J. A. "Drew" Hamilton, Jr., Ph.D.

Chair, NSA Cyber Operations Community of Practice

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

This work funded by NSA Contract #H98230-19-1-0291

CCI
2 Research Blvd.
Starkville, MS 39759

Voice: (662) 325-2294
Fax: (662) 325-7692
drew@drew-hamilton.com

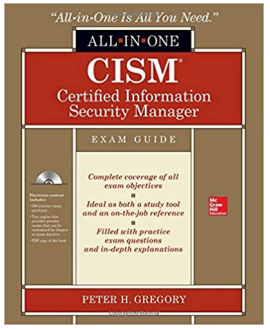
Domain 1 Information Security Governance

References:

Drew Hamilton Lecture Notes

CISM Review Manual, 15th Edition

CISM All-in-One Exam Guide, 1st Edition



Domain Outline

- Introduction and Certification
- Information Security Governance
- Organizational Roles and Responsibilities
- Information Security Governance Metrics
- Information Security Strategy
- Information Security Program Objectives
- Strategy Resources
- Strategy Constraints and Action Plan for Strategy Implementation

Introduction and Certification

Domain 1
Information Security Governance

Source:
ISACA CISM Review Manual 15th Edition

ISACA

- As a nonprofit, global membership association for IT and information systems professionals, ISACA is committed to providing its diverse constituency of more than 140,000 professionals worldwide with the tools they need to achieve individual and organizational success.
- Through more than 200 chapters established in more than 80 countries, ISACA provides its members with education, resource sharing, advocacy, professional networking, and a host of other benefits on a local level.

ISACA Membership

- COBIT
- ISACA.ORG
  - Dedicated to industry-accepted practices and high professional standards
  - Serious about enhancing their professional knowledge and skills
  - Connected with the standards, resources and global network of colleagues that only ISACA can provide
- Certifications

Certified Information System Management

- The management-focused CISM is the globally accepted standard for individuals who design, build and manage enterprise information security programs. CISM is the leading credential for information security managers.
- The recent quarterly *IT Skills and Certifications Pay Index* (ITSCPI) from Foote Partners ranked CISM among the most sought-after and highest-paying IT certifications.
- DOD 8140 compliant

Preparing for the CISM Exam

- Use multiple resources
- Consider ISACA Membership
- NIST Publications
- CISM Self-Assessment
  - http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Prepare-for-the-Exam/Pages/CISM-Self-Assessment.aspx

DoD Approved Baseline Certifications

Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+ CE CCNA-Security Network+ CE SSCP	CCNA Security CSA+ GICSP GSEC Security+ CE SSCP	CASP CE CCNP Security CISA CISSP (or Associate) GCED GCIH
IAM Level I	**IAM Level II**	**IAM Level III**
CAP GSLC Security+ CE	CAP CASP CE CISM CISSP (or Associate) GSLC	CISM CISSP (or Associate) GSLC
IASAE I	**IASAE II**	**IASAE III**
CASP CE CISSP (or Associate) CSSLP	CASP CE CISSP (or Associate) CSSLP	CISSP-ISSAP CISSP-ISSEP
CSSP Analyst	**CSSP Infrastructure Support**	**CSSP Incident Responder**
CEH CFR CSA+ GCIA GCIH GICSP SCYBER	CEH CSA+ GICSP SSCP	CEH CFR CSA+ GCFA GCIH SCYBER
CSSP Auditor	**CSSP Manager**	
CEH CSA+ CISA GSNA	CISM CISSP-ISSMP	

CSIAC
Cyber Security & Information Systems Information Analysis Center
266 Genese Street
Utica, NY 13502
Phone: 1-800-214-7921

Build and Operate a Trusted DoDIN

Cybersecurity-Related Policies and Issuances
Developed by the DoD Deputy CIO for Cybersecurity
Last Updated: January 7, 2019
Send questions/suggestions to
info@csiac.org

ORGANIZE

Lead and Govern

- EO 13800: Strengthening Cybersecurity of Fed Nets and CI
- EO 13636: Improving Critical Infrastructure Cybersecurity
- PPD 41: United States Cyber Incident Coordination
- PPD 21: Critical Infrastructure Security and Resilience
- National Cyber Strategy
- U.S. Int'l Strategy for Cyberspace
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- 2017 National Security Strategy
- National Defense Strategy (NDS)
- CNSSP-24 Policy on Assured Info Sharing (AIS) for National Security Systems(NSS)
- DoDD 8000.01 Management of the DOD Information Enterprise
- DoDI 8500.01 Cybersecurity
- 2018 DoD Cyber Strategy
- DoD Defending Networks, Systems and Data Strategy
- DoD Information Technology Environment Strategic Plan
- National Military Strategy (NMS)
- National Military Strategy for Cyberspace Operations (NMS-CO)
- National Military Strategic Plan for the War on Terrorism

ORGANIZE

Design for the Fight

- NIST SP 800-119 Guidelines for the Secure Deployment of IPv6
- Common Criteria Evaluation and Validation Scheme (CCEVS)
- CNSSP-11 Nat'l Policy Governing the Acquisition of IA and IA-Enable IT
- DFARS Subpart 208.74, Enterprise Software Agreements
- DoDD 5000.01 The Defense Acquisition System
- DoDD 7045.20 Capability Portfolio Management
- DoDI 8115.01 IT Portfolio Management
- DoDI 5000.02 Operation of the Defense Acquisition System
- DoDI 5200.44 Protection of Mission Critical Functions to Achieve TSN
- DoDI 7000.14 Financial Management Policy and Procedures (FPPBE)
- DoDI 8115.02 IT Portfolio Management Implementation
- DoDI 8310.01 Information Technology Standards in the DoD
- DoDI 8330.01 Interoperability of IT and National Security Systems (NSS)
- DoDI 8510.01 Risk Management Framework for DoD IT
- DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System
- RMF Knowledge Service
- MOA between DoD CIO and ODNI CIO Establishing Net-Centric Software Licensing Agreements
- DODAF (Version 2.02) DoD Architecture Framework
- CJCSI 31 Joint Capabilities I Development Sy
- Joint Publication 6-0 Joint Communications System
- CNSS National Secret Fabric Architecture Recommendations
- MOA Between DoD and DHS (Jan. 19, 2017, requires CAC)

