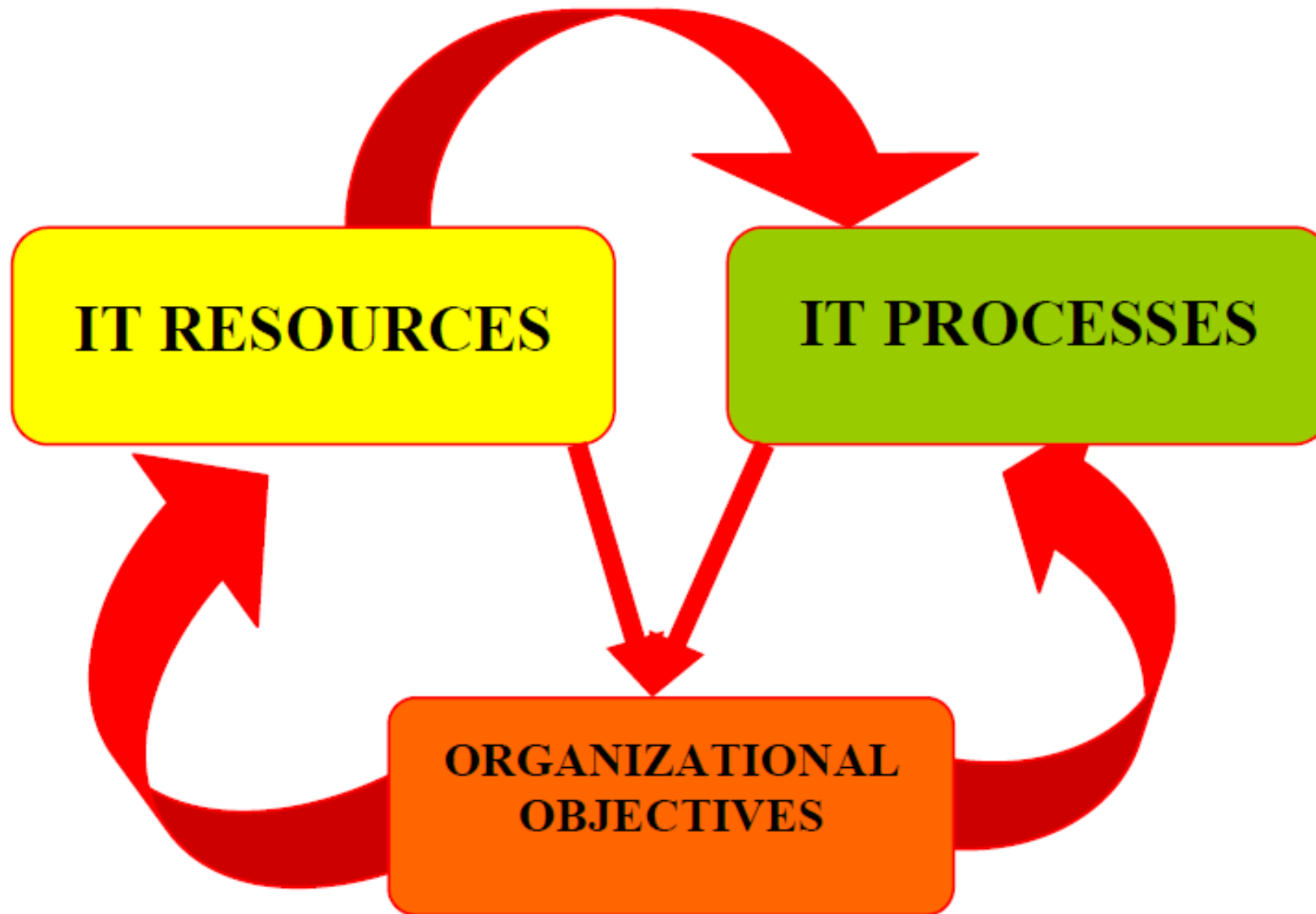


SRS 4400 Engagements To Perform Agreed-upon Procedures Regarding Financial Information

