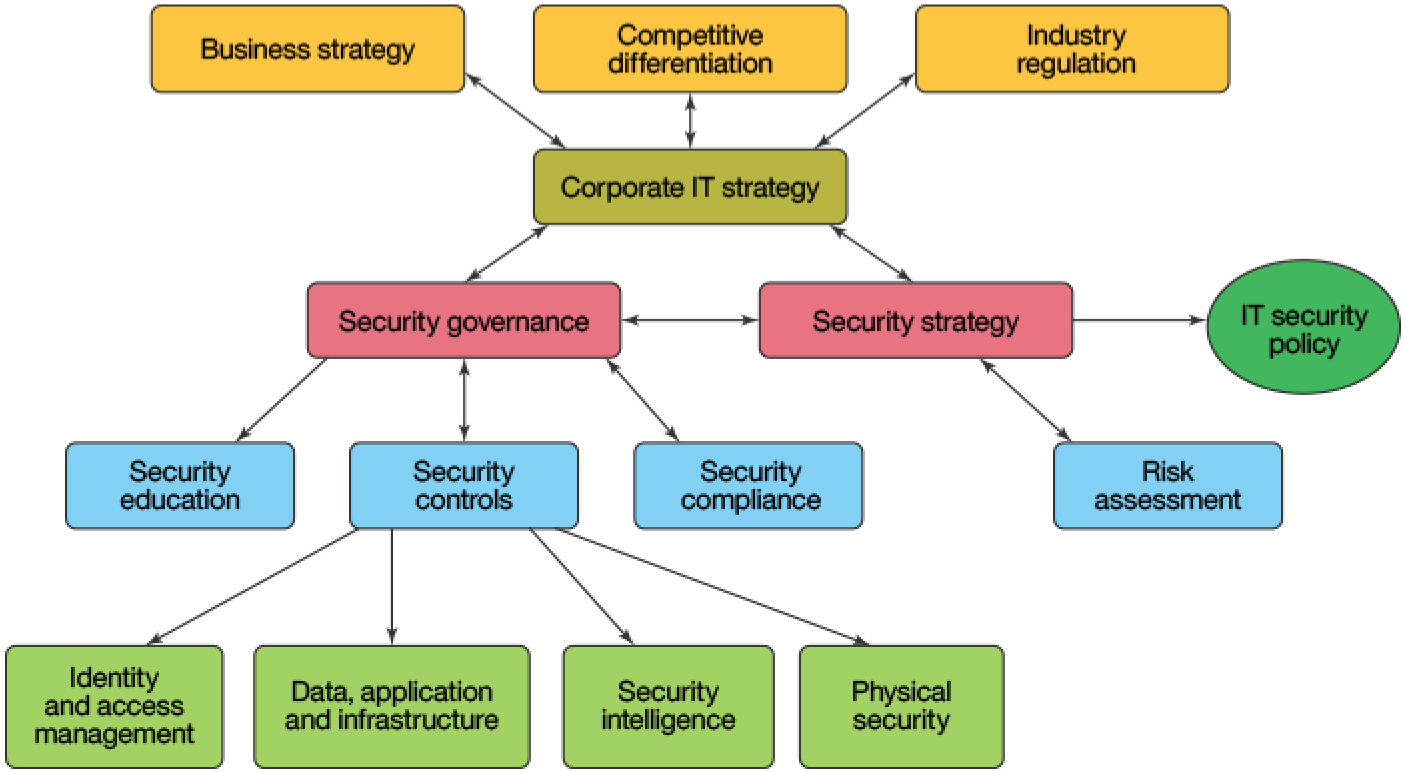
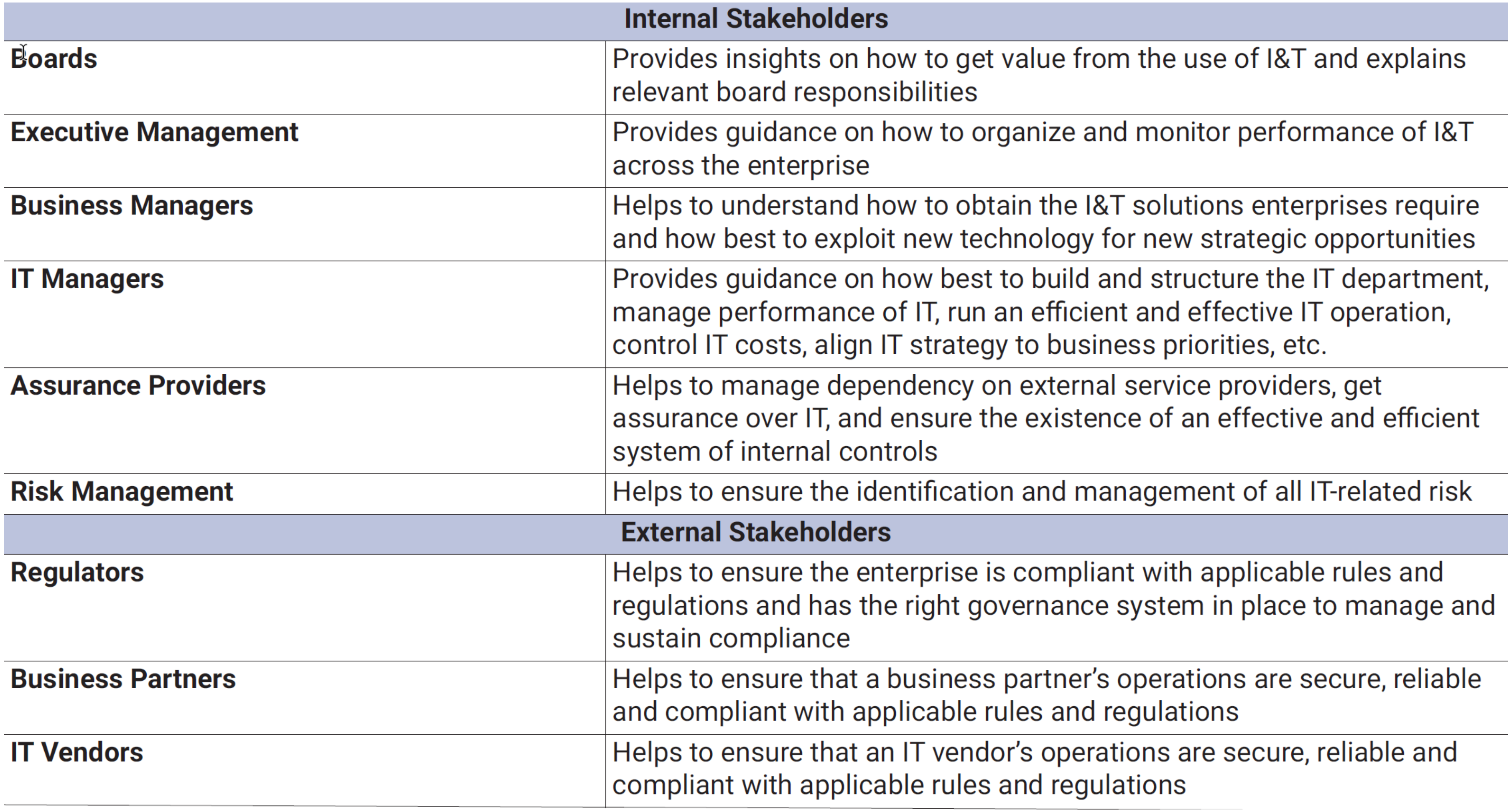
So what is governance