Develop the Workforce

- CNSSD-500 Information Assurance (IA) Education, Training, and Awareness
- NSTISSD-501 National Training Program for INFOSEC Professionals
- CNSSI-4000 Maintenance of Communications Security (COMSEC) Equipment
- NSTISSI-4011 National Training Standard for INFOSEC Professionals
- CNSSI-4012 National IA Training Standard for Senior Systems Managers
- CNSSI-4013 National IA Training Standard For System Administrators (SA)
- CNSSI-4014 National IA Training Standard For Information Systems Security Officers
- NSTISSI-4015 National Training Standard for System Certifiers
- CNSSI-4016 National IA Training Standard For Risk Analysts
- DoDD 8140.01 Cyberspace Workforce Management
- DoD 8570.01-M Information Assurance Workforce Improvement Program
- DoDI 8550.01 DoD Internet Services and Internet-Based Capabilities

Partner for Strength

- NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
- NIST SP 800-171, R1 Protecting CUI in Nonfederal Systems and Organizations
- CNSSP-14 National Policy Governing the Release of IA Products/Services…
- CNSSI-1253 Security Categorization and Control Selection for Nat'l Security Systems
- CNSSI-1253F, Atchs 1-5 Security Overlays
- CNSSI-4007 Communications Security (COMSEC) Utility Program
- CNSSI-4008 Program for the Mgt and Use of Nat'l Reserve IA Security Equipment
- DoDI 5205.13 Defense Industrial Base Cyber Security / IA Activities
- DoD 5220.22-M, Ch. 2 National Industrial Security Program Operating Manual (NISPOM)
- ICD 503 IT Systems Security Risk Management and C&A

ENABLE

Secure Data in Transit

- FIPS 140-2 Security Requirements for Cryptographic Modules
- NIST SP 800-153 Guidelines for Securing Wireless Local Area Networks
- CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material
- CNSSP-15 Use of Pub Standards for Secure Sharing of Info Among NSS
- CNSSP-17 Policy on Wireless Communications: Protecting Nat'l Security Info
- CNSSP-19 National Policy Governing the Use of HAIPE Products
- CNSSP-25 National Policy for PKI in National Security Systems
- NSTISSP-101 National Policy on Securing Voice Communications
- *NACSI-2005 Communications Security (COMSEC) End Item Modification*
- CNSSI-5000 Voice Over Internet Protocol (VoIP) Computer Telephony (Annex I, VoSIP)
- CNSSI-5001 Type-Acceptance Program for VoIP Telephones
- NACSI-6002 Nat'l COMSEC Instruction Protection of Gov't Contractor Telecomm's
- CNSSI-7003 Protected Distribution Systems (PDS)
- DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG
- DoDD 8521.01E Department of Defense Biometrics
- DoDI 4650.01 Policy and Procedures for Mgt and Use of the Electromagnetic Spectrum
- DoDI 8100.04 DoD Unified Capabilities (UC)
- DoDI 8420.01 Commercial WLAN Devices, Systems, and Technologies
- DoDI 8523.01 Communications Security (COMSEC)
- DoDI S-5200.16 Objectives and Min Stds for COMSEC Measures used in NC2 Comms
- *CJCSI 6510.02E Cryptographic Modernization Plan*
- *CJCSI 6510.06C Communications Security Releases to Foreign Nations*

Manage Access

- HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors
- FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors
- CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information
- CNSSP-16 National Policy for the Destruction of COMSEC Paper Material
- CNSSI-1300 Instructions for NSS PKI X.509
- NSTISSI-3028 Operational Security Doctrine for the FORTEZZA User PCMCIA Card
- CNSSI-4001 Controlled Cryptographic Items
- CNSSI-4003 Reporting and Evaluating COMSEC Incidents
- CNSSI-4005 Safeguarding COMSEC Facilities and Materials, amended by CNSS-008-14
- CNSSI-4006 Controlling Authorities for COMSEC Material
- DoDI 1000.25 DoD Personnel Identity Protection (PIP) Program
- DoDI 5200.01 DoD Information Security Program and Protection of SCI
- DoDI 5200.08 Security of DoD Installations and Resources and the DoD PSRB
- DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling
- DoDI 8520.03 Identity Authentication for Information Systems
- DoDM 1000.13, Vol. 1 DoD ID Cards: ID Card Life-cycle

Assure Information Sharing

- DoDI 8320.02 Sharing Data, Info, and IT Services in the DoD
- DoDI 8582.01 Security of Unclassified DoD Information on Non-DoD Info Systems
- DoD Information Sharing Strategy
- United States Intelligence Community Information Sharing Strategy
- CJCSI 6211.02D Defense Information System Network: (DISN) Responsibilities
- *CJCSM 3213.02D, Joint Staff Focal Point*

