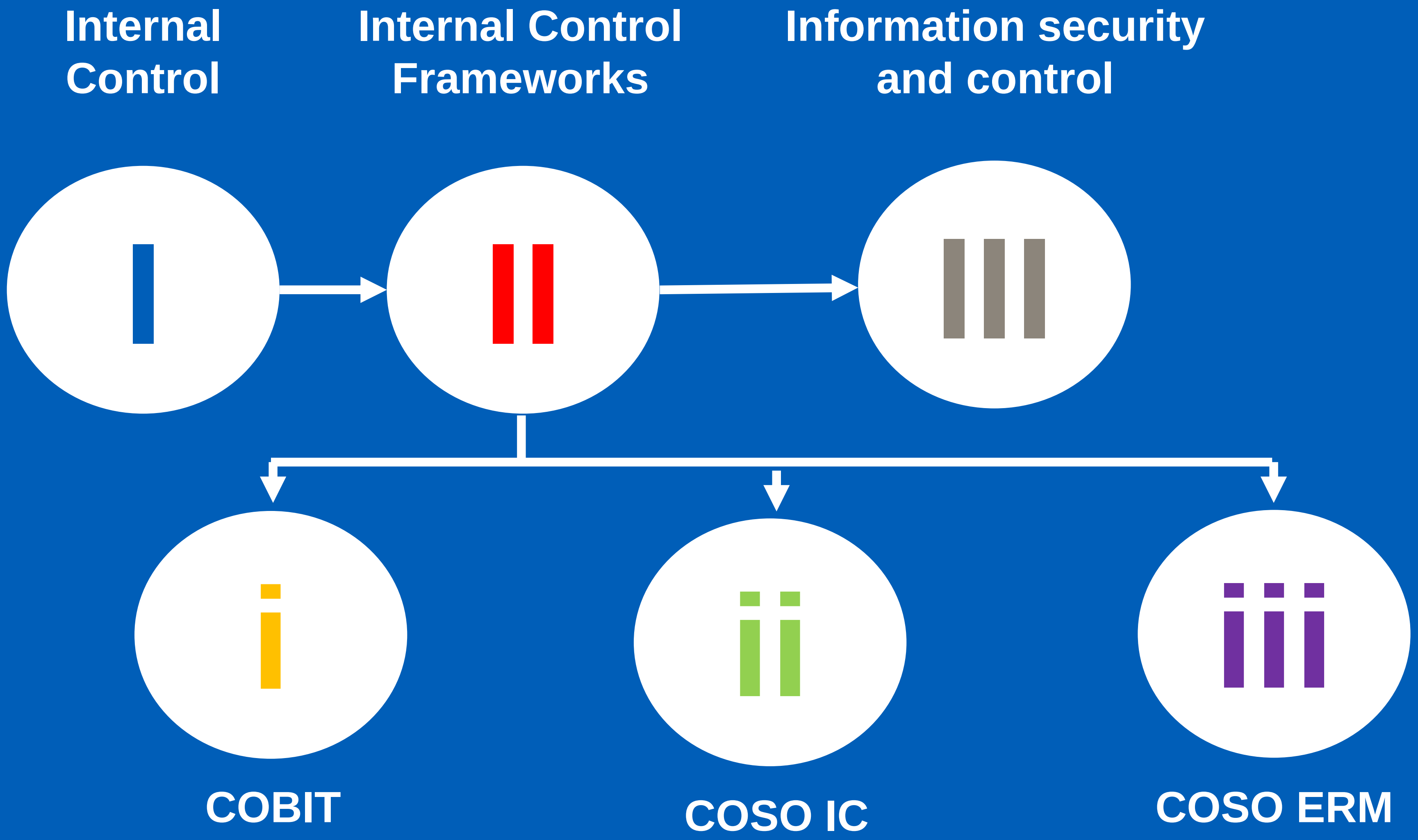
Aalto University
School of Business

Control & Accounting Information System

by Vikash Sinha



Internal Control

I

Internal Control Frameworks

II

Information security and control

III

i

COBIT

ii

COSO IC

iii

COSO ERM

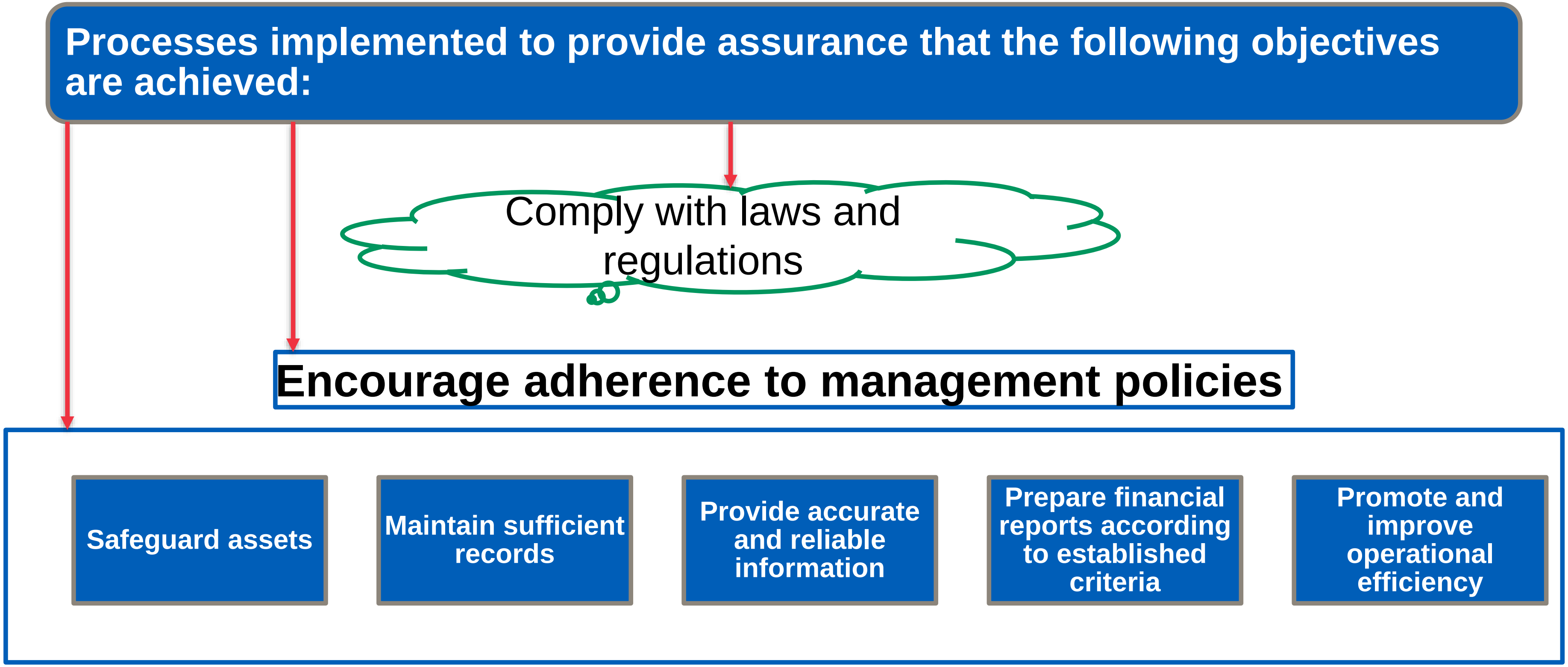
I. Internal Control

Why is control needed?

THREATS

What are internal controls?