administration
corporate
committees
rules
policy
GOVERNANCE
board
staff
ethics
mission
decision making
responsibility

Security Governance example

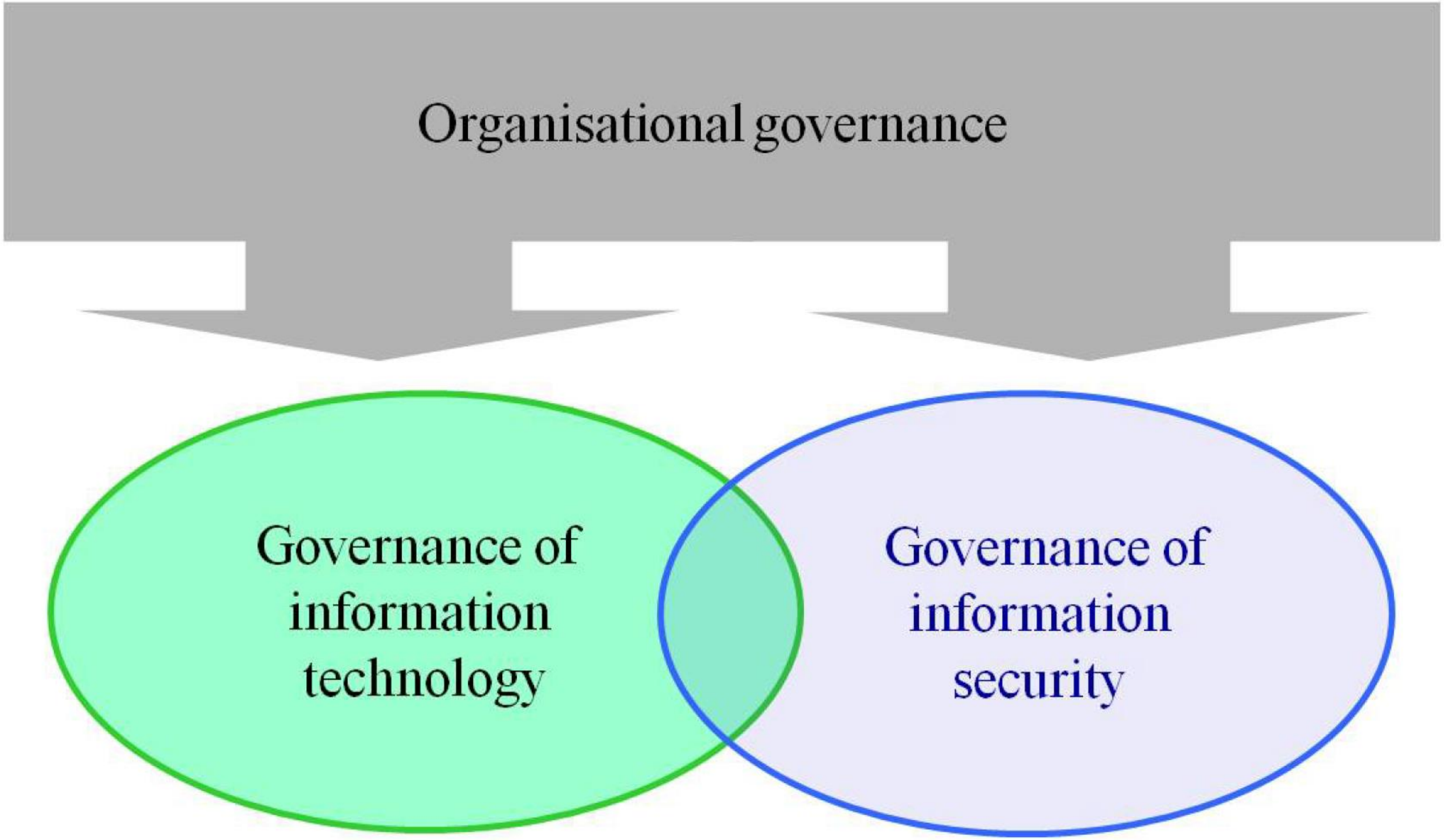


Roles within an organization

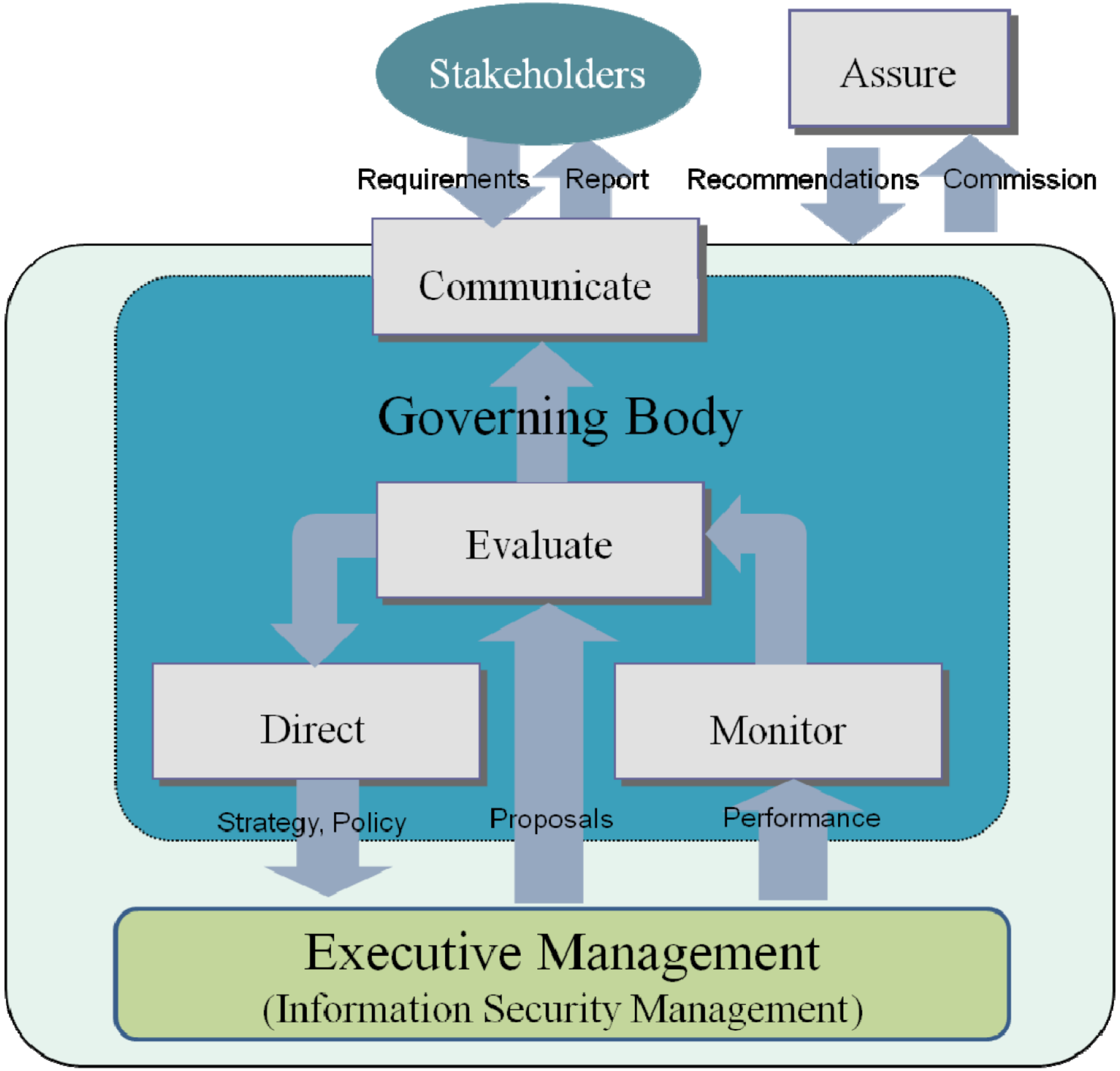


Internal Stakeholders	
Boards	Provides insights on how to get value from the use of I&T and explains relevant board responsibilities
Executive Management	Provides guidance on how to organize and monitor performance of I&T across the enterprise
Business Managers	Helps to understand how to obtain the I&T solutions enterprises require and how best to exploit new technology for new strategic opportunities
IT Managers	Provides guidance on how best to build and structure the IT department, manage performance of IT, run an efficient and effective IT operation, control IT costs, align IT strategy to business priorities, etc.
Assurance Providers	Helps to manage dependency on external service providers, get assurance over IT, and ensure the existence of an effective and efficient system of internal controls
Risk Management	Helps to ensure the identification and management of all IT-related risk
External Stakeholders	
Regulators	Helps to ensure the enterprise is compliant with applicable rules and regulations and has the right governance system in place to manage and sustain compliance
Business Partners	Helps to ensure that a business partner's operations are secure, reliable and compliant with applicable rules and regulations
IT Vendors	Helps to ensure that an IT vendor's operations are secure, reliable and compliant with applicable rules and regulations

Reference
CoBIT 5


Organisational governance
Governance of information technology
Governance of information security

Relationship between governance of information security and governance of information technology