ANTICIPATE

Understand the Battlespace

- FIPS 199 Standards for Security Categorization of Federal Info. and Info. Systems
- NIST SP 800-59 Guideline for Identifying an Information System as a NSS
- NIST SP 800-60, Vol 1, R1 Guide for Mapping Types of Info and Info Systems to Security Categories
- NIST SP 800-92 Guide to Computer Security Log Management
- NIST SP 800-101, R1 Guidelines on Mobile Device Forensics
- NISTIR 7693 Specification for Asset Identification 1.1
- CNSSP-28 Cybersecurity of Unmanned National Security Systems
- DoDI S-5240.23 Counterintelligence (CI) Activities in Cyberspace

Prevent and Delay Attackers and Prevent Attackers from Staying

- FIPS 200 Minimum Security Requirements for Federal Information Systems
- NIST SP 800-37 R1 Guide for Applying the Risk Mgt Framework to Fed. Info. Systems
- NIST SP 800-53 R4 Security & Privacy Controls for Federal Information Systems
- NIST SP 800-53A R4 Assessing Security & Privacy Controls in Fed. Info. Systems & Orgs.
- NIST SP 800-61, R2 Computer Security Incident Handling Guide
- NIST SP 800-124, R1 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-128 Guide for Security-Focused Configuration Mgt of Info Systems
- CNSSAM IA 1-10, Reducing Risk of Removable Media in NSS
- DoDI 5200.39 CPI Identification and Protection within RDT&E
- DoDI 8551.01 Ports, Protocols, and Services Management (PPSM)
- DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations
- DoD O-8530.1-M CND Service Provider Certification and Accreditation Program
- DoDM 5105.21V1, SCI Admin Security Manual: Info and Info Sys Security
- CJCSI 6510.01F Information Assurance (IA) and Computer Network Defense (CND)
- CJCSM 6510.01B Cyber Incident Handling Program
- *CJCSM 6510.02 IA Vulnerability Mgt Program*
- DTM 17-007, Defense Support to Cyber Incident Response

PREPARE

Develop and Maintain Trust

- CNSSP-12 National IA Policy for Space Systems Used to Support NSS
- CNSSP-21 National IA Policy on Enterprise Architectures for NSS
- NSTISSD-600 Communications Security (COMSEC) Monitoring
- CNSSI-5002, National Information Assurance (IA) Instruction for Computerized Telephone Systems
- DoDD 3020.40 Mission Assurance
- DoDD 3100.10 Space Policy
- DoDI 8581.01 IA Policy for Space Systems Used by the DoD
- DoDD 5144.02 DoD Chief Information Officer

Strengthen Cyber Readiness

- NIST SP 800-18, R1 Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-30, R1 Guide for Conducting Risk Assessments
- NIST SP 800-126, R3 SCAP Ver. 1.3
- NIST SP 800-137 Continuous Monitoring
- NIST SP 800-39 Managing Information Security Risk
- DoDD 3700.01 DoD Command and Control (C2) Enabling Capabilities
- DoDD S-3710.01 National Leadership Command Capability
- DoDI 8560.01 COMSEC Monitoring

Sustain Missions

- CNSSP-18 National Policy on Classified Information Spillage
- CNSSP-22, IA Risk Management Policy for National Security Systems
- *CNSSP-300 National Policy on Control of Compromising Emanations*
- CNSSI-1001 National Instruction on Classified Information Spillage
- *CNSSI-4004.1, Destruction and Emergency Protection Procedures for COMSEC and Class. Material*
- *CNSSI-7000 TEMPEST Countermeasures for Facilities*
- *NSTISSI-7001 NONSTOP Countermeasures*
- DoDD 3020.26 DoD Continuity Policy
- DoDD 3020.44 Defense Crisis Management
- DoDI 8410.02 NetOps for the Global Information Grid (GIG)
- Defense Acquisition Guidebook RMF for DoD IT
- *NSA IA Directorate (IAD) Management Directive MD-110 Cryptographic Key Protection*

AUTHORITIES

- Title 10 Armed Forces (§§2224, 3013(b), 5013(b), 8013(b))
- Title 14 Cooperation With Other Agencies (Ch. 7:§§ 141,144,145,148,149,150)
- Title 32 National Guard (§102)
- Title 40 Public Buildings, Property, and Works (Ch. 113: §§11302, 11315, 11331)
- Title 44 Federal Information Security Mod. Act, (Chapter 35)
- Title 50 War and National Defense (§§3002, 1801)
- Clinger-Cohen Act, Pub. L. 104-106
- UCP Unified Command Plan (US Constitution Art II, Title 10 & 50)

NATIONAL / FEDERAL

- Computer Fraud and Abuse Act Title 18 (§1030)
- Federal Wiretap Act Title 18 (§2510 et seq.)
- Stored Communications Act Title 18 (§2701 et seq.)
- Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)
- Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)
- Executive Order 13231 as Amended by EO 13286 - Critical Infrastructure Protection in the Info Age
- Executive Order 13526 Classified National Security Information
- Executive Order 13587 Structural Reforms To Improve Classified Nets
- Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing
- NSD 42, National Policy for the Security of Nat'l Security Telecom and Information Systems
- PPD 28, Signals Intelligence Activities
- *NSPD 54 / HSPD 23 Computer Security and Monitoring*
- A-130, Management of Fed Info Resources
- FAR Federal Acquisition Regulation
- Ethics Regulations
- National Strategy to Secure Cyberspace
- NIST Special Publication 800 Series
- NIST SP 800-125A, R1, Security Recommendations for Hypervisor Platforms
- NISTIR 7298, R2, Glossary of Key Information Security Terms
- CNSSD-502 National Directive On Security of National Security Systems
- CNSSD-900, Governing Procedures of the Committee on National Security Systems
- CNSSD-901 Nat'l Security Telecomm's and Info Sys Security (CNSS) Issuance System
- CNSSI-4009 Cmte on National Security Systems Glossary