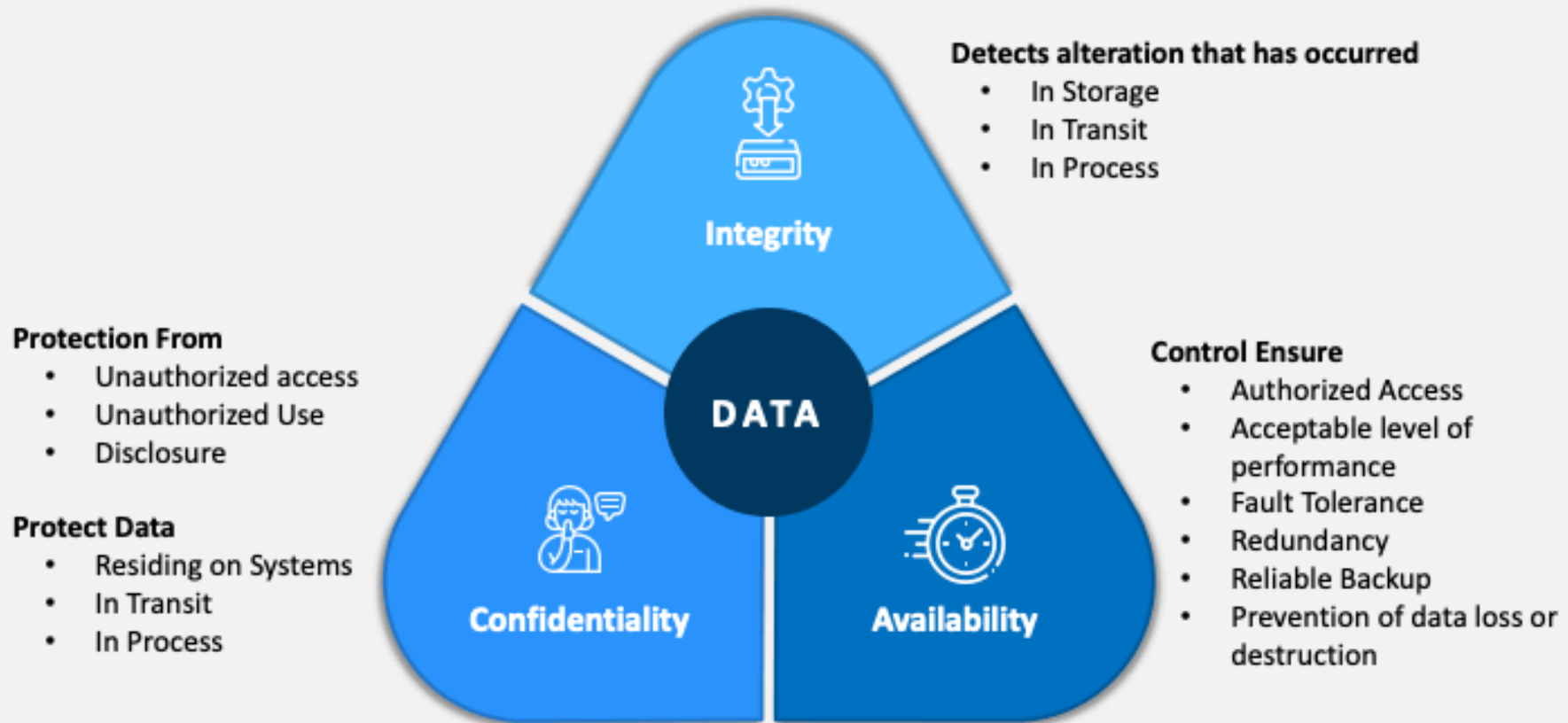
Areas of IT/IS audit

S. No	Areas	Nature of engagement
1	Core IT Operations reviews	Application review, ERP remediation
2	Cybersecurity / Information Security	Vulnerability Assessment and Penetration testing
3	Regulatory compliance	RBI/ SEBI/ NHB/ IDRBT/ IRDA
4	Business Change	Technology and IPR valuation
5	Assurance compliances	SOX testing and ITGC





Over all Objective of IT audits



Regulatory Requirements

- Companies act, 2013 Section 143(1)
- RBI regulations on IT - Gap Analysis and IT- governance frameworks NBFCs
- RBI Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds for Banks
- SEBI - IT guidelines for Stock brokers and depository participants
- IRDAI Guidelines on Information and cyber security for insurers.
- Information Technology Act, 2000 and rules made there under
- ITGI Control Objectives For Sarbanes Oxley Act.
- Credit bureau – IS audit mandates
- IRDAI cyber security assurance audit for insurance companies, brokers, agents etc.,

Best Practice Frameworks

Internal Controls

- COSO Internal Control – Integrated Framework (Most Popular)

General Computer Controls

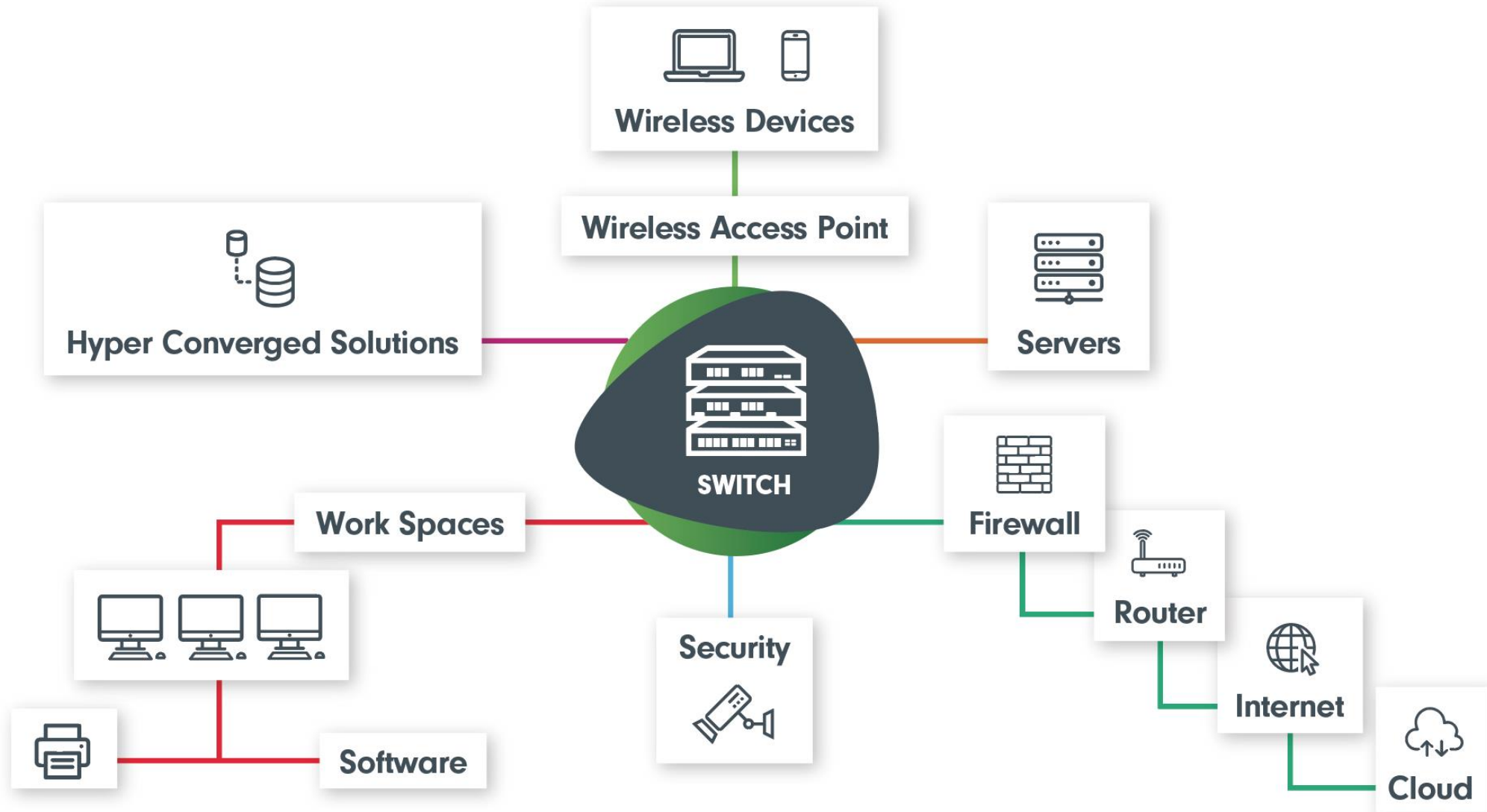
- COBIT (Most Popular)
Control Objectives for Information and Related Technology
Generally applicable and accepted standard for good IT security and control practices that provides a reference framework for management, users, and audit practitioners
Developed by the IT Governance Institute
- ISO 27000-1-ISMS
- Payment Card Industry Data Security Standard (PCI- DSS)

Information
Technology General
Controls





IT Infrastructure



Summary of ITGC



GC over IT- infrastructure/
architecture over which
business is hosted



Review of business process
followed for IT – infrastructure.