Internal controls



Processes implemented to provide assurance that the following objectives are achieved:

Comply with laws and regulations

Encourage adherence to management policies

Safeguard assets

Maintain sufficient records

Provide accurate and reliable information

Prepare financial reports according to established criteria

Promote and improve operational efficiency

Aalto University
School of Business
© Vikash Sinha, 2019

Foreign Corrupt Practices (FCPA) and Sarbanes–Oxley Acts (SOX)

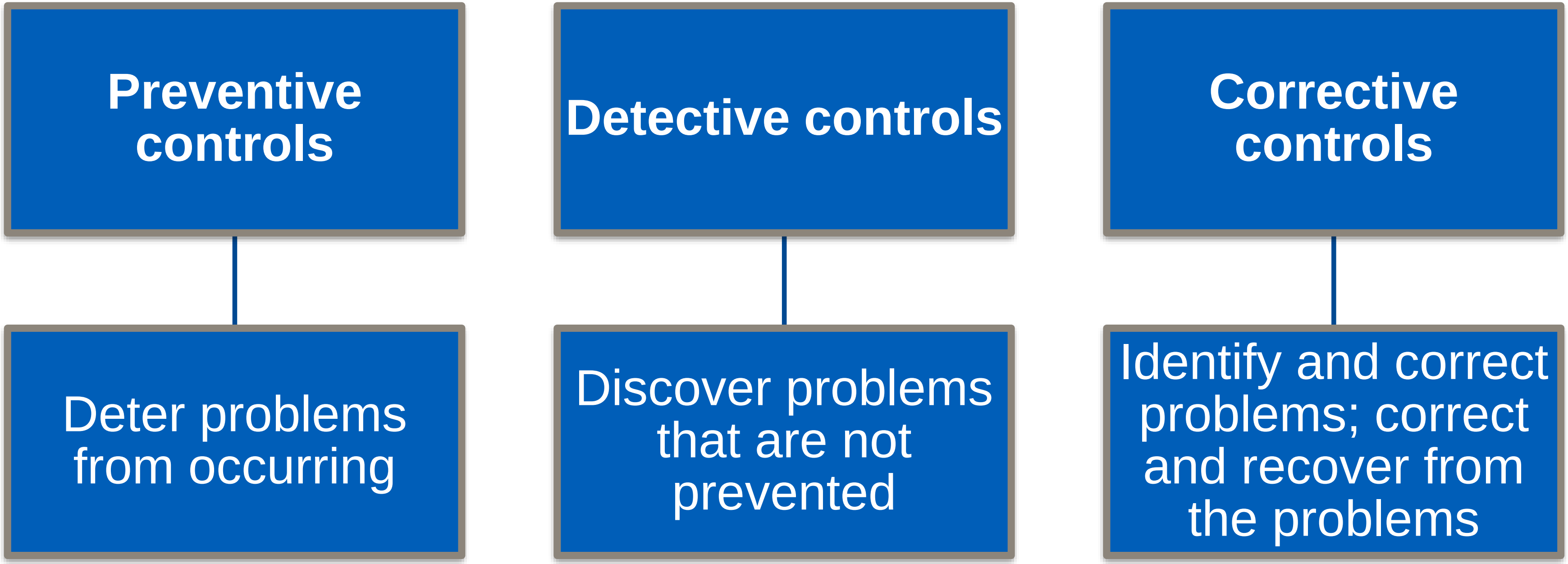
FCPA is legislation passed (1977) to

- Prevent companies from bribing foreign officials to obtain business
- Requires all publicly owned corporations to maintain a system of internal accounting controls.

SOX is legislation passed (2002) applies to publicly held companies and their auditors to

- Prevent financial statement fraud
- Financial report transparent
- Protect investors
- Strengthen internal controls
- Punish executives who perpetrate fraud

Function of internal controls



Preventive controls

Deter problems from occurring

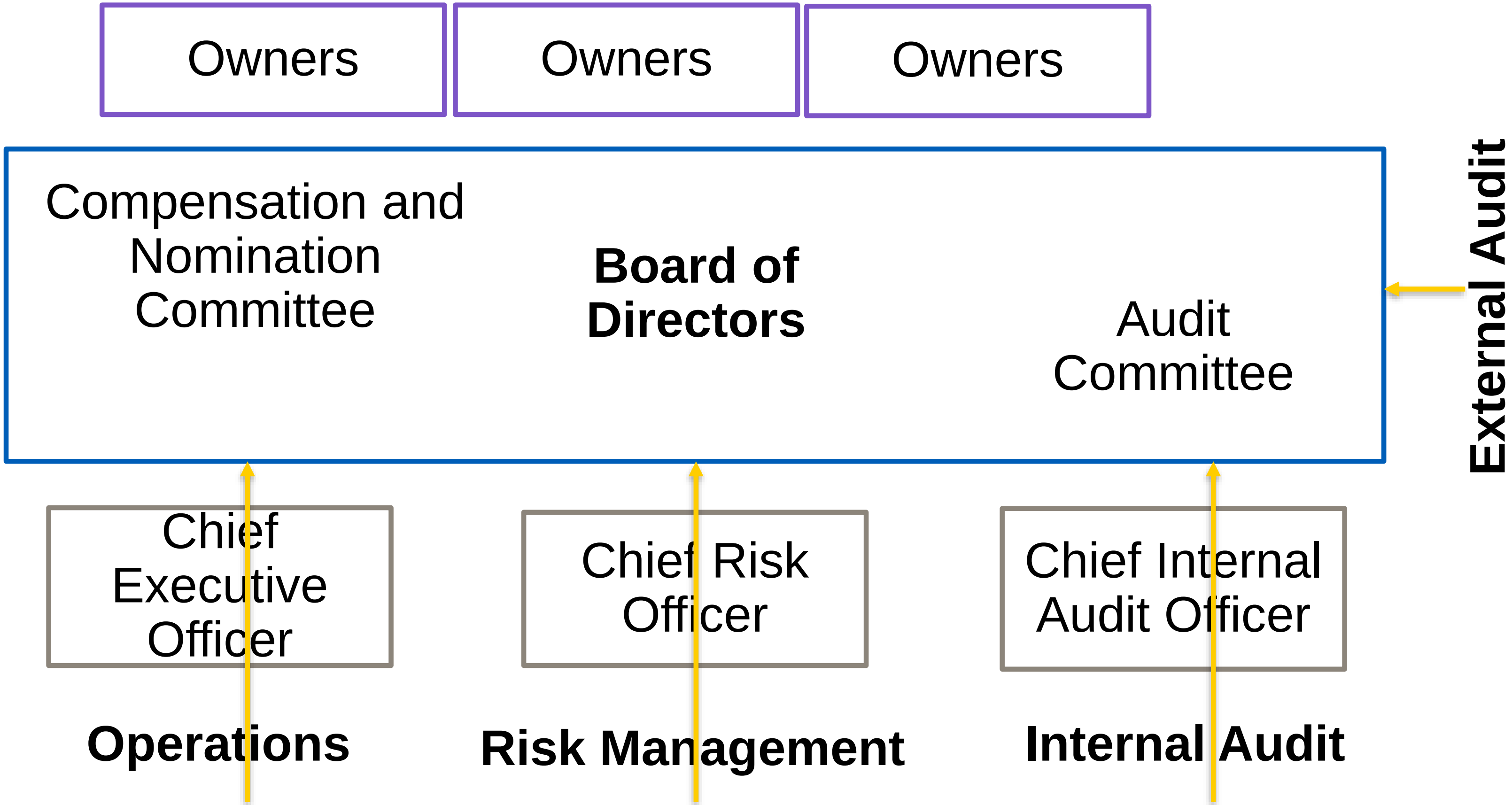
Detective controls

Discover problems that are not prevented

Corrective controls

Identify and correct problems; correct and recover from the problems

Three lines of defense



II. Internal Control Frameworks

What are the important control frameworks?

Different control frameworks

Control Objectives for Information and Related Technologies (COBIT) by Information Systems Audit and Control Association (ISACA)

- Framework for IT control

Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control (IC) Framework

- Framework for enterprise internal controls (control-based approach)