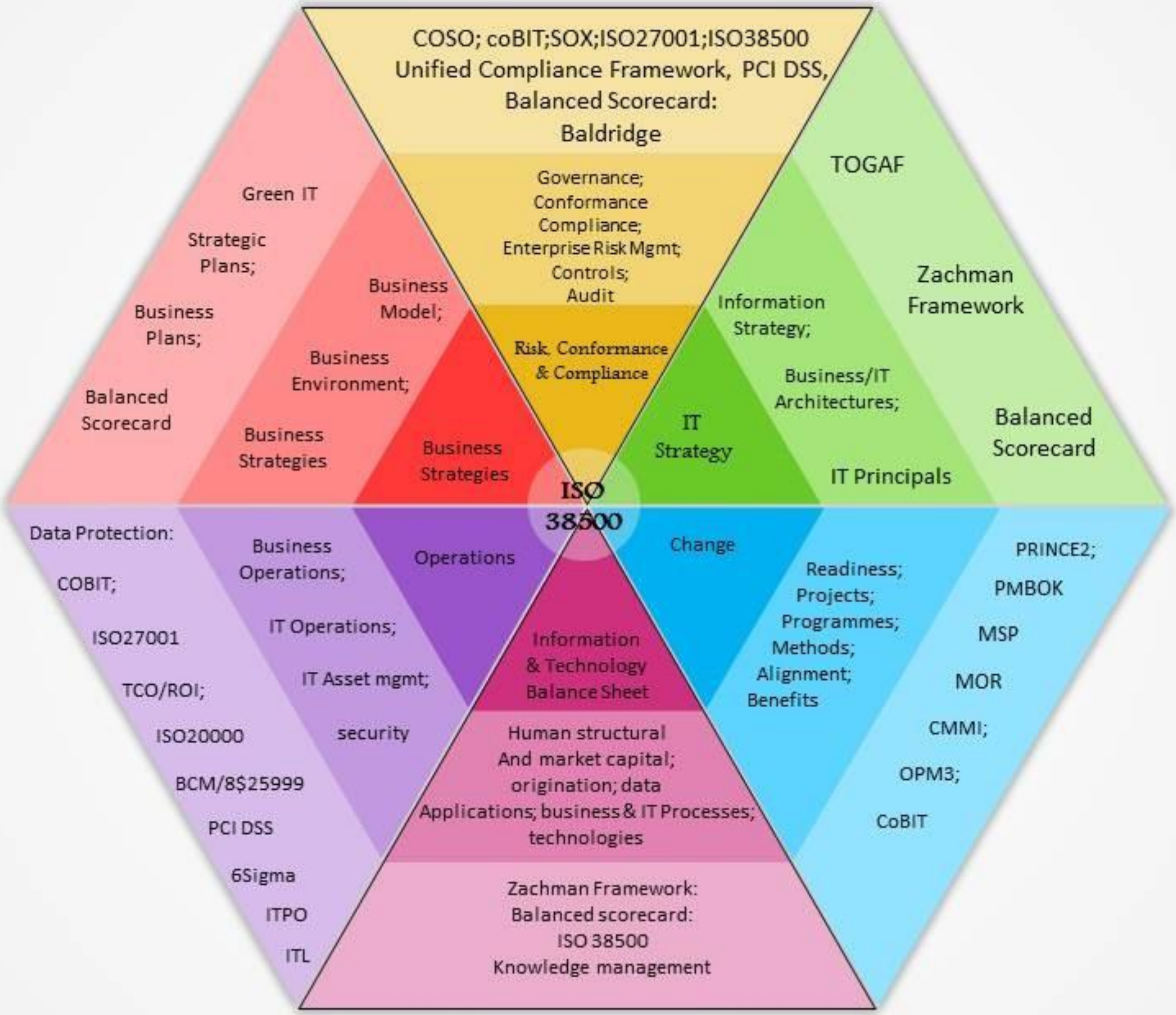
Implementation of the governance model for information security

Key Security control frameworks covered in this course. But there will be dedicated courses for the below ones.

We will cover implementation of following in separate courses:

- ISO 27001 for Information Security
- ISO 27017 for Cloud Security
- ISO 27005 for IT Risk management
- ISO 27018 for Personally Identifiable Information (PII)
- ISO 20000 for ITIL implementation
- CoBIT 5 for IT Governance
- PCI DSS for payment card data security
- ISO 22301 for Business continuity and disaster recovery management (BCP & DRP)
- ISO 38500 and various other standards
- And finally Unified Integrated Management System (UIMS) something that I developed over many years which ended being used by many top organizations!

The IT Governance Framework



COSO; coBIT;SOX;ISO27001;ISO38500
Unified Compliance Framework, PCI DSS,
Balanced Scorecard:
Baldridge

Governance;
Conformance
Compliance;
Enterprise Risk Mgmt;
Controls;
Audit

Risk, Conformance
& Compliance

Green IT

Strategic
Plans;

Business
Plans;

Balanced
Scorecard

Business
Model;

Business
Environment;

Business
Strategies

Business
Strategies

TOGAF

Zachman
Framework

Balanced
Scorecard

Information
Strategy;

Business/IT
Architectures;

IT Principals

IT
Strategy

ISO
38500

Data Protection:

COBIT;

ISO27001

TCO/ROI;

ISO20000

BCM/8$25999

PCI DSS

6Sigma

ITPO

ITL

Business
Operations;

IT Operations;

IT Asset mgmt;

security

Operations

Information
& Technology
Balance Sheet

Human structural
And market capital;
origination; data
Applications; business & IT Processes;
technologies

Zachman Framework:
Balanced scorecard:
ISO 38500
Knowledge management

Change

Readiness;
Projects;
Programmes;
Methods;
Alignment;
Benefits

PRINCE2;

PMBOK

MSP

MOR

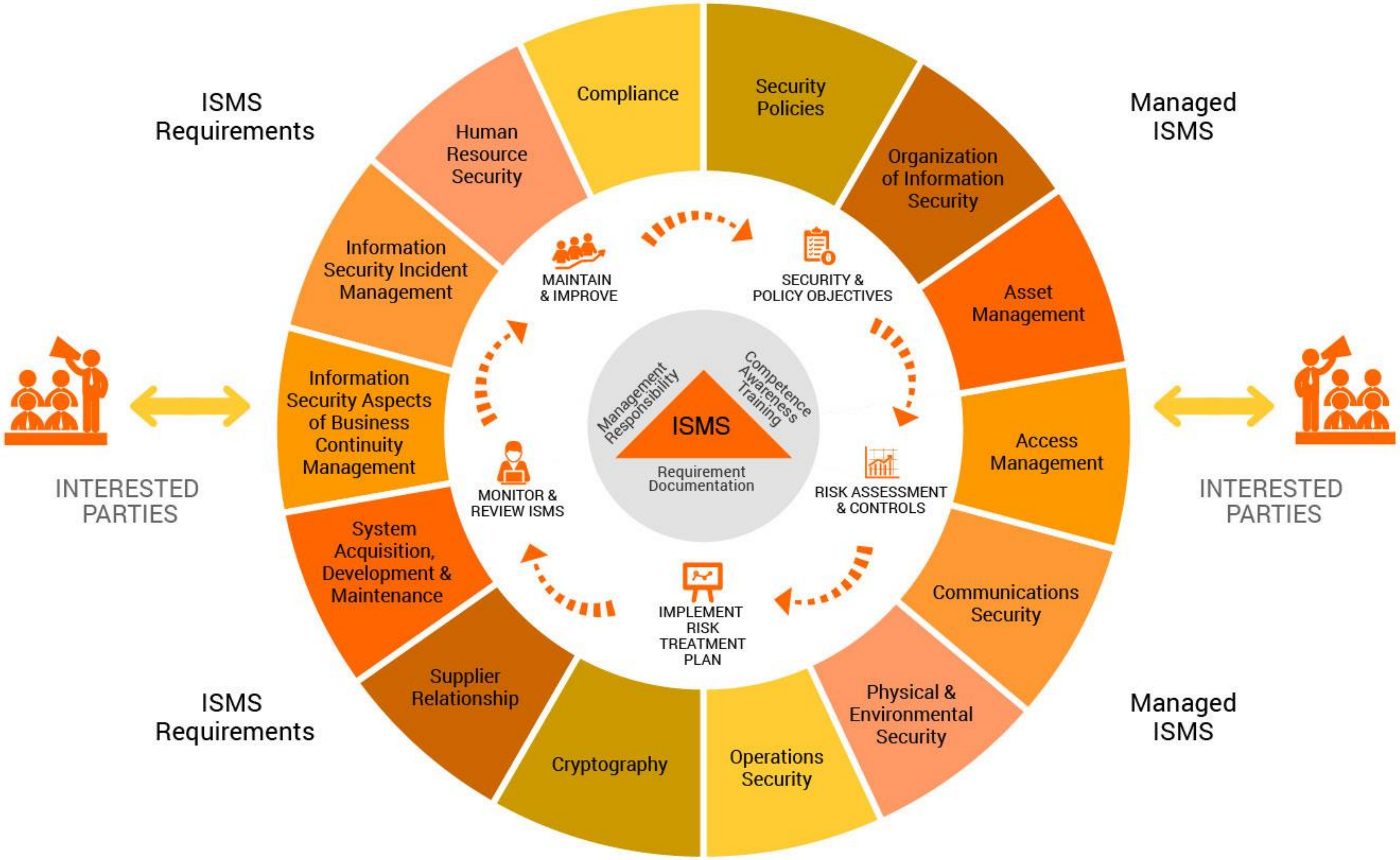
CMMI;