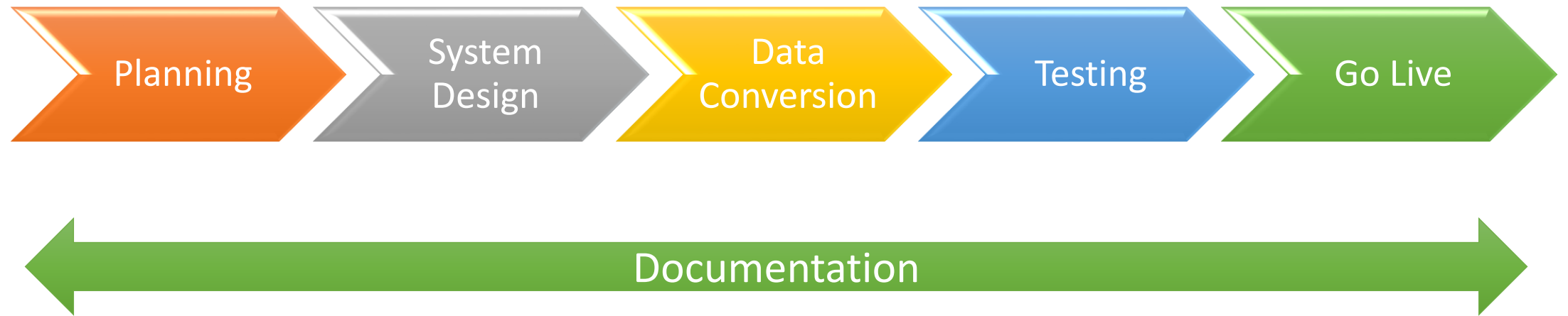


Documentation of controls
around these business
processes.