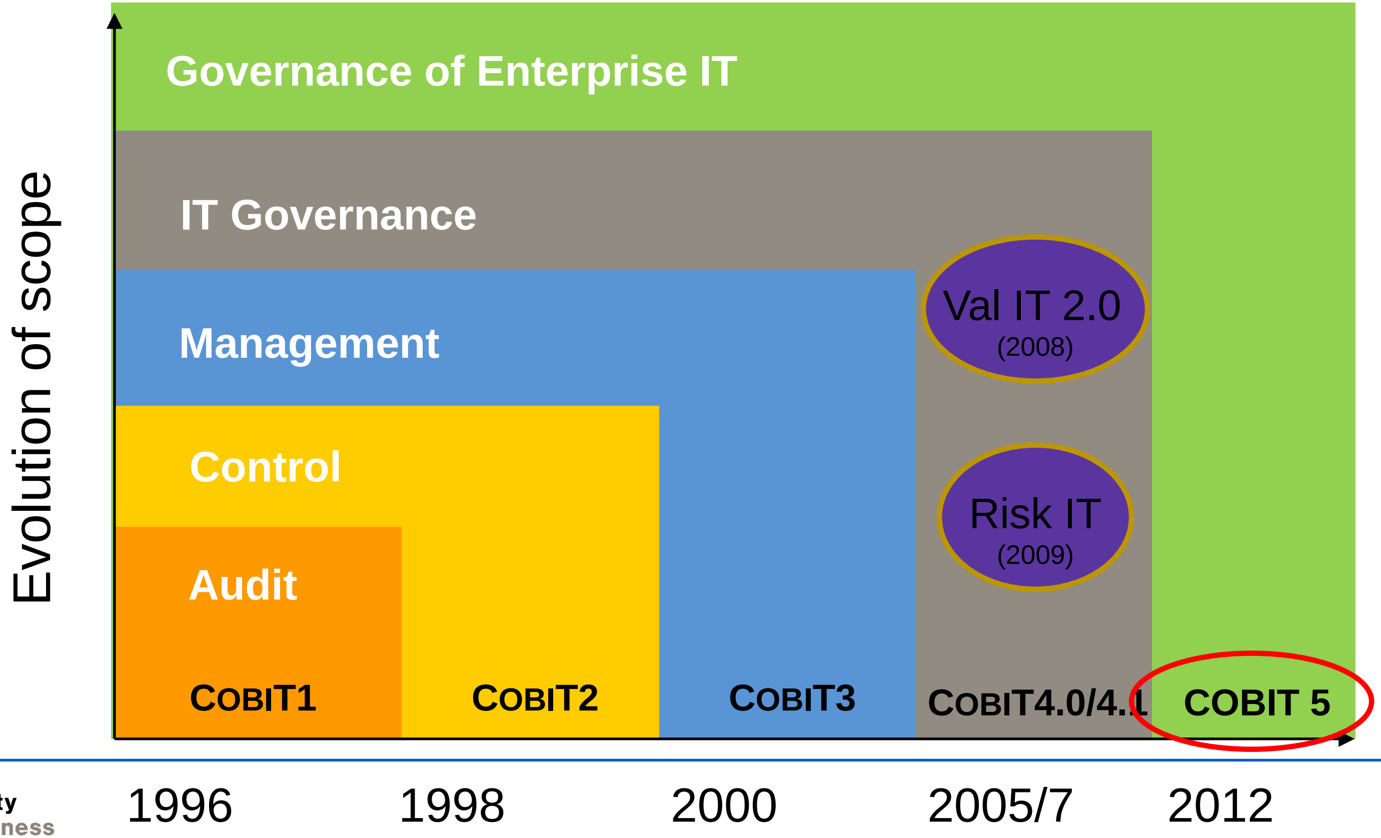
COSO Enterprise Risk Management Framework

- Expands COSO framework taking a risk-based approach

II.i COBIT

Historical evolution of COBIT

A framework from ISACA, at www.isaca.org/cobit



Aalto University
School of Business
© Vikash Sinha, 2019

A HISTORICAL TIMELINE

The COBIT® Framework

COBIT 2019

1995
2000
2005
2010
2015

1996

ISACA released the first edition of COBIT framework.

1998

The debut of the second edition of COBIT added Control to its framework.

2000

A third edition of COBIT, with new Management Guidelines, was published.

2003

ISACA created an online version of the third edition of COBIT.

2005

COBIT 4.0 becomes the fourth edition in the COBIT series of releases.

2007

COBIT upgraded to version 4.1.

2012

COBIT 5 integrated the COBIT 4.1, Val IT 2.0 and Risk IT frameworks, and drew from ISACA's IT Assurance Framework (ITAF) and the Business Model for Information Security (BMIS). COBIT 5 also coordinated with frameworks and standards such as ITIL, ISO, PMBOK, PRINCE2 and TOGAF.

2018

ISACA publishes COBIT 2019, an update that adds design factors and focus areas to make it more practical and customizable.

1995

Windows 95, Java, and HTML 2.0 (first formal html standard) debuted, as did Amazon.com, craigslist.com, match.com and ebay.com

1997

Original wireless LAN standard (IEEE 802.11) released, DVD technology appeared, and Google.com registered as domain—incorporating a year later and launching in 1999.

2001

Internet Archive "Wayback Machine" (archive.org) launched, Wikipedia started publishing, and Apple released iPod.

2002

U.S. Sarbanes-Oxley law revolutionized corporate recordkeeping and retention standards, leading to new IT regulatory requirements.

2003

Third WiFi standard created proliferation of "hotspots" as Skype, LinkedIn and WordPress started up. U.S. CAN-SPAM Act became law.

2006

Twitter founded and Google acquired YouTube.

2007

Apple iPhone signaled move to touchscreen devices; Apple App Store went online one year later.

2012

Worldwide e-commerce tops $1 trillion in sales.

2014

Internet of Things (IoT) technology standard ushered new wave of smart devices.

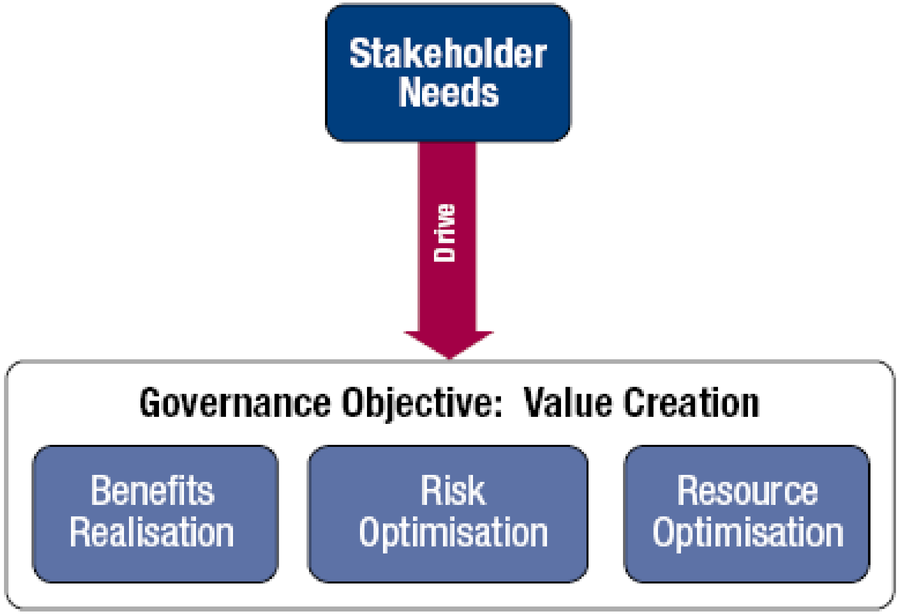
2016

ISACA acquired CMMI Institute and its business maturity and capability models, adding these resources to the ISACA/COBIT framework portfolio.

Five principles of COBIT 5

- Meeting Stakeholder Needs
- Covering the Enterprise End-to-end
- Applying a Single Integrated Framework
- Enabling a Holistic Approach
- Separating Governance From Management

Meeting stakeholder needs



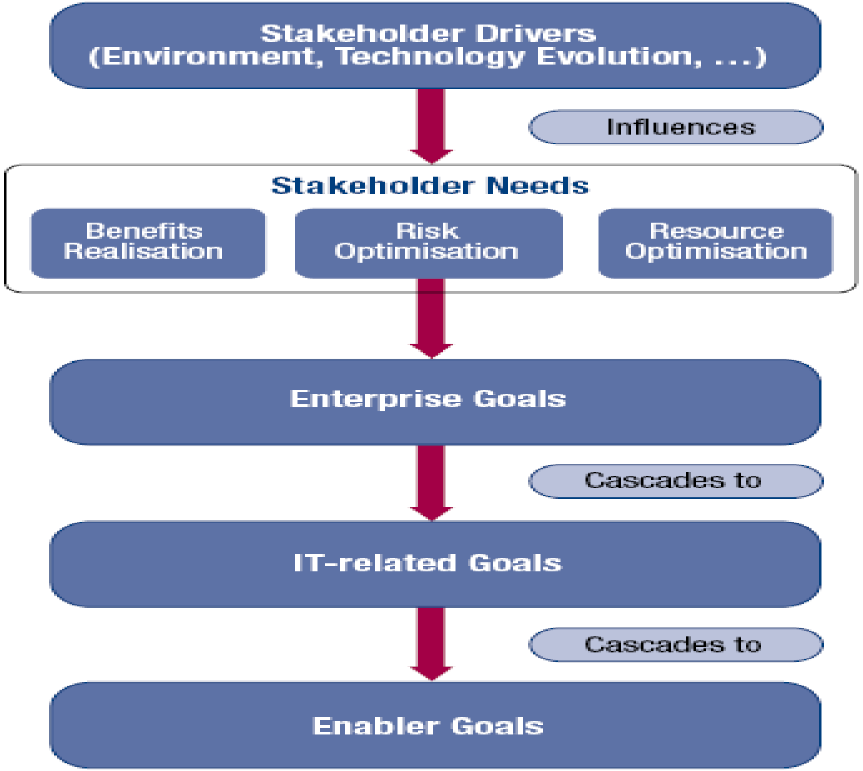
Source: COBIT® 5, figure 3. © 2012 ISACA® All rights reserved.