OPM3;

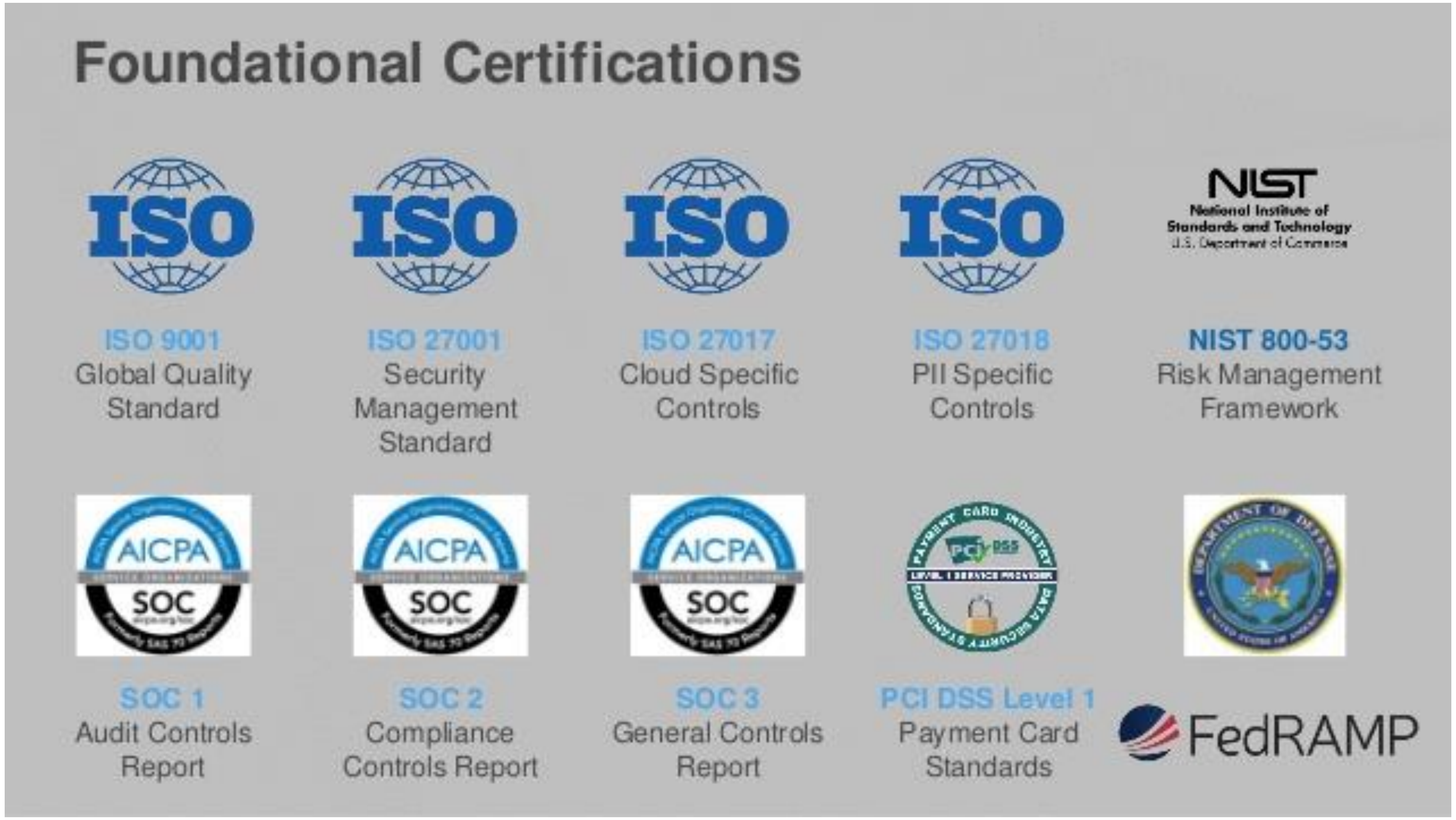
CoBIT

Your Logo

ISO 27001


ISMS Requirements
Managed ISMS
Compliance
Security Policies
Human Resource Security
Organization of Information Security
Information Security Incident Management
Asset Management
Information Security Aspects of Business Continuity Management
Access Management
System Acquisition, Development & Maintenance
Communications Security
Supplier Relationship
Physical & Environmental Security
Cryptography
Operations Security
MAINTAIN & IMPROVE
SECURITY & POLICY OBJECTIVES
RISK ASSESSMENT & CONTROLS
IMPLEMENT RISK TREATMENT PLAN
MONITOR & REVIEW ISMS
Management Responsibility
Competence Awareness Training
ISMS
Requirement Documentation
INTERESTED PARTIES
INTERESTED PARTIES
ISMS Requirements
Managed ISMS