System Development and ERPs

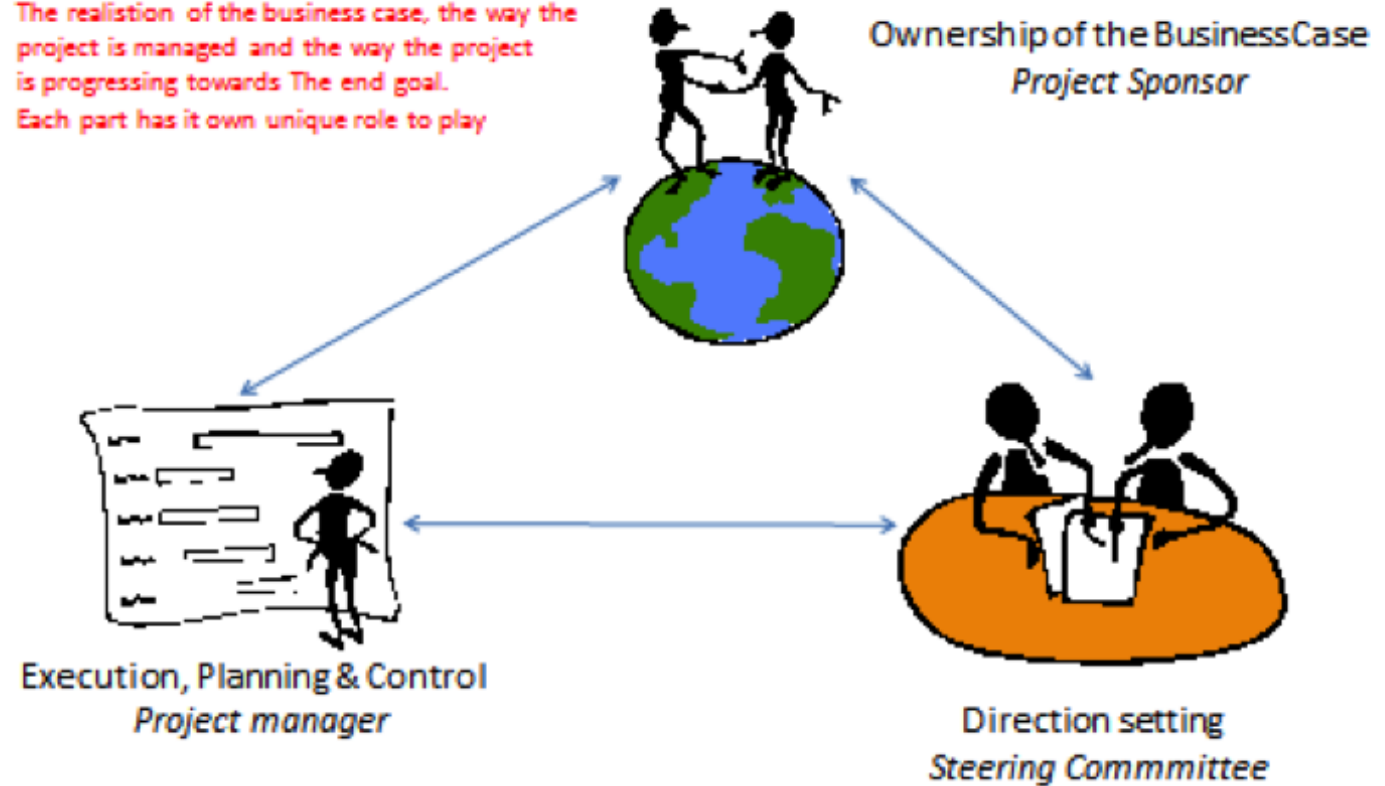
SDLC



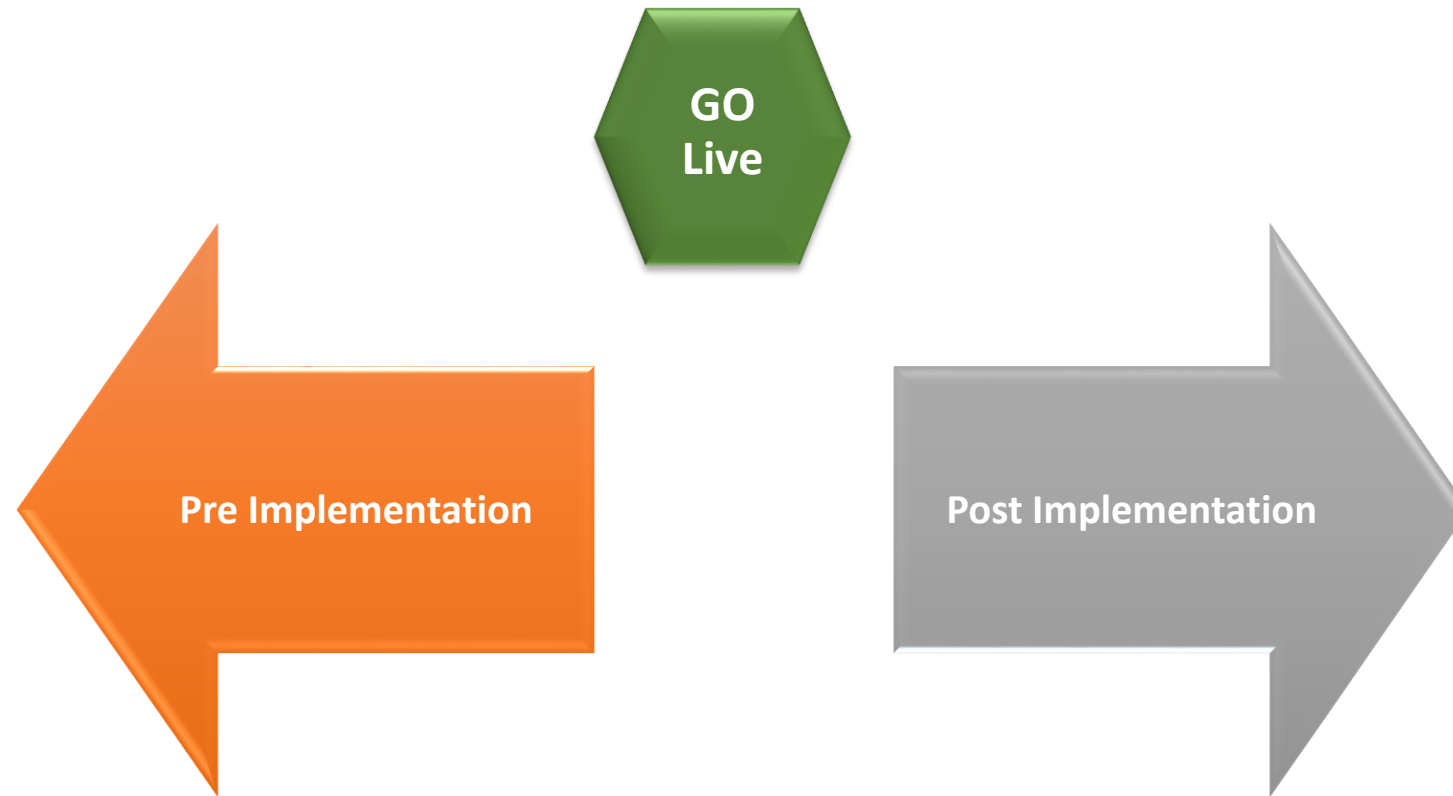
Steering
committee

Triangular relationship

During each project realisation there are 3 forces at play
The realisation of the business case, the way the project is managed and the way the project is progressing towards the end goal.
Each part has its own unique role to play



Auditing System Migrations



Auditing system migration

Pre-implementation review

**Parallel User Acceptance
Testing**

Post-implementation review

**Return on Investment and
Value for money assessment
on ERP implementation**

Need of Auditing Data Migration



Application Migration (ERP, Email, CRM,
Web Applications)