Meeting stakeholder needs

- **Enterprises have many stakeholders, and 'creating value' means different—and sometimes conflicting—things to each of them.**
- **Governance is about negotiating and deciding amongst different stakeholders' value interests.**
- **The governance system should consider all stakeholders when making benefit, resource and risk assessment decisions.**
- **For each decision, the following can and should be asked:**
  - **Who receives the benefits?**
  - **Who bears the risk?**
  - **What resources are required?**

Source: COBIT® 5, figure 3. © 2012 ISACA® All rights reserved.

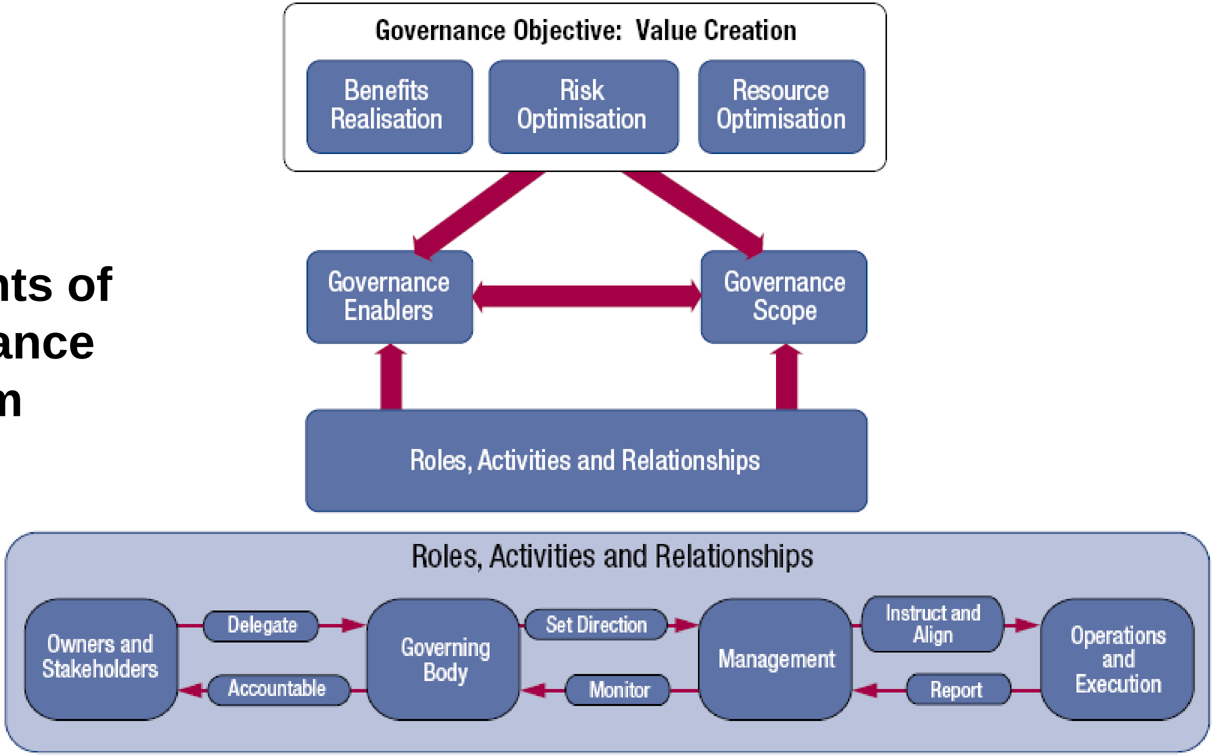
Meeting stakeholder needs



Source: COBIT® 5, figure 3. © 2012 ISACA® All rights reserved.

Covering the enterprise end-to-end

Key components of a governance system



Source: COBIT® 5, figure 3. © 2012 ISACA® All rights reserved.

Applying a single integrated framework

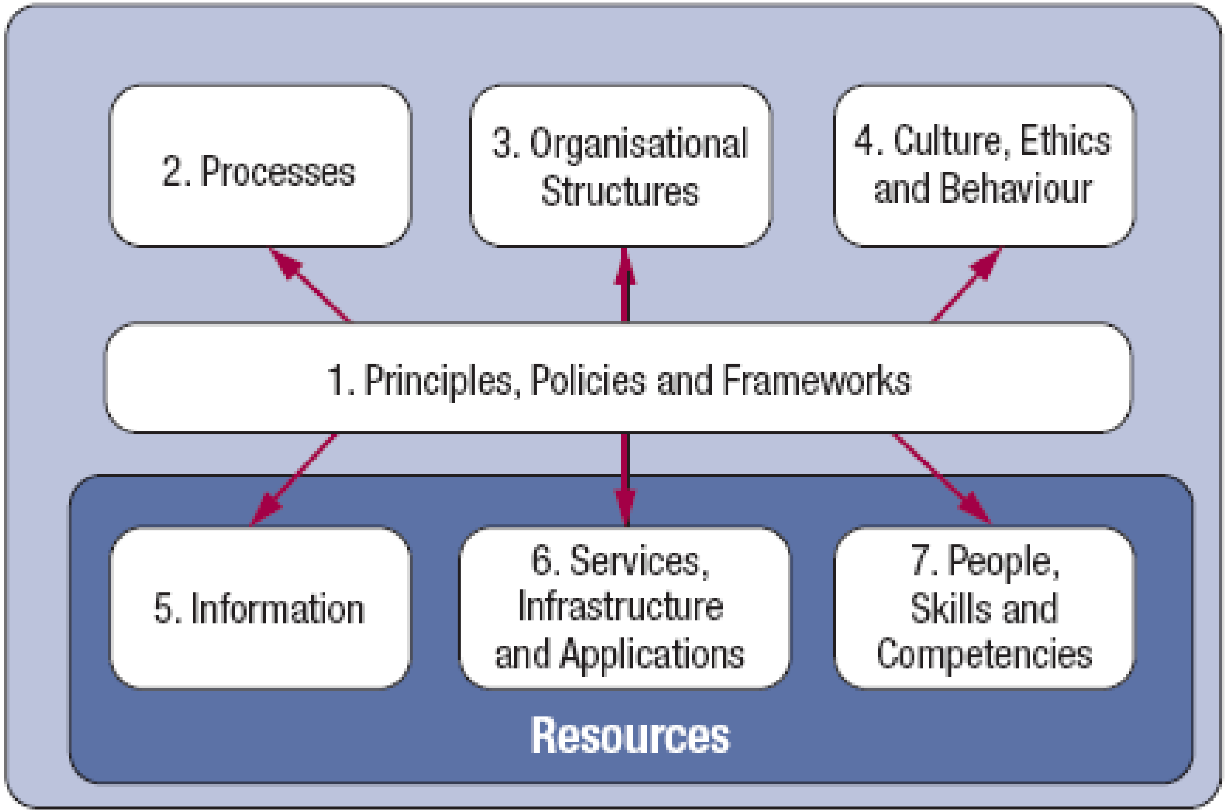
- **COBIT 5 aligns with the latest relevant other standards and frameworks used by enterprises:**
  - Enterprise: COSO, COSO ERM, ISO/IEC 9000 (quality management system), ISO/IEC 31000 (risk management)
  - IT-related: ISO/IEC 38500 (IT governance), ITIL, ISO/IEC 27000 series (information security related), TOGAF, PMBOK/PRINCE2, CMMI

ITIL: Information Technology Infrastructure Library
TOGAF: The Open Group Architecture Framework
*PRINCE: **PR**ojects **IN** **C**ontrolled **E**nvironments*

PMBOK: Project Management Body of Knowledge
CMMI: Capability Maturity Model Integration