Key security and Compliance certs in North America

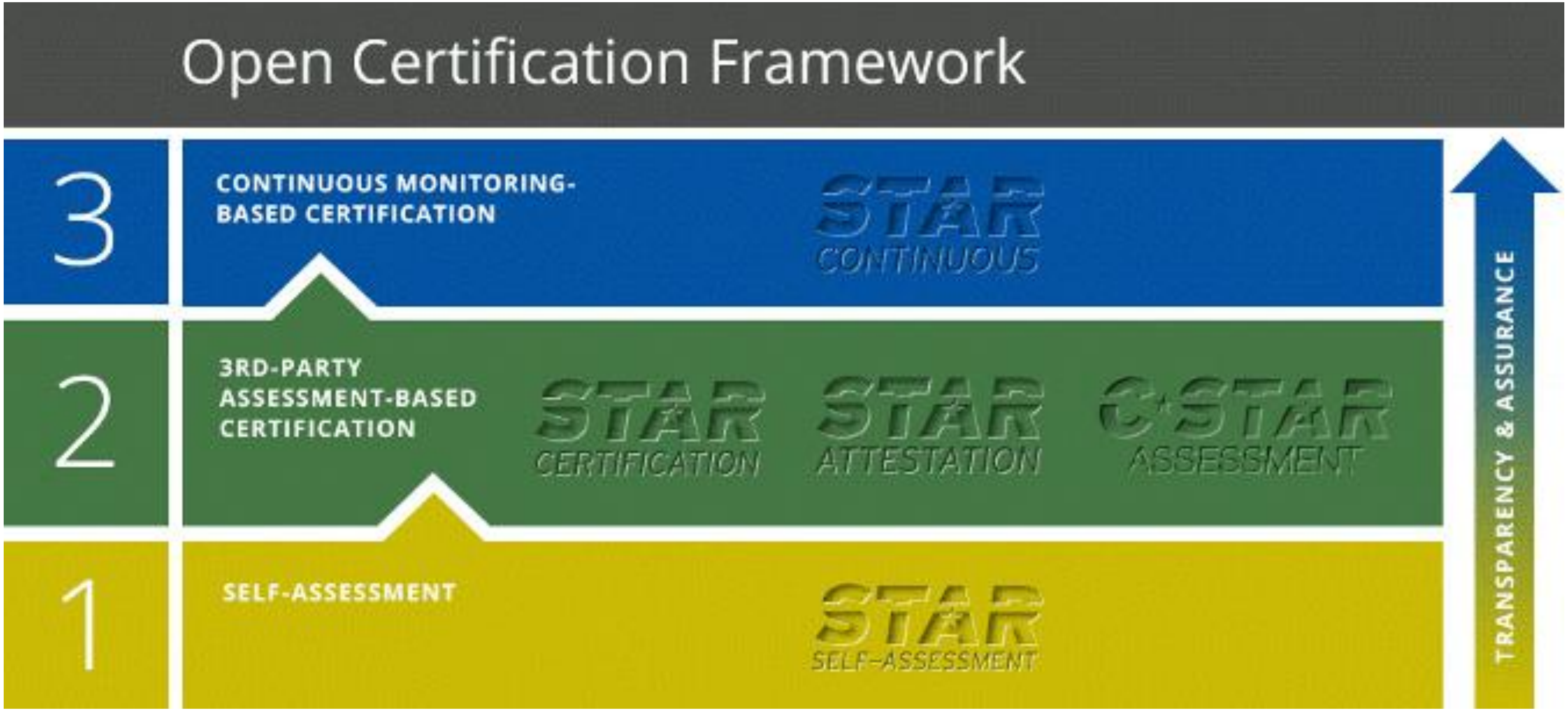


ISO
ISO
ISO
ISO
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
AICPA
SOC
AICPA
SOC
AICPA
SOC
FedRAMP