OPERATIONAL

- *SI 527-01 DoD INFOCON System Procedures*
- *SI 504-04 Readiness Reporting*
- *SI 507-01 NetOps Community of Interest (NCOI) Charter*
- *SI 701-01 NetOps Reporting*
- *STRATCOM CONPLAN 8039-08*
- *STRATCOM OPLANs*
- *Computer Network Directives (CTO, FRAGO, WARNORD)*

SUBORDINATE POLICY

- Security Configuration Guides (SCGs)
- *Component-level Policy (Directives, Instructions, Publications, Memoranda)*
- *Security Readiness Review Scripts (SRRs)*
- Security Technical Implementation Guides (STIGs)

ABOUT THIS CHART

- This chart organizes cybersecurity policies and guidance by Strategic Goal and Office of Primary Responsibility (see Color Key). Double-clicking on the box directs users to the most authoritative publicly accessible source.
- *Policies in italics indicate the document is marked for limited distribution or no authoritative public-facing hyperlink is currently available.*
- The linked sites are not controlled by the developers of this chart. We check the integrity of the links on a regular basis, but you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.
- CNSS policies link only to the CNSS site, per restrictions implemented by its website design.
- Boxes with red borders reflect recent updates.
- Note: Users of the iPad, iPhone or iPod Touch may find they can view this Chart but that its hyperlinks are inoperable, because of Apple's decision not to fully support certain Adobe products. For those who desire a workaround for this issue, there are apps in the iTunes store for less than $1.00.
- For the latest version of this chart go to http://iac.dtic.mil/csiac/ia_policychart.html. You can sign up to be alerted by e-mail to any updates to this document.

Color Key - OPRs

- ASD(NII)/ASD(C3I) /DOD CIO
- CNSS/NSTISS
- DISA
- DNI
- JCS
- NIAP
- NIST
- NSA
- OSD
- STRATCOM
- USD(AT&L)
- USD(C)
- USD(I)
- USD(P)
- USD(P&R)
- Other Agencies
- Recently updated policy and/or link
- Expired, Update pending

Distribution Statement A: Approved for Public Release. Distribution is unlimited.

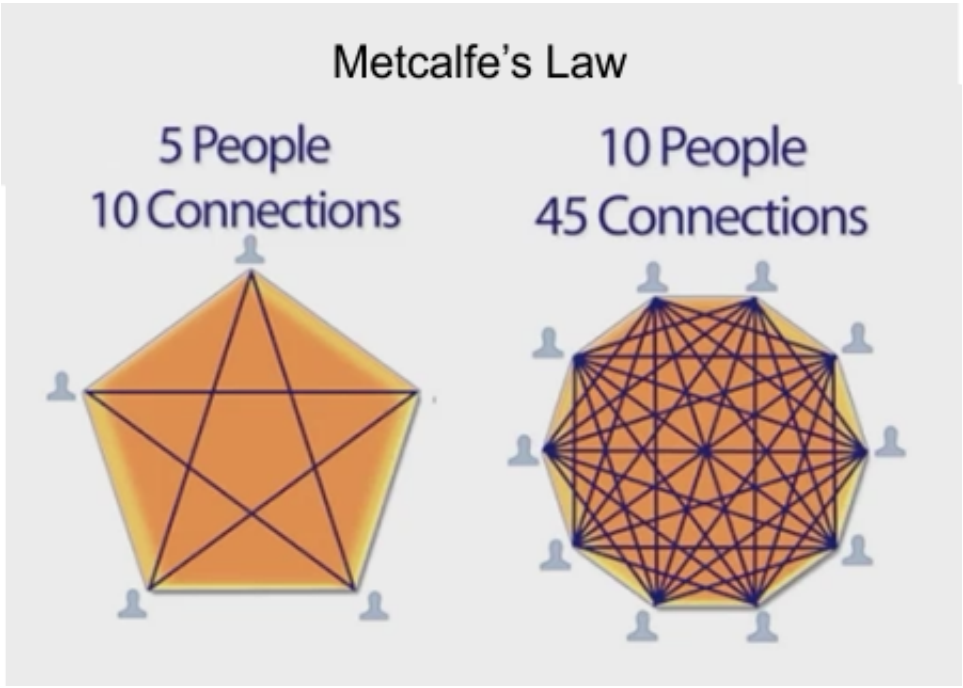
Information Security Governance Effective Information Security Governance

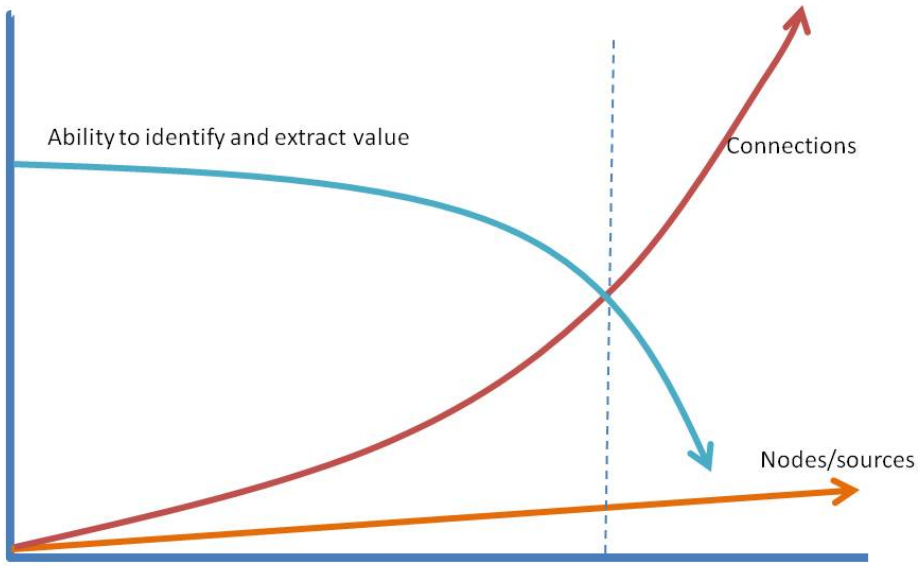
Domain 1
Information Security Governance