Database Migration



Data center Migration

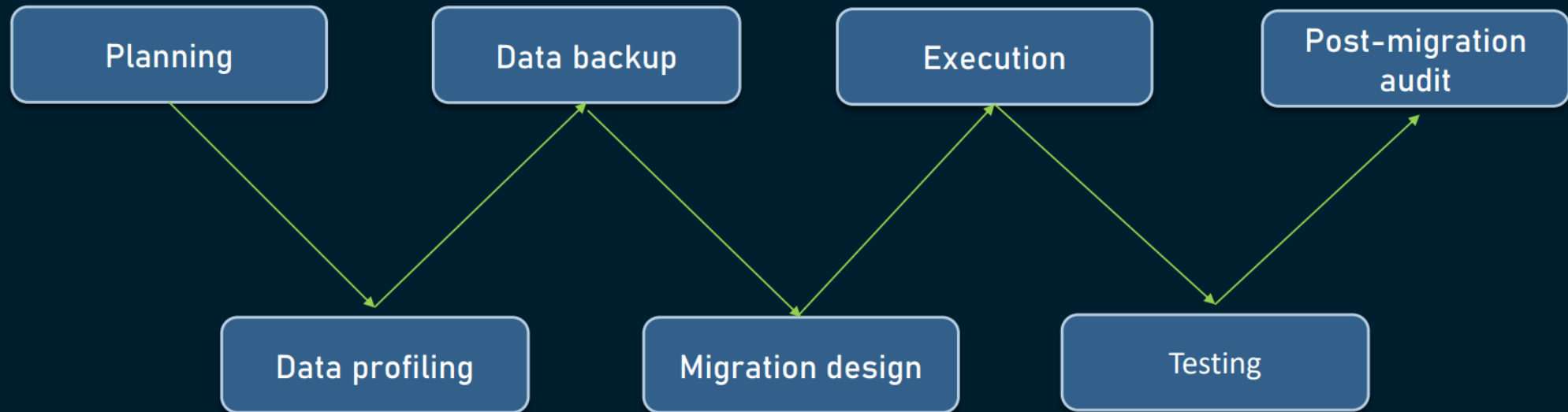


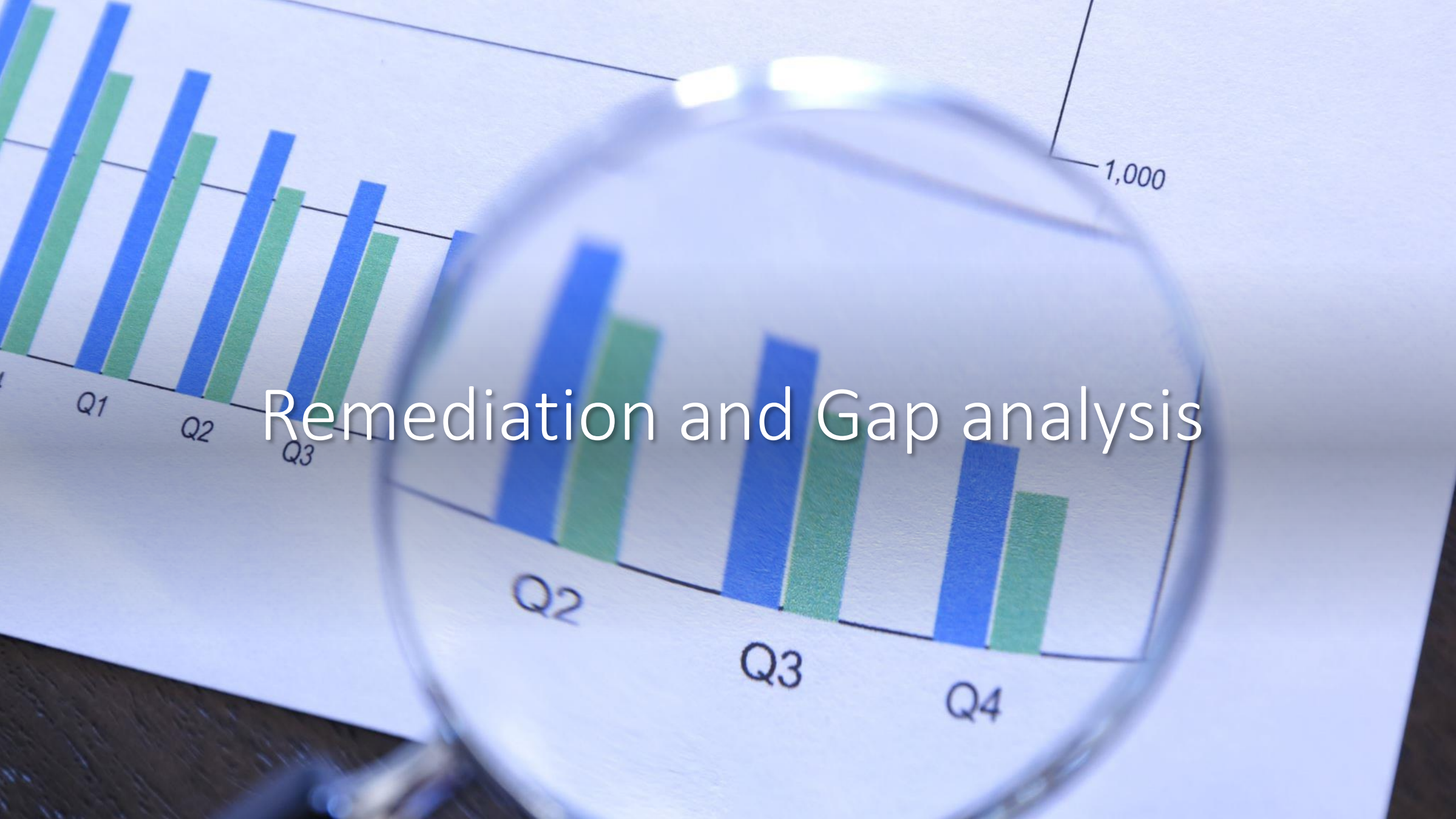
Service Provider Migration

Scope and Objectives

- Comparing Migrated Records to Records Generated by the Destination System
- Ensuring that migrated records are complete and of the appropriate context.
- Summary Verification – using record counts and checksums. Here, the number of records migrated is compiled from the destination system and then compared to the number of records migrated.
- Compare Migrated Records to Sources