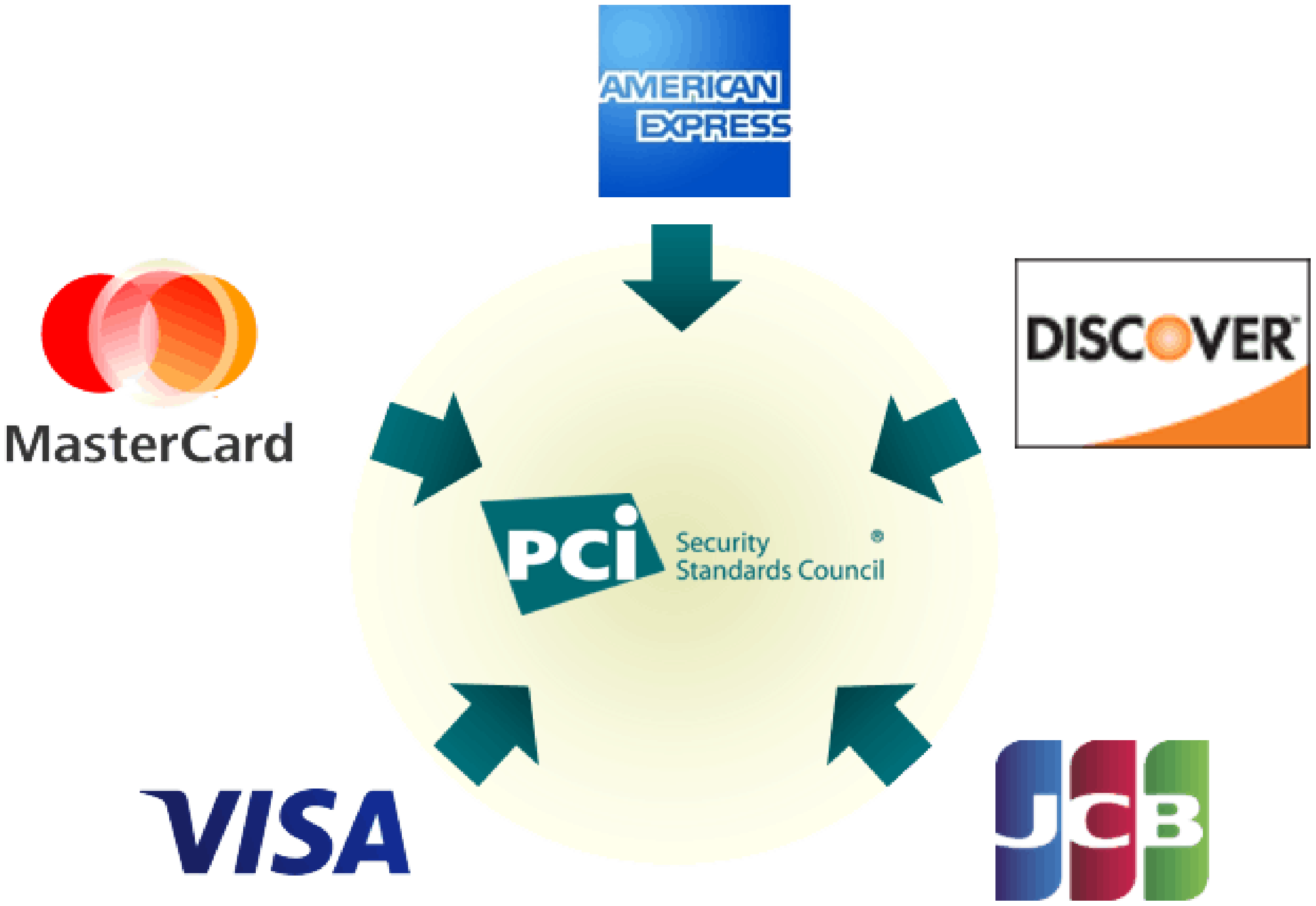
Foundational Certifications

- **ISO 9001** Global Quality Standard
- **ISO 27001** Security Management Standard
- **ISO 27017** Cloud Specific Controls
- **ISO 27018** PII Specific Controls
- **NIST 800-53** Risk Management Framework
- **SOC 1** Audit Controls Report
- **SOC 2** Compliance Controls Report
- **SOC 3** General Controls Report
- **PCI DSS Level 1** Payment Card Standards