Introduction

- Information security governance is a subset of corporate governance and must be consistent with enterprise governance.
- Governance frameworks
  - COBIT
  - ISO/IEC 27000

Size Affects Governance (1 of 2)





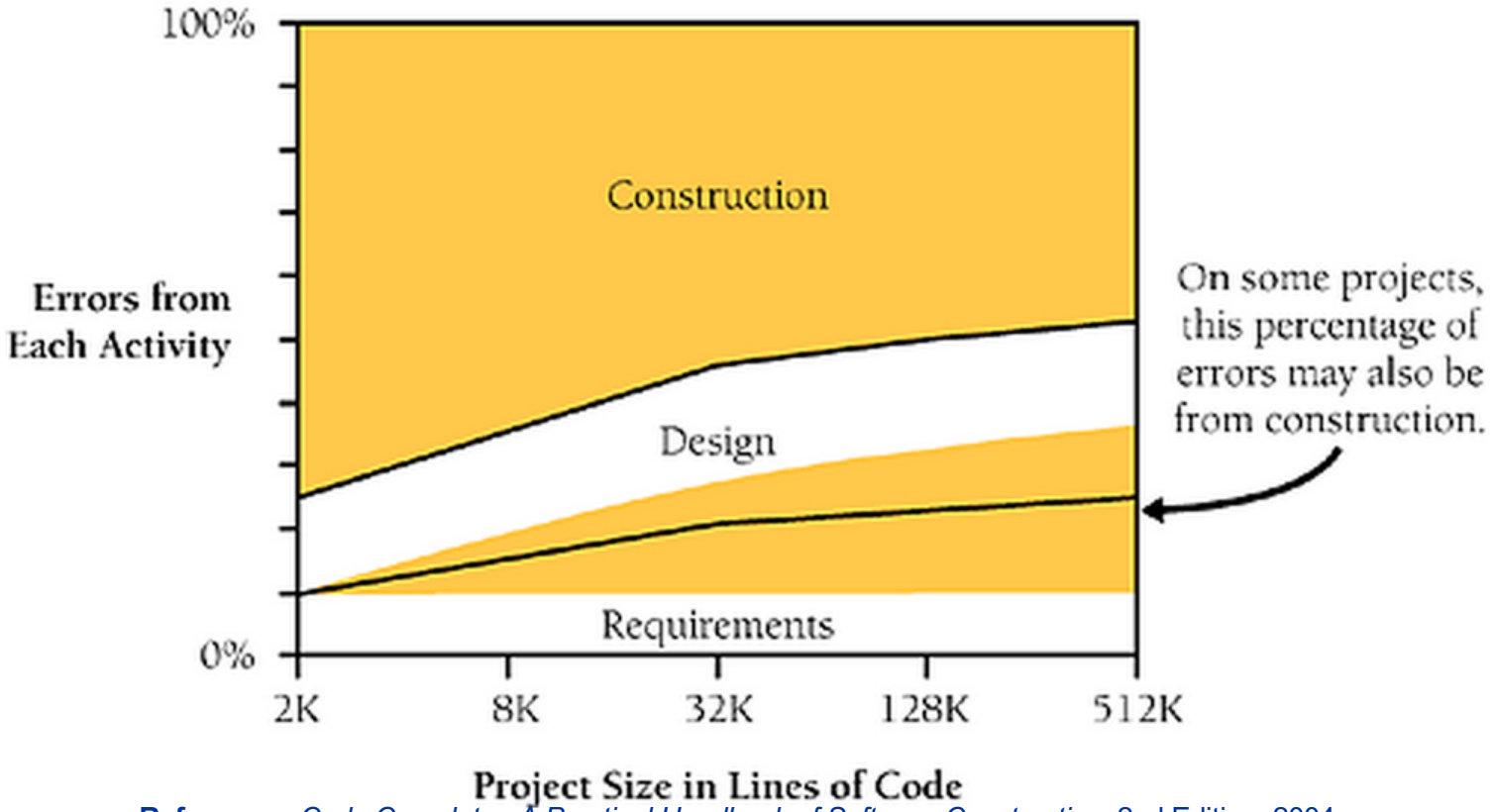
Number of connections (or interfaces) = n * (n – 1) / 2

Reference: *Code Complete: A Practical Handbook of Software Construction*, 2nd Edition, 2004

CISSP CBK Review Software Development Security Domain v. 5.10

Size Affects Governance (2 of 2)

- **"*As project size increases, errors usually come more from requirements and design…* (Boehm 1981, Grady 1987, Jones 1998)"**



Reference: *Code Complete: A Practical Handbook of Software Construction*, 2nd Edition, 2004