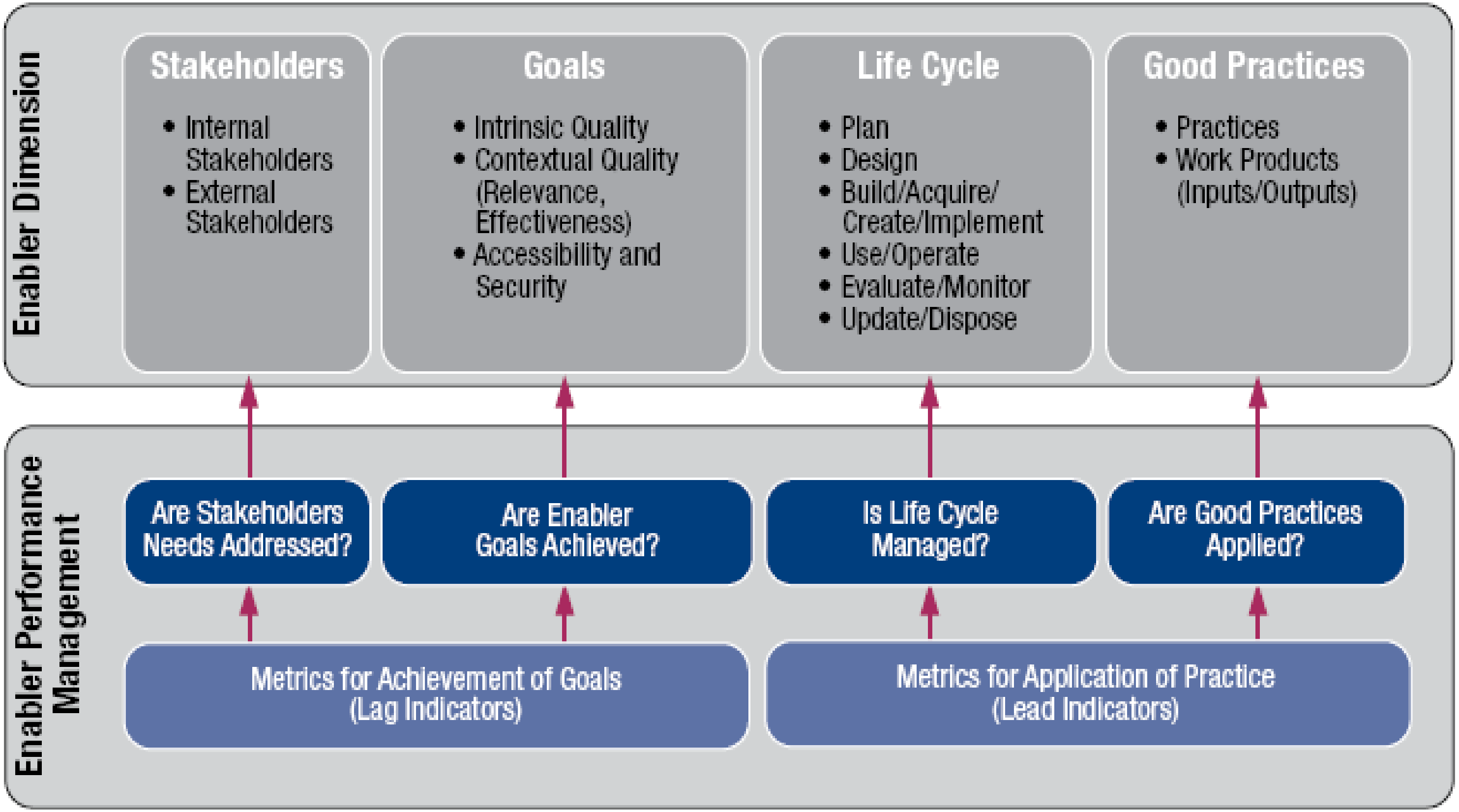
Source: COBIT® 5, figure 3. © 2012 ISACA® All rights reserved.

Enabling a holistic approach


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Source: COBIT® 5, figure 3. © 2012 ISACA® All rights reserved.

Enabling a holistic approach



Enabler Dimension

Stakeholders

- Internal Stakeholders
- External Stakeholders

Goals

- Intrinsic Quality
- Contextual Quality (Relevance, Effectiveness)
- Accessibility and Security

Life Cycle

- Plan
- Design
- Build/Acquire/ Create/Implement
- Use/Operate
- Evaluate/Monitor
- Update/Dispose

Good Practices

- Practices
- Work Products (Inputs/Outputs)

Enabler Performance Management

Are Stakeholders Needs Addressed?

Are Enabler Goals Achieved?

Is Life Cycle Managed?

Are Good Practices Applied?

Metrics for Achievement of Goals (Lag Indicators)

Metrics for Application of Practice (Lead Indicators)

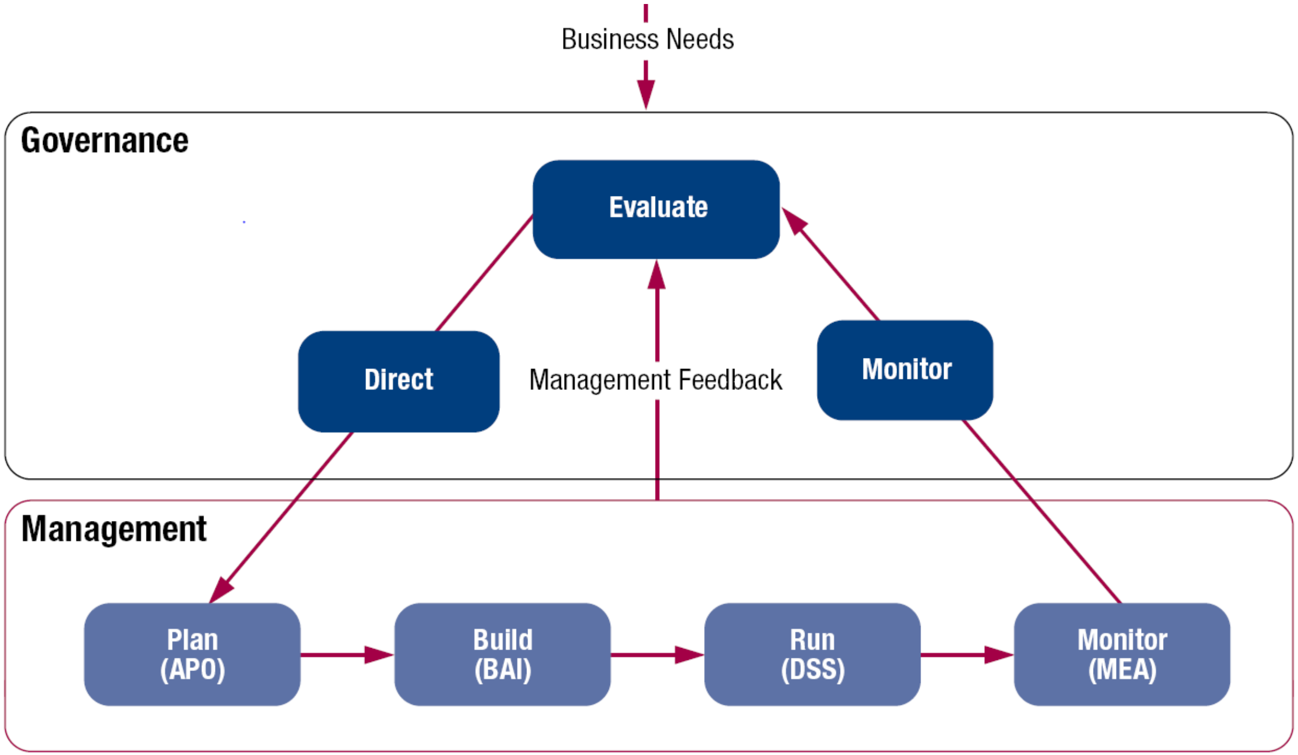
Source: COBIT® 5, figure 3. © 2012 ISACA® All rights reserved.

Separating governance from management

- **Governance—In most enterprises, governance is the responsibility of the board of directors under the leadership of the chairperson.**
  - Governance ensures that stakeholders needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives (EDM).
- **Management—In most enterprises, management is the responsibility of the executive management under the leadership of the CEO.**
  - Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM).

Source: COBIT® 5, figure 3. © 2012 ISACA® All rights reserved.

