

AIS

Control Activities

preventative

detective

corrective

Control Frame Works

COBIT Control Objectives for Information and Related Technology

NIST US National Institute of Standards and Technology

HIPPA Health Insurance Portability and Accountability Act

PCI DSS Payment Card Industry Data Security Standard

CIS Center for Internet Security

GDPR General Data Protection Regulation

COSO The Committee of Sponsoring Organizations of the Internal Treadway Commission control

Internal Controls == **process** designed to provide **reasonable assurance** regarding **operations, reporting** and **compliance**

Conversions

Strategy in Risk order

Direct conversion **nightmare situation**

Phased conversion Rollout modules systemwide but not whole system

Pilot conversion Single area implementation before full roll out

Parallel conversion Run both concurrent

Testing

Unit tests component/ function in isolation

Conversions (cont)

Integration tests ensure that the modules are talking to each other correctly

System tests whole system functionality validation

User acceptance test (UAT) confirm that it meets the business requirements

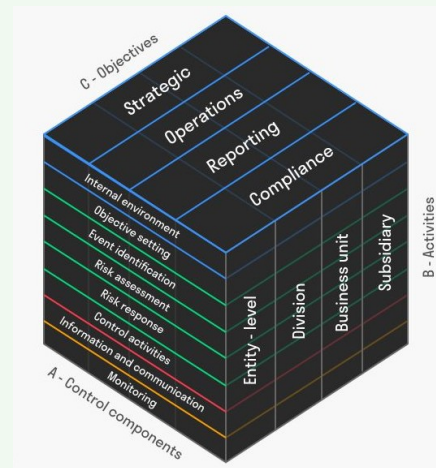
Performance tests assess max load system speed and responsiveness

Security tests id data vulnerabilities

Regression tests no lost functionality with updates

DOCUMENT DOCUMENT DOCUMENT

COSO Cube



TOP → Objectives

SIDE → Organizational

FRONT → Components

CRIME =

-Control Activities

-Risk Assessment

-Information and communication

-Monitoring

-Environment (most important)

Architecture

Centralized	connects ALL users to one location
Decent- ralized	MULTIPLE locations that each maintain a copy of the data
Distributed	all the users and systems are directly connected to one another

ERP

Enterprise Resource Planning

Why?	Improve data integrity and transparency
	Automate routine business processes
	Enhance operational efficiency
	Supports scalability and future growth

6 common modules

Financial accounting
SCM (Supply Chain Mgmt)
Production
CRM (Customer Relationship Mgmt)
Sales management
Human Resources Mgmt (HRM)

SOCs

SOC 1

Purpose	controls over financial reporting
	Internal Control over Financial Reporting (ICFR)
Users	auditors and financial statement users

SOC 2

Purpose	controls over non-financial (operational) controls
Users	Limited to parties stated in the report

SOC 3

Purpose	General Use Report simplified version of the SOC2 report
Users	Interested Parties

SOCs (cont)

SOC 1 Type 1

We have financial controls

SOC 1 Type 2

We have financial controls and we can prove that they are working

SOC 2 Type 1

We have operational controls @ pit

SOC 2 Type 1

We have operational controls and it has been tested over time