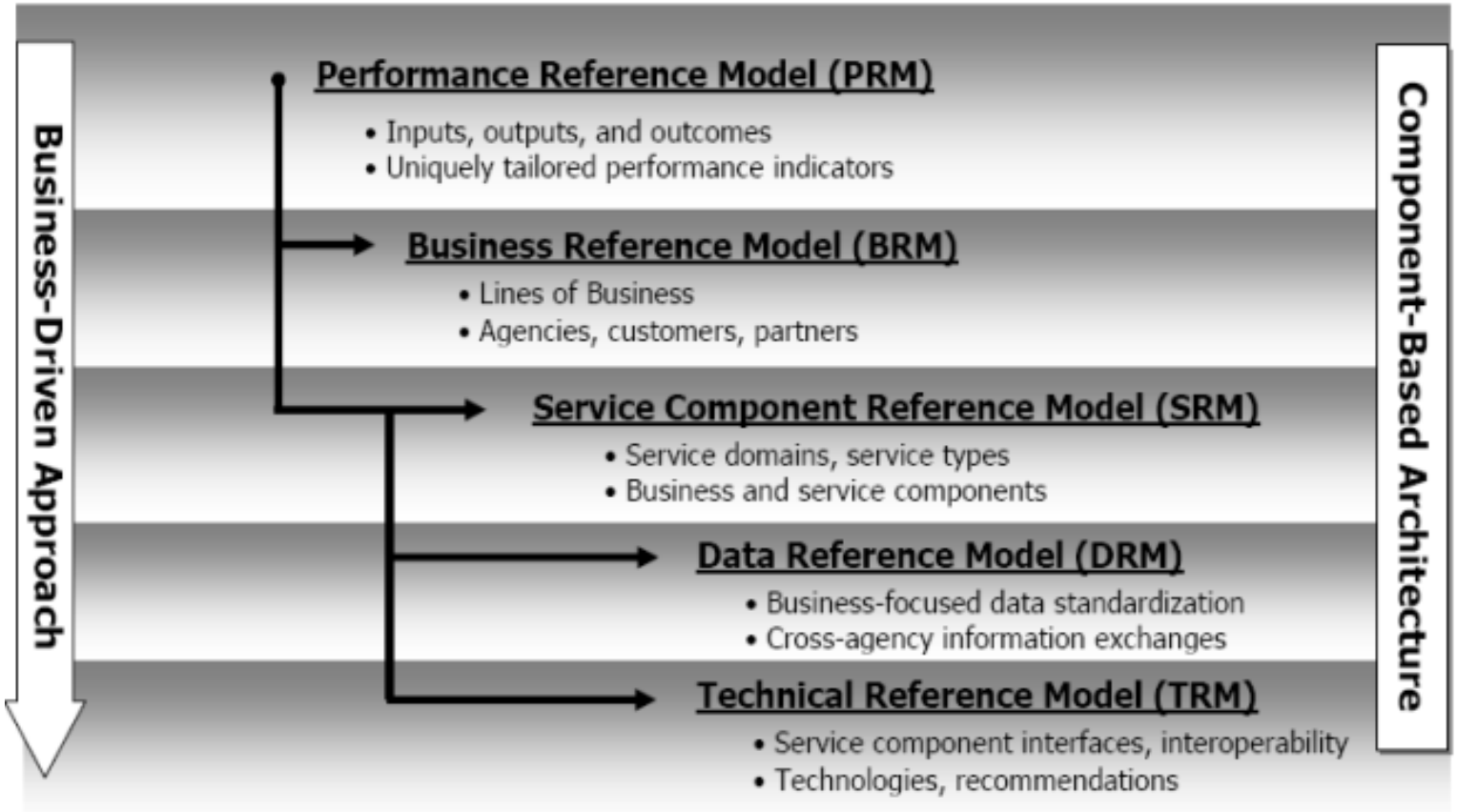
Clinger-Cohen Act of 1996 (CCA)

- The Clinger-Cohen Act of 1996 (a.k.a. ITMRA) defined the Federal agencies and DoD's acquisition, management, and usage of IT.
- Key Elements
  - Defines the roles & responsibilities of Federal agencies and their executives (i.e. directors and CIOs.)
  - Requires Federal agencies to implement performance and result-based management for capital planning and investment control (CPIC).
  - Defines the IT acquisition process.
  - Requires IT architecture be defined for all Federal agencies. (i.e. Federal Enterprise Architecture (FEA)).

CISSP CBK Review Software Development Security Domain v. 5.10

GFederal Enterprise Architecture (FEA) Framework

- **Federal Enterprise Architecture Framework (FEAF) focuses on BUSINESS**

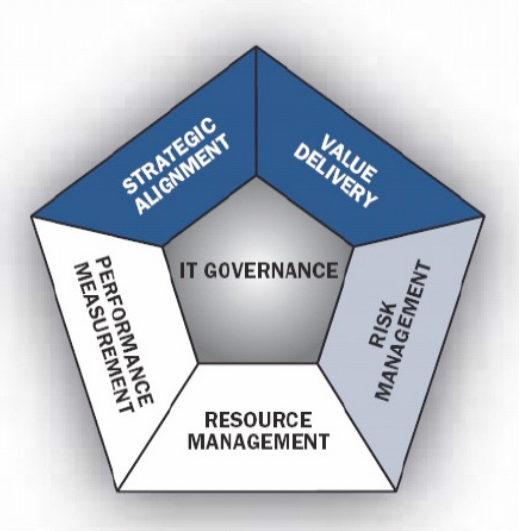


Reference: *Federal Enterprise Architecture Consolidated Reference Model, May 2005*

COBIT Governance Framework

- **Control Objectives for Information and related Technology (COBIT) is an IT Governance Framework created by Information Systems Audit and Control Association (ISACA)**
- **COBIT controls can encompass:**
  - **Information security controls (e.g., NIST SP 800-53, CNSS 1253, ISO/IEC 27001:2005)**
  - **IT processes management frameworks (e.g., ITIL, CMMI, ISO/IEC 27000 IT Service Management, PMBOK)**
- **COBIT governance is composed of 5 focus areas:**
  - **Strategic alignment**
  - **Value delivery**
  - **Resource management**
  - **Risk management**
  - **Performance measurement**