Separating governance from management



Business Needs

Governance

Evaluate

Direct

Management Feedback

Monitor

Management

Plan
(APO)

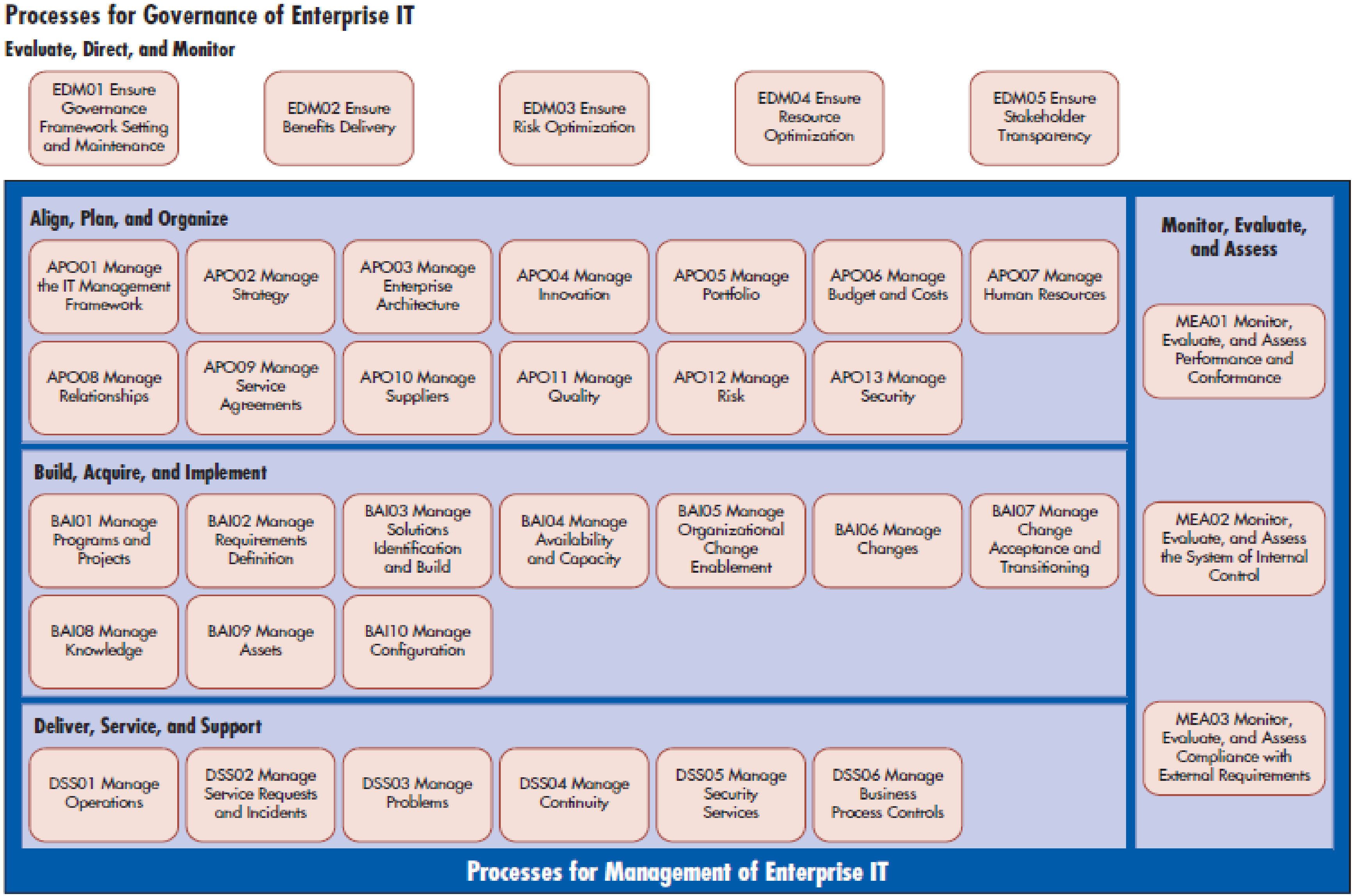
Build
(BAI)

Run
(DSS)

Monitor
(MEA)

APO: Align, plan, and organize
BAI: Build, acquire, and implement
DSS: Deliver, service, and support
MEA: Monitor, evaluate, and assess

Source: COBIT® 5, figure 3. © 2012 ISACA® All rights reserved.



Processes for Governance of Enterprise IT

Evaluate, Direct, and Monitor

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimization
- EDM04 Ensure Resource Optimization
- EDM05 Ensure Stakeholder Transparency

Align, Plan, and Organize

- APO01 Manage the IT Management Framework
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- APO08 Manage Relationships
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- APO12 Manage Risk
- APO13 Manage Security

Build, Acquire, and Implement

- BAI01 Manage Programs and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organizational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

Deliver, Service, and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

Monitor, Evaluate, and Assess

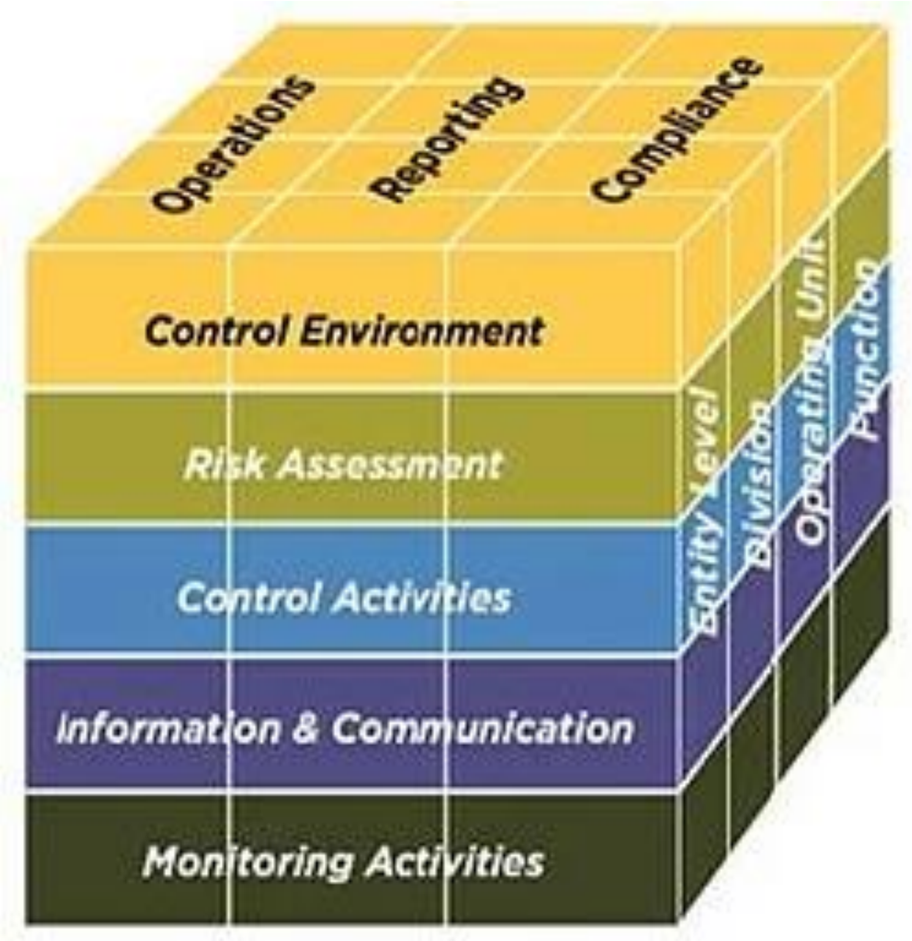
- MEA01 Monitor, Evaluate, and Assess Performance and Conformance
- MEA02 Monitor, Evaluate, and Assess the System of Internal Control
- MEA03 Monitor, Evaluate, and Assess Compliance with External Requirements