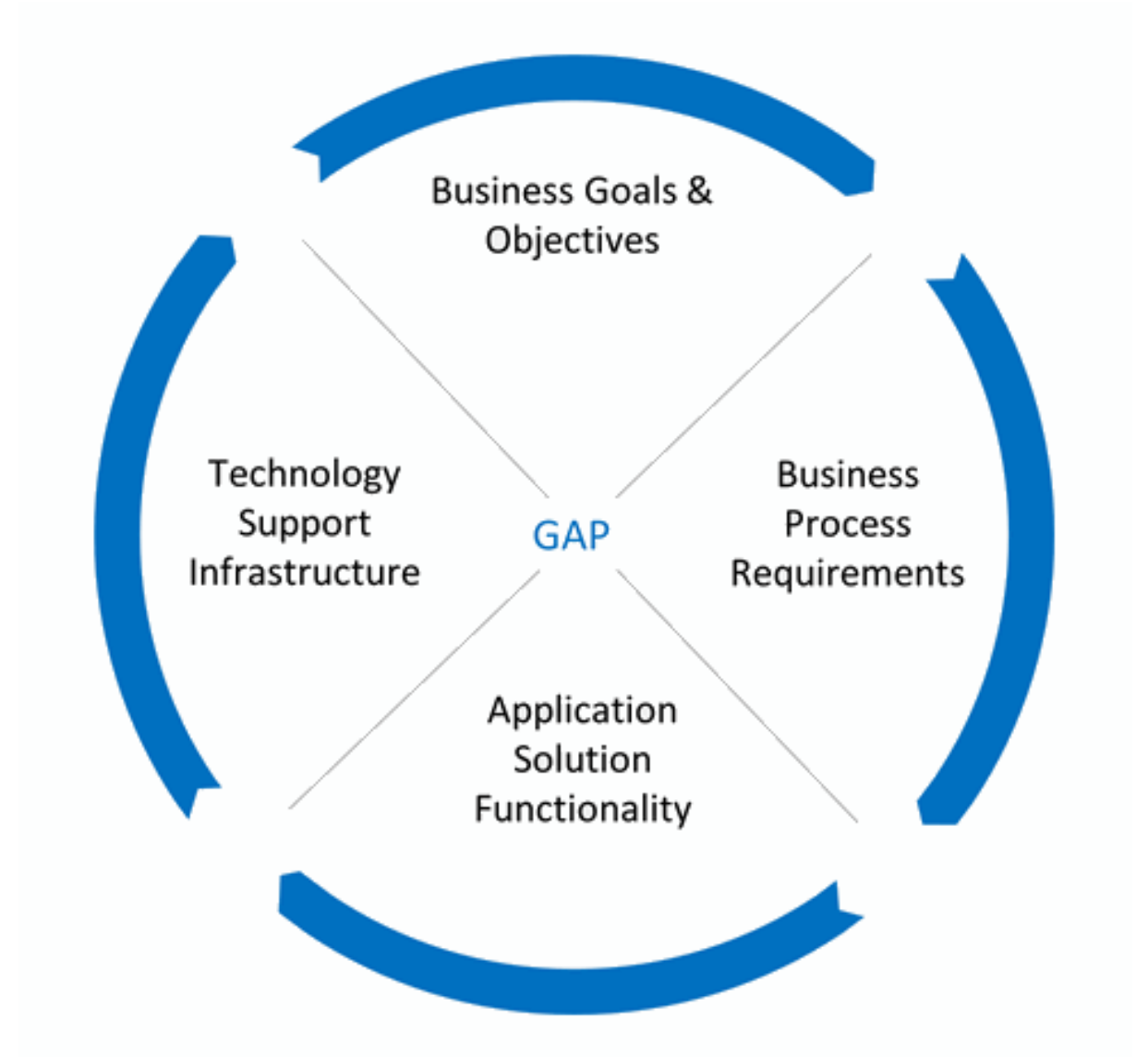
PHASES OF DATA MIGRATION





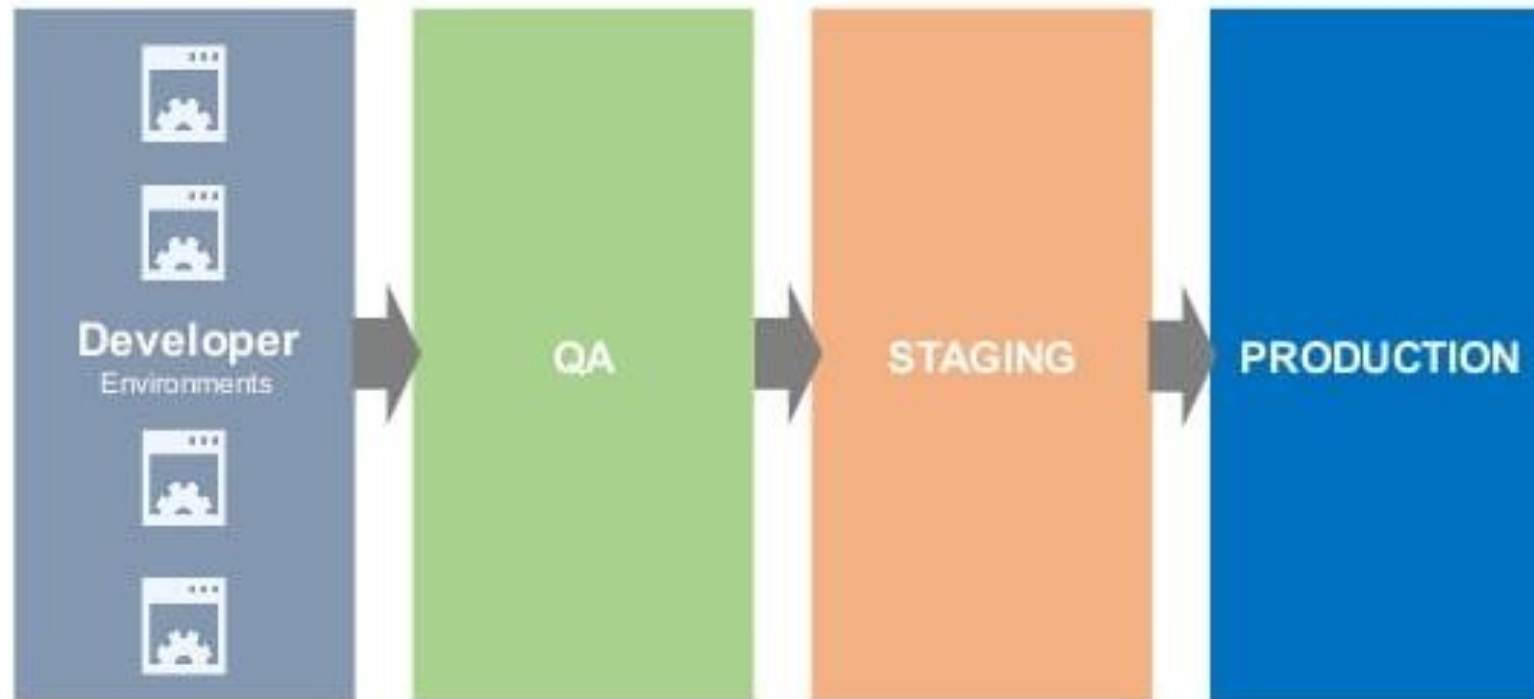
Remediation and Gap analysis

IT Gap Analysis



Application review

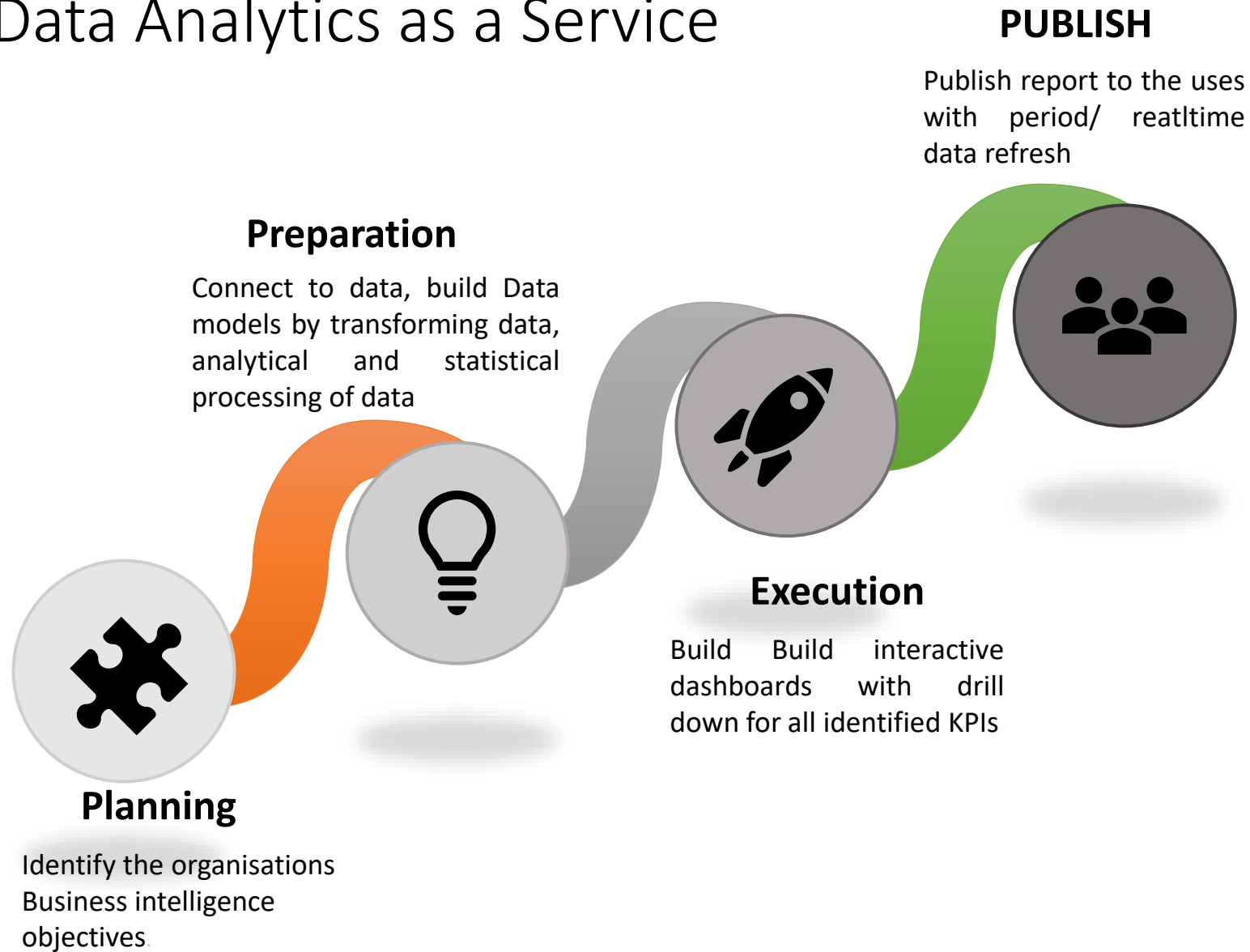
- An IS audit focused on a particular application. The scope will revolve around evaluating the input, processing and output controls of that particular application or software.