Reference: *COBIT 4.1* (http://www.isaca.org/)



What is IT Governance (MITRE)

A framework

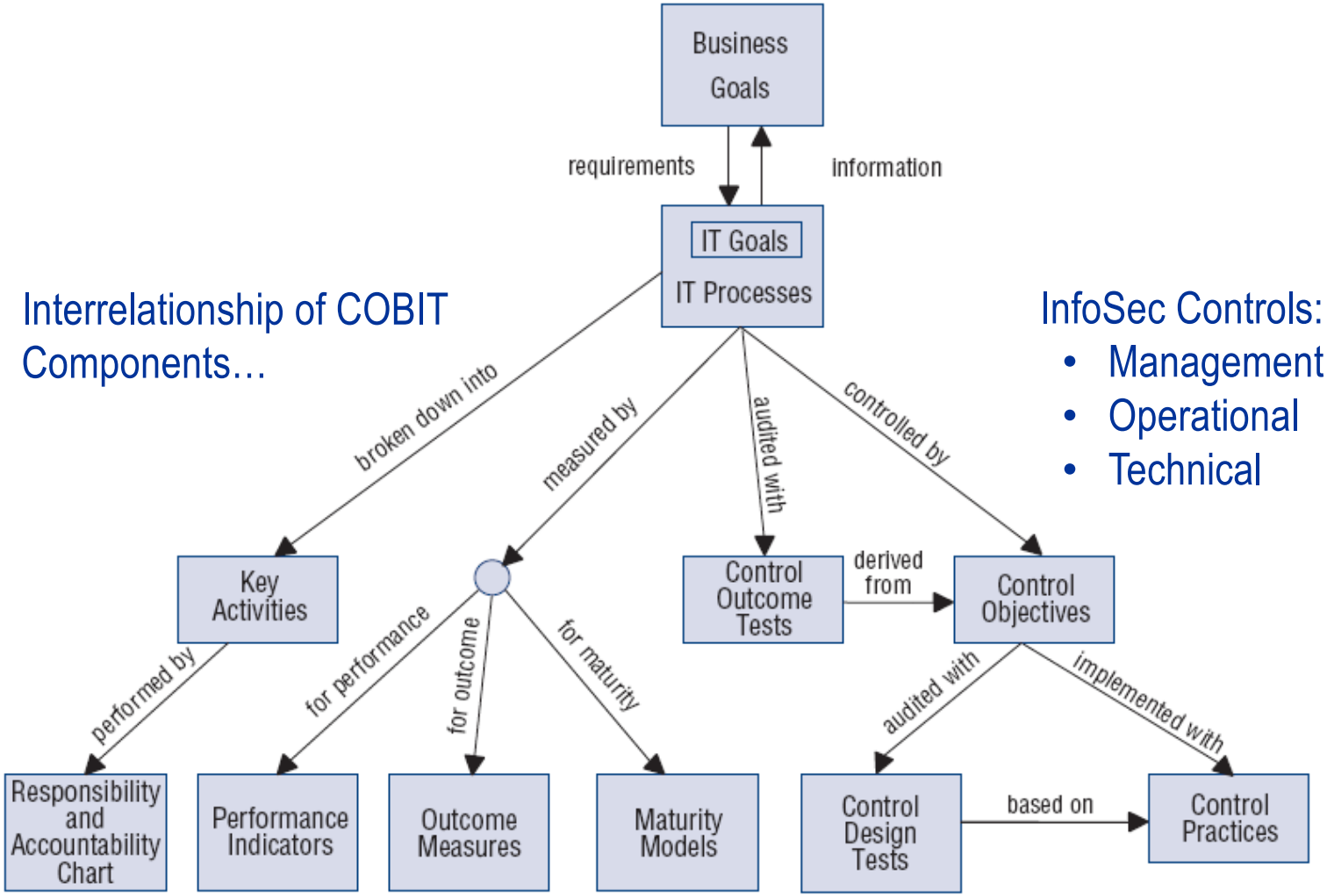
- for establishing the methods for decision making (not making the decisions themselves)

Objectives

- Strong stakeholder and customer partnerships
- Effective business processes
- Balanced portfolio
- Predictable investment performance and costs

Augment IT Governance with Information Security

Interrelationship of COBIT Components…



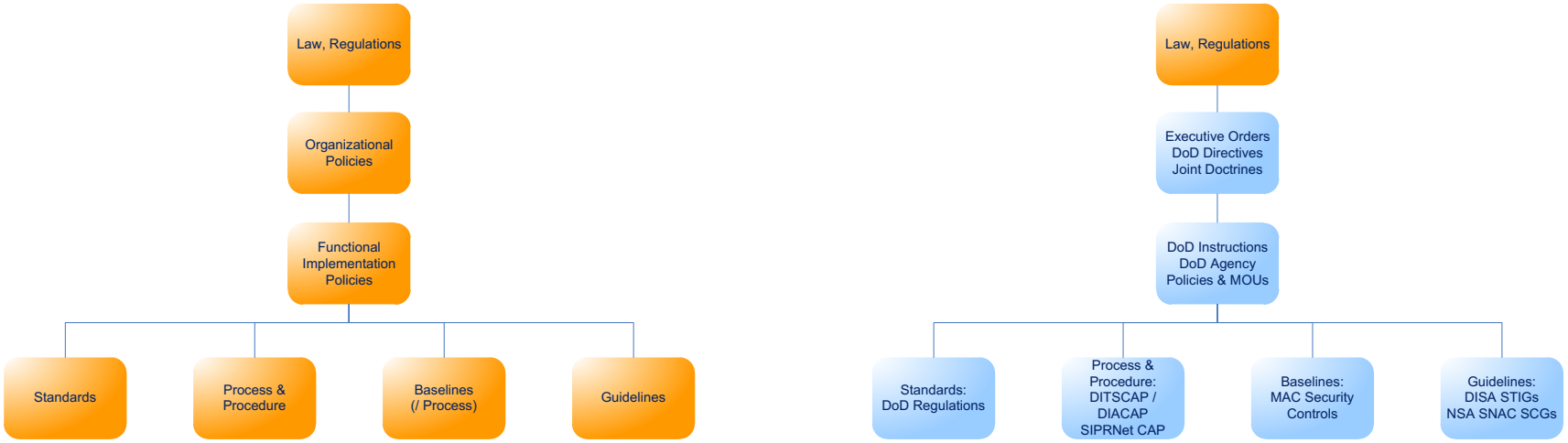
InfoSec Controls:

- Management
- Operational
- Technical

- **Information security is an ubiquitous practice…**

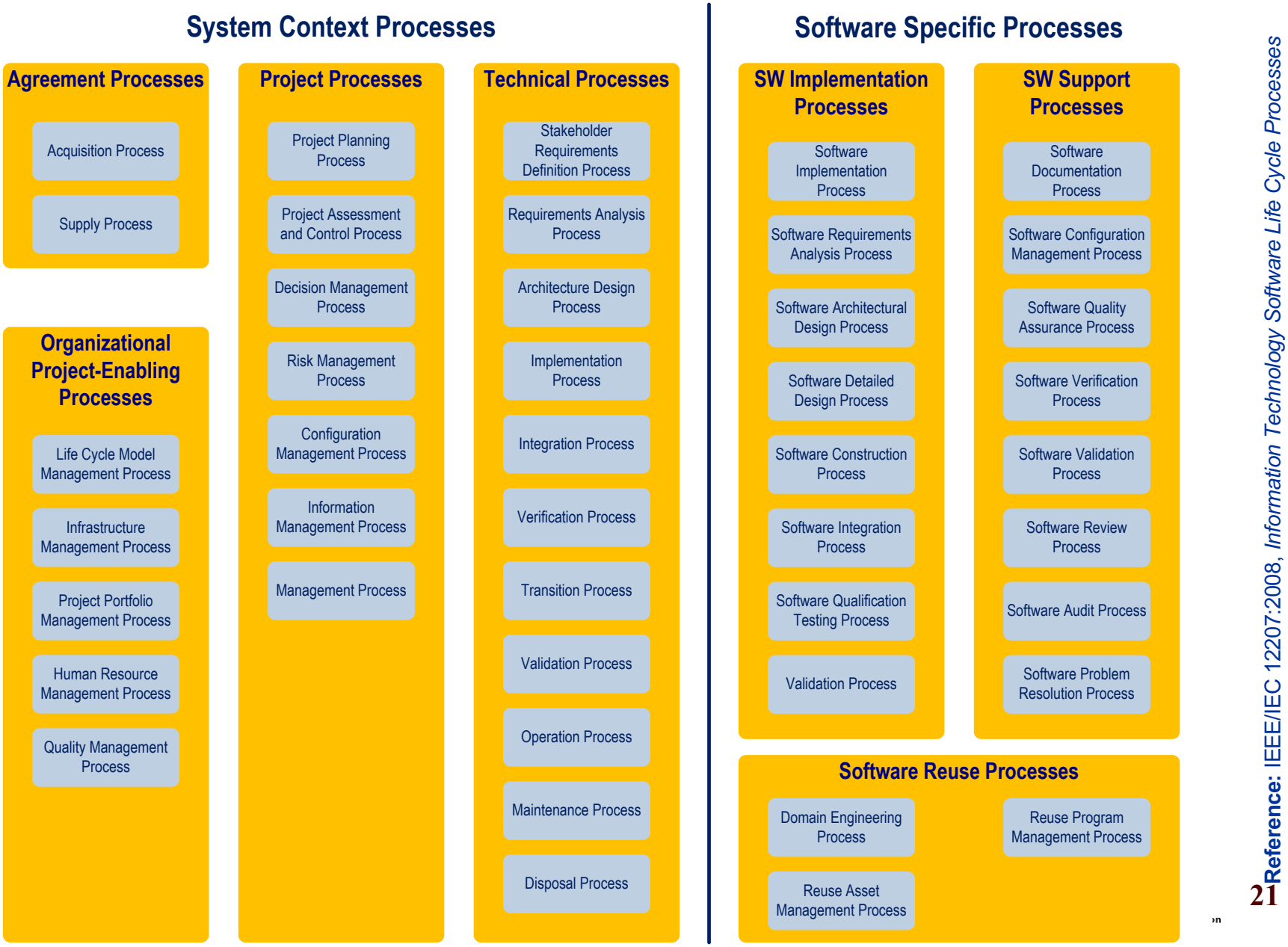
Reference: *COBIT 4.1* (http://www.isaca.org/)

Information Security Governance



- **Policy. Management directives that establish expectations (goals & objectives), and assign roles & responsibilities.**
- **Standards. Functional specific mandatory activities, actions, and rules.**
- **Procedure. Step-by-step implementation instructions.**
- **Baseline (or Process). Mandatory description of how to implement security packages to ensure consistent security posture.**
- **Guidelines. General statement, framework, or recommendations to augment baselines or procedures.**

ISO/IEC 12207:2008, Software Life Cycle Processes