Processes for Management of Enterprise IT

II.ii COSO IC

Internal control framework COSO 1992

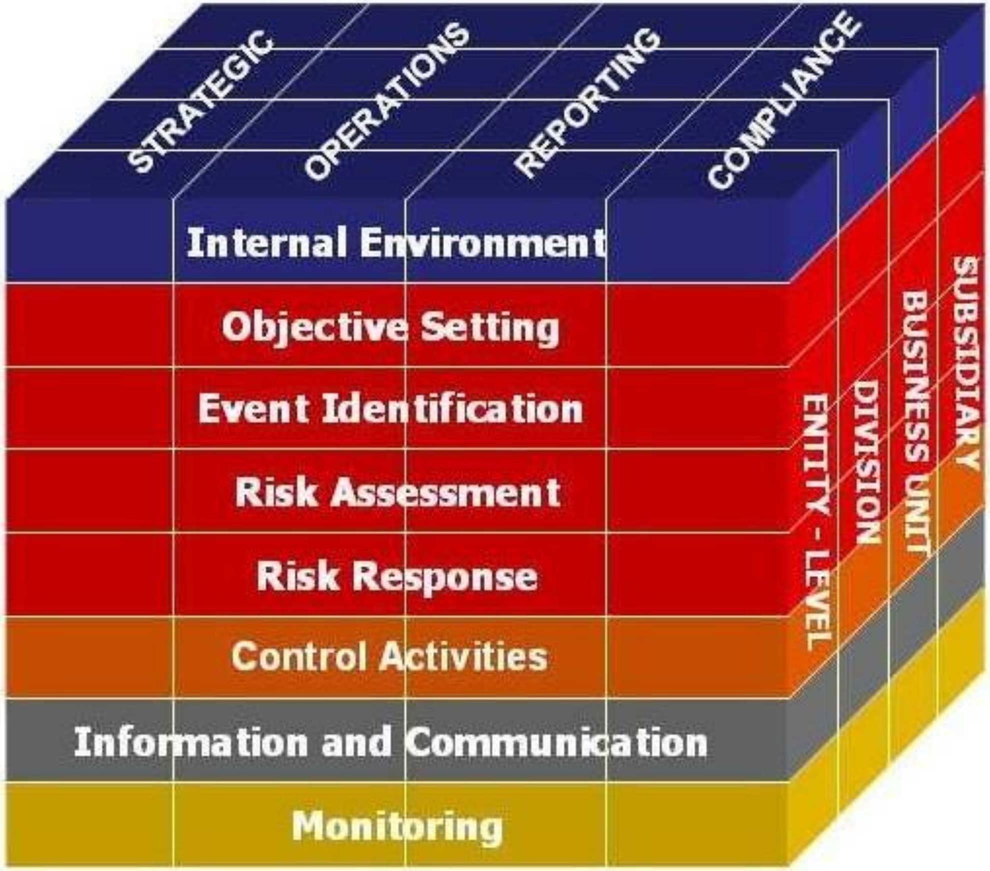
Committee of Sponsoring Organizations of the Treadway Commission (COSO)



II.iii COSO ERM

Risk management framework COSO 2004

Committee of Sponsoring Organizations of the Treadway Commission (COSO)



Components of COSO framework

COSO

- Control (internal) environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

COSO-ERM

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring

Internal environment

- Management’s philosophy, operating style, and risk appetite
- Commitment to integrity, ethical values, and competence
- Internal control oversight by Board of Directors
- Organizing structure
- Methods of assigning authority and responsibility
- Human resource standards

Objective setting

Strategic objectives	• High-level goals
Operations objectives	• Effectiveness and efficiency of operations
Reporting objectives	• Improve decision making and monitor performance
Compliance objectives	• Compliance with applicable laws and regulations

Event identification

Identifying incidents both external and internal to the organization that could affect the achievement of the organizations objectives

Key Management Questions:

What could go wrong?

How can it go wrong?

What is the potential harm?

What can be done about it?

Risk assessment

Risk is assessed from two perspectives:

Likelihood

- Probability that the event will occur

Impact

- Estimate potential loss if event occurs

Types of risk

Inherent

- Risk that exists before plans are made to control it

Residual

- Risk that is left over after you control it

Risk response

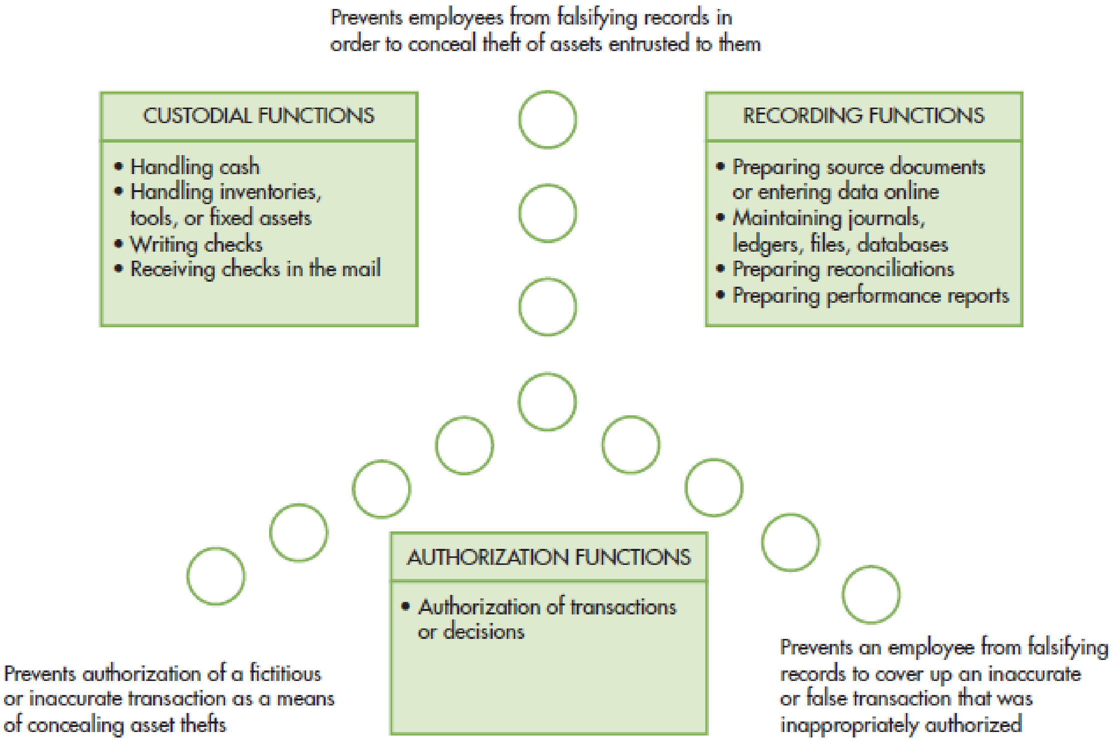
Reduce	• Implement effective internal control
Accept	• Do nothing, accept likelihood, and impact of risk
Share	• Buy insurance, outsource, or hedge
Avoid	• Do not engage in the activity

Control activities

- Proper authorization of transactions and activities
- Segregation of duties
- Project development and acquisition controls
- Change management controls
- Design and use of documents and records
- Safeguarding assets, records, and data
- Independent checks on performance

Information and communication

Segregation of accounting duties



Prevents employees from falsifying records in order to conceal theft of assets entrusted to them

CUSTODIAL FUNCTIONS

- Handling cash
- Handling inventories, tools, or fixed assets
- Writing checks
- Receiving checks in the mail

RECORDING FUNCTIONS

- Preparing source documents or entering data online
- Maintaining journals, ledgers, files, databases
- Preparing reconciliations
- Preparing performance reports

AUTHORIZATION FUNCTIONS

- Authorization of transactions or decisions

Prevents authorization of a fictitious or inaccurate transaction as a means of concealing asset thefts

Prevents an employee from falsifying records to cover up an inaccurate or false transaction that was inappropriately authorized

Information and communication

Segregation of systems duties as to divide authority and responsibility between the following systems functions

- System administration
- Network management
- Security management
- Change management
- Users
- Systems analysts
- Programmers
- Computer operators
- Information system librarian
- Data control

Monitoring

Perform internal control evaluations (e.g., internal audit)

Implement effective supervision

Use responsibility accounting systems (e.g., budgets)

Monitor system activities

Track purchased software and mobile devices

Conduct periodic audits (e.g., external, internal, network security)

Employ computer security officer

Engage forensic specialists

Install fraud detection software

Implement fraud hotline

III. Information security and control

Trust services framework

Security

- Access to the system and data is controlled and restricted to legitimate users.

Confidentiality

- Sensitive organizational data is protected.