Data Driven audits

Data Analytics as a Service



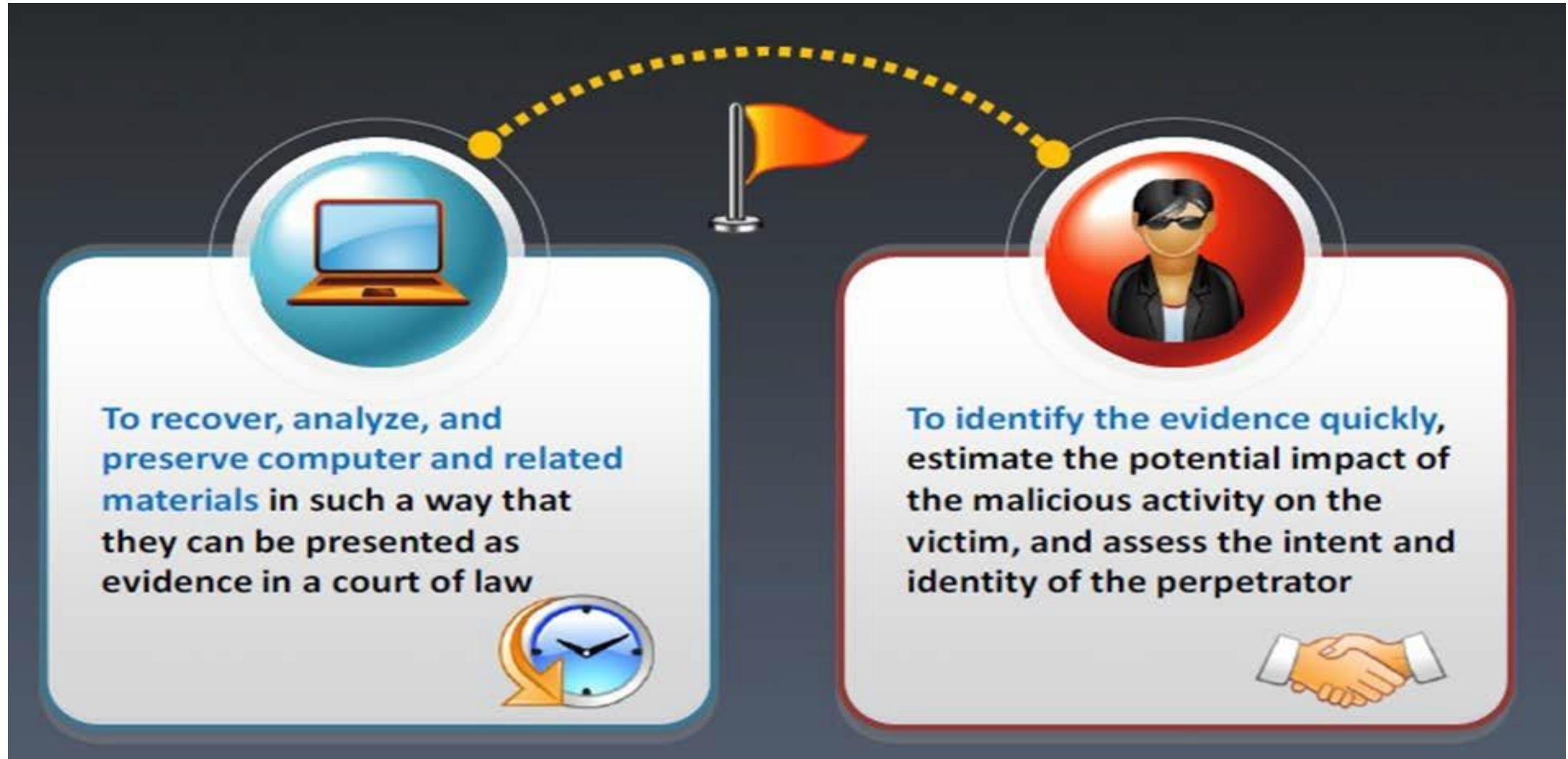
Service organisation certificates

Independent Assurance for Service Organisations – SOC 1, SOC 2 and SOC 3 third party assurance reports issued under ISAE 3402 / SSAE 16 or ISAE 3000 standards