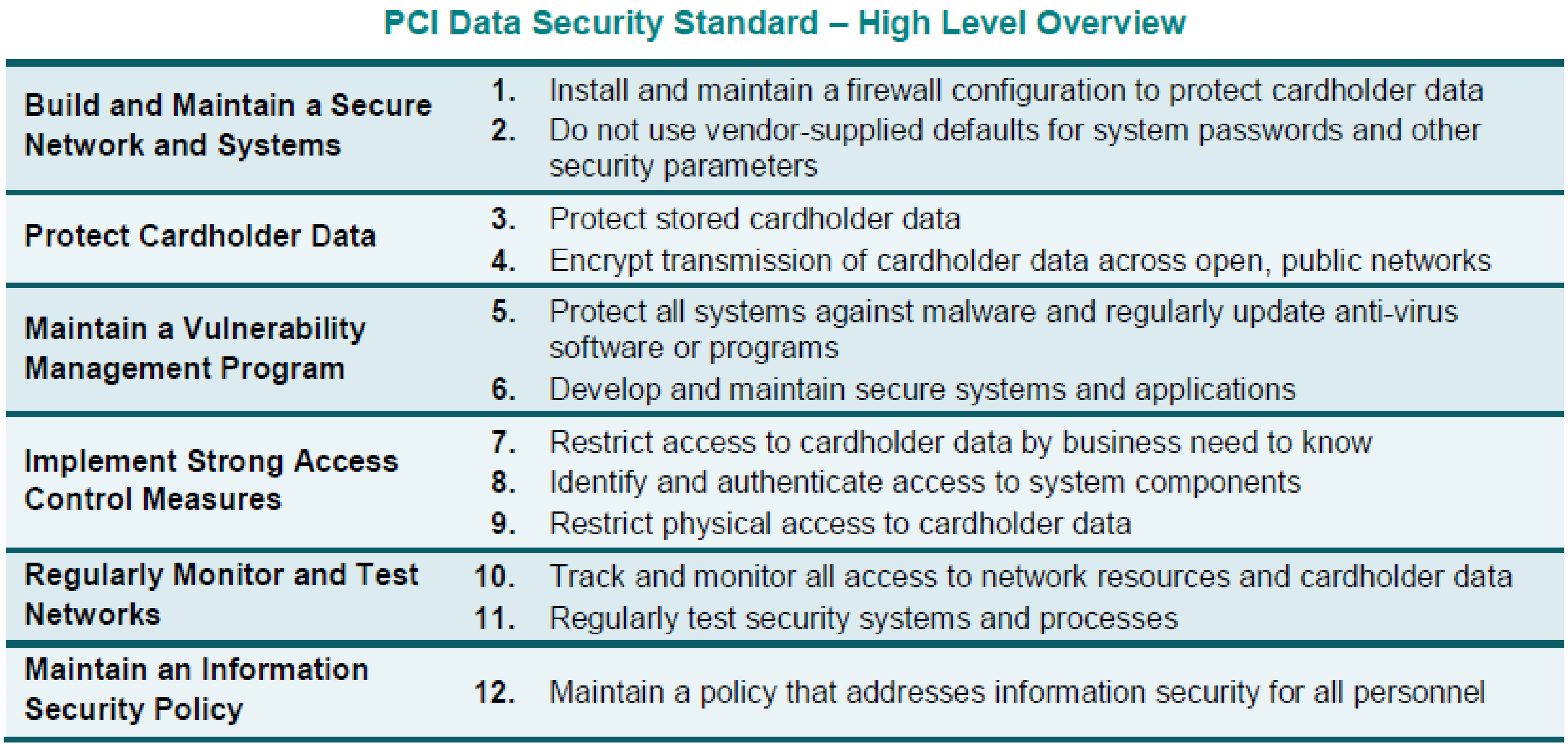
CSA cloud certification



PCI DSS


AMERICAN EXPRESS
DISCOVER
MasterCard
PCI Security Standards Council
VISA
JCB

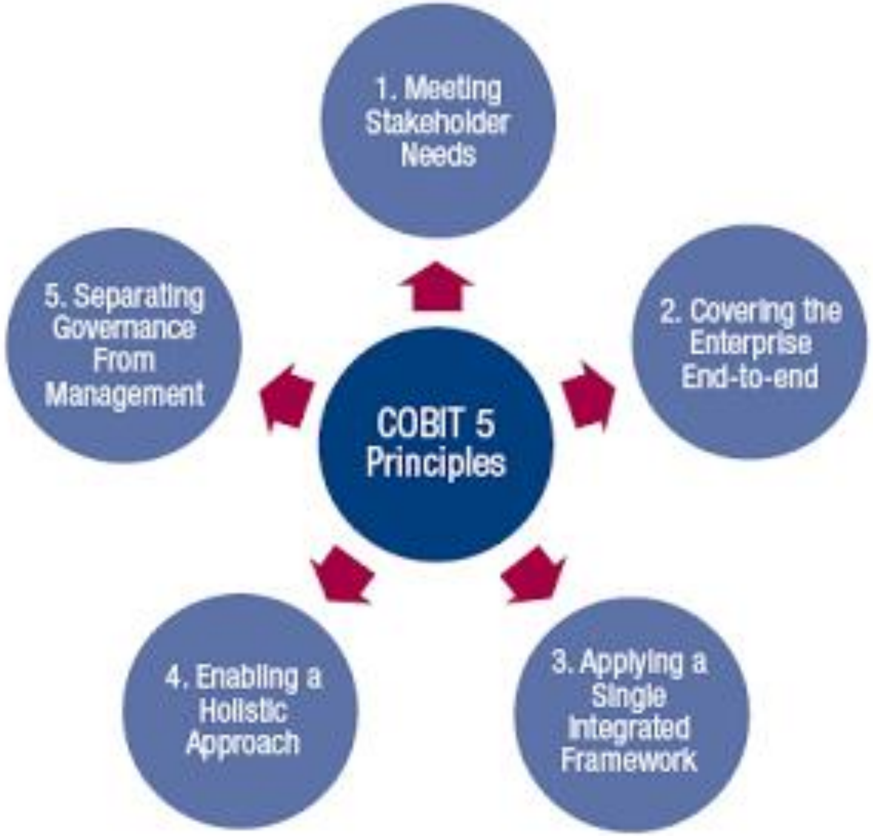
PCI DSS key requirements



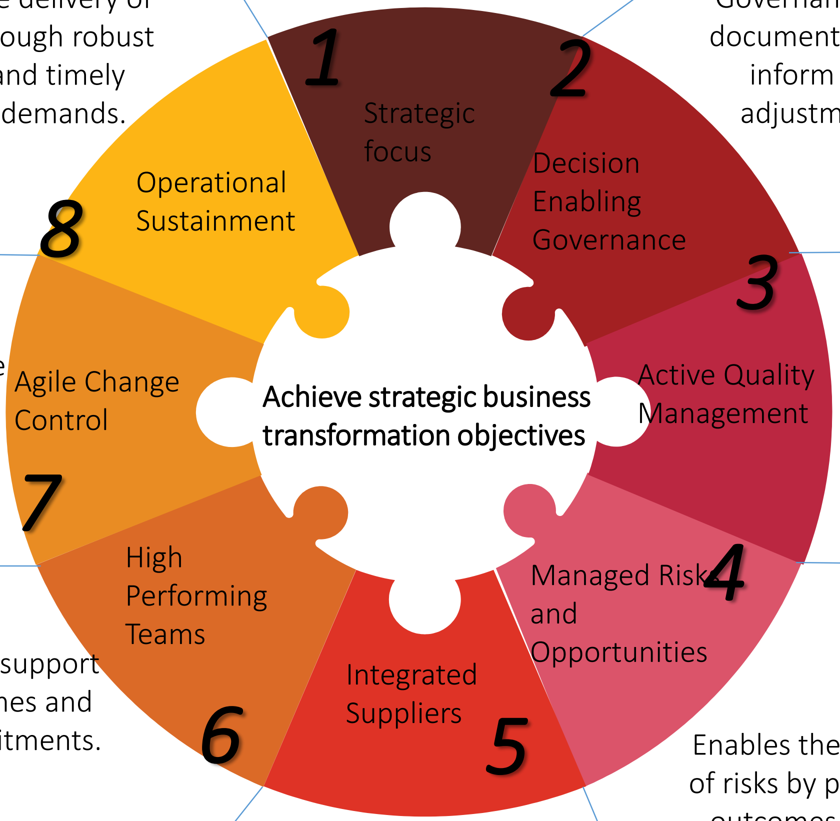
PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**1.**	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.**	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.**	Protect all systems against malware and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.**	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.**	Track and monitor all access to network resources and cardholder data
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	**12.**	Maintain a policy that addresses information security for all personnel

CoBIT 5


COBIT 5 Principles
1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management

My own Unified Integrated Management System (UIMS) framework


1
Strategic focus
2
Decision Enabling Governance
3
Active Quality Management
4
Managed Risk and Opportunities
5
Integrated Suppliers
6
High Performing Teams
7
Agile Change Control
8
Operational Sustainment
Achieve strategic business transformation objectives

Measurement system is clearly aligned to the organization’s key business strategy outcomes

Governance is clearly defined, documented and monitored to inform key decisions and adjustment requirements.

Evidence of independent quality assurance over the delivery of products and service commitments.

Enables the monitoring and management of risks by providing focus on key business outcomes and performance indicators. Indication of risks awareness and appropriate gear to address them.

Supports effective vendor management by defining and rigorously measuring contractual obligations.

Clear accountabilities to support business desired outcomes and achieve customer commitments.

Measurement framework is adaptable to evolving industry requirements

Position management for a greater consistency in the delivery of service commitments through robust operational reporting and timely responses to changing demands.

Brand Enhancement

Integrated compliance framework

Efficiencies and Savings in audit fees !

جزاك اللهُ

To ask questions, please logon to the portal https://alnafi.com/login/ and use your username and password. We will circle back to you in 2-3 business days inshAllah.