Privacy

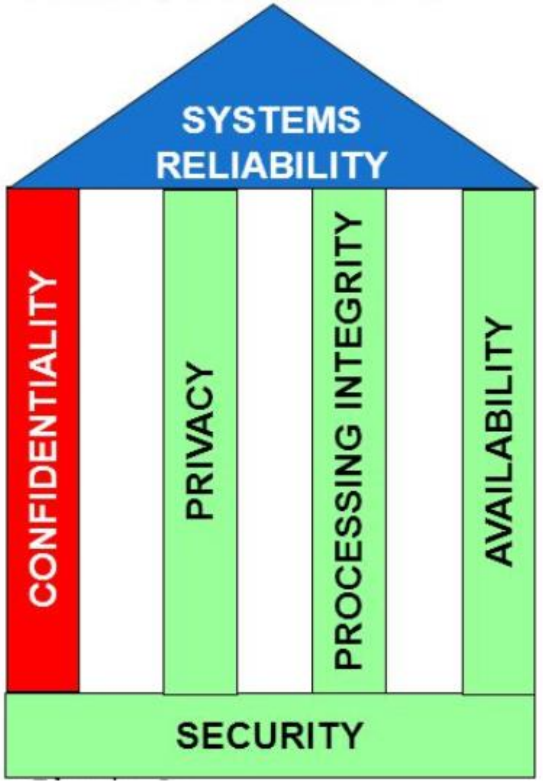
- Personal information about trading partners, investors, and employees are protected.

Processing integrity

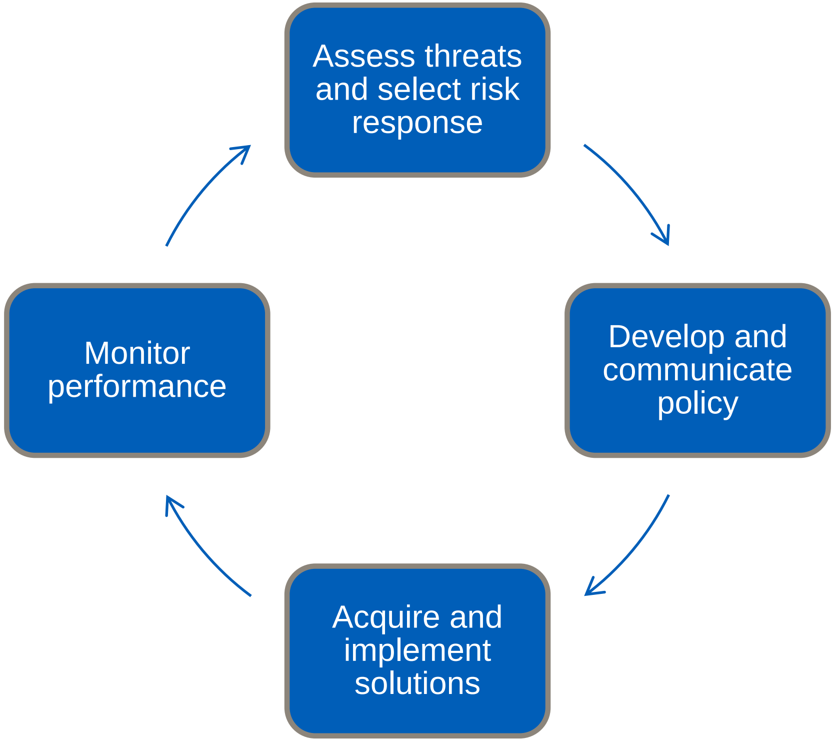
- Data are processed accurately, completely, in a timely manner, and only with proper authorization.

Availability

- System and information are available.



Security lifecycle: a management issue


Assess threats and select risk response
Develop and communicate policy
Acquire and implement solutions
Monitor performance

Time-based model, security is effective if:

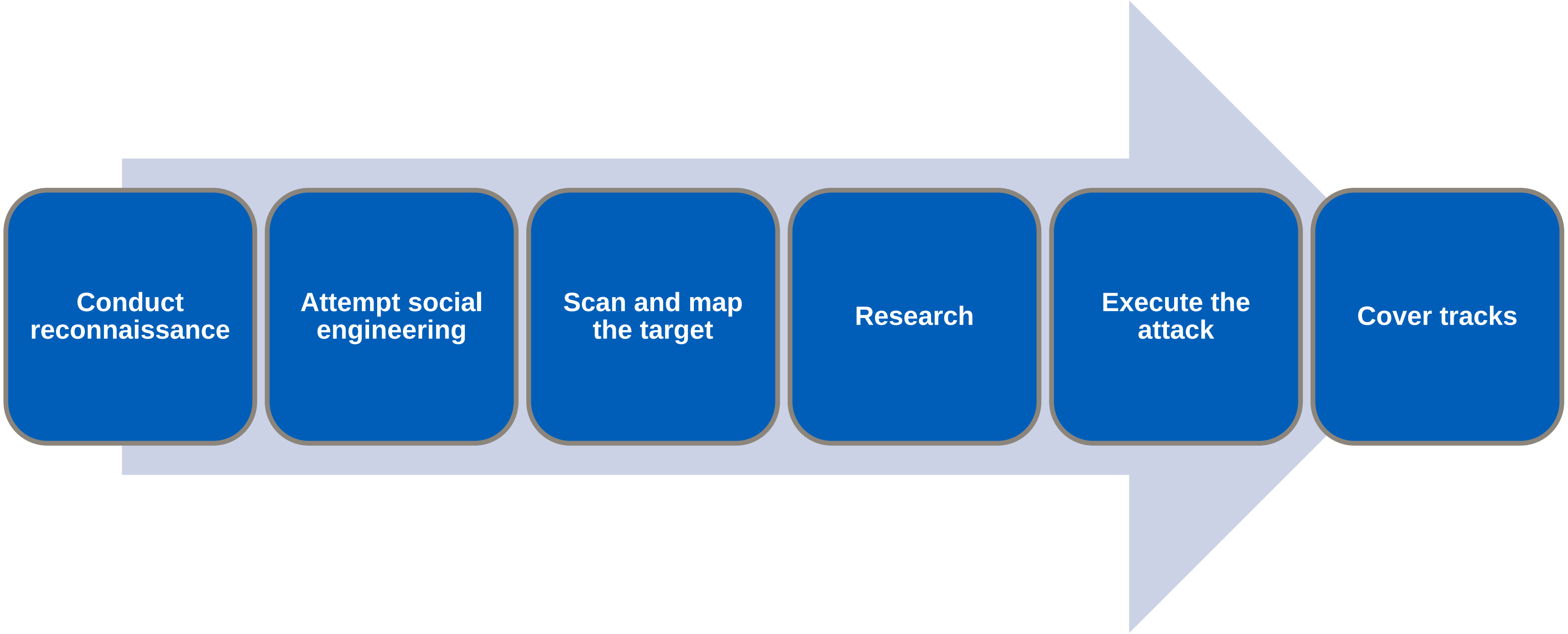
P > D + C where

P is time it takes an attacker to break through preventive controls

D is time it takes to detect an attack is in progress

C is time it takes to respond to the attack and take corrective action

Security breach process of criminals



Examples of different types of controls

Preventive Controls

- People
- Process
- IT Solutions
- Physical security

Detective Controls

- Log analysis
- Intrusion detection systems
- Continuous monitoring

Response / Corrective controls

- Computer Incident Response Teams (CIRT)
- Chief Information Security Officer (CISO)

Protecting confidentiality and privacy

Identify and classify information to protect

- Where is it located and who has access?
- Classify value of information to organization

Encryption

- Protect information in transit and in storage

Access controls

- Information Rights Management (IRM)
- Data loss prevention (DLP)
- Digital watermarks

Training

Processing integrity controls

Input Process Stage

- Forms design
  - *Sequentially prenumbered*
- Turnaround documents
- Cancelation and storage of source documents
- Data entry controls

Processing integrity: data entry controls

Field check	Characters in a field are proper type
Sign check	Data in a field is appropriate sign (positive/negative)
Limit check	Tests numerical amount against a fixed value
Range check	Tests numerical amount against lower and upper limits

Size check	Input data fits into the field
Completeness check	Verifies that all required data is entered
Validity check	Compares data from transaction file to that of master file to verify existence
Reasonableness test	Correctness of logical relationship between two data items
Check digit verification	Recalculating check digit to verify data entry error has not been made

Additional data entry controls

Batch processing

- Sequence check -Test of batch data in proper numerical or alphabetical sequence
- Batch totals - Summarize numeric values for a batch of input records
  - Financial total
  - Hash total
  - Record count

Prompting

- System prompts you for input (online completeness check)

Closed-loop verification

- Checks accuracy of input data by using it to retrieve and display other related information (e.g., customer account # retrieves the customer name)

Output controls

User review of output

Reconciliation procedures

- Procedures to reconcile to control reports (e.g., general ledger A/R account reconciled to Accounts Receivable Subsidiary Ledger)
- External data reconciliation

Data transmission controls

- Checksums
- Parity bits