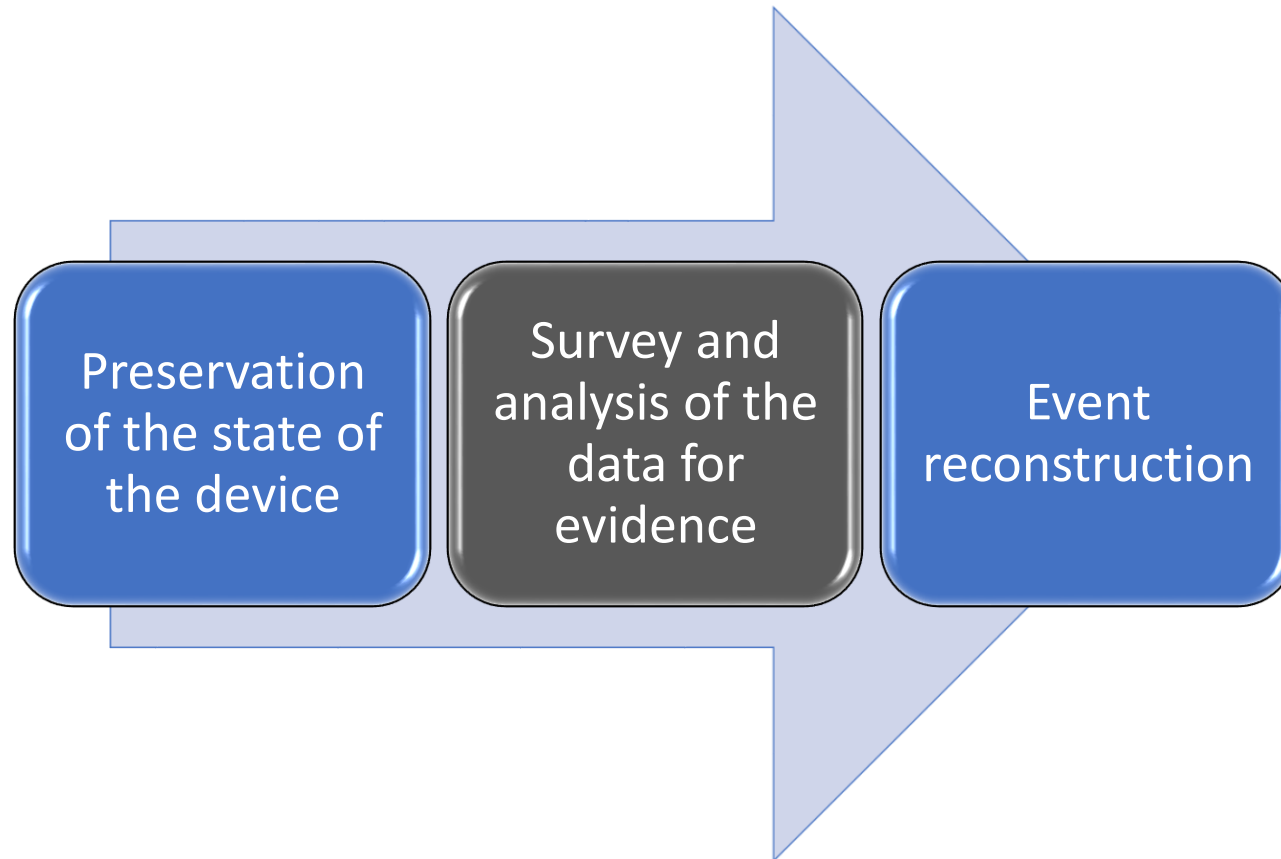


Digital forensics

Why Digital Forensic



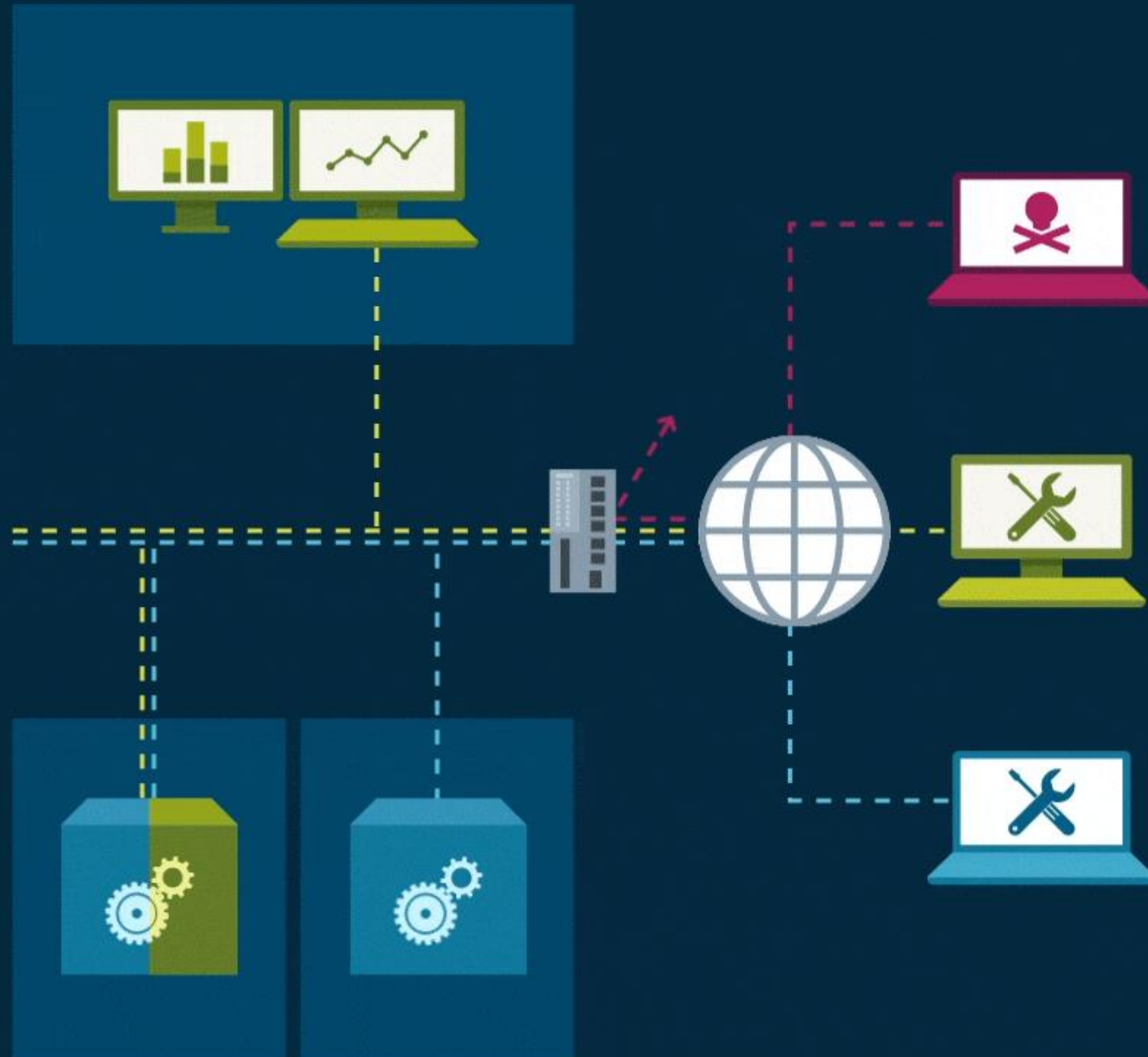
Steps and techniques in Digital Forensics





Cyber security

Office network



Computing
systems

PENETRATION TESTING



VS

VULNERABILITY ASSESSMENT



“The Purple People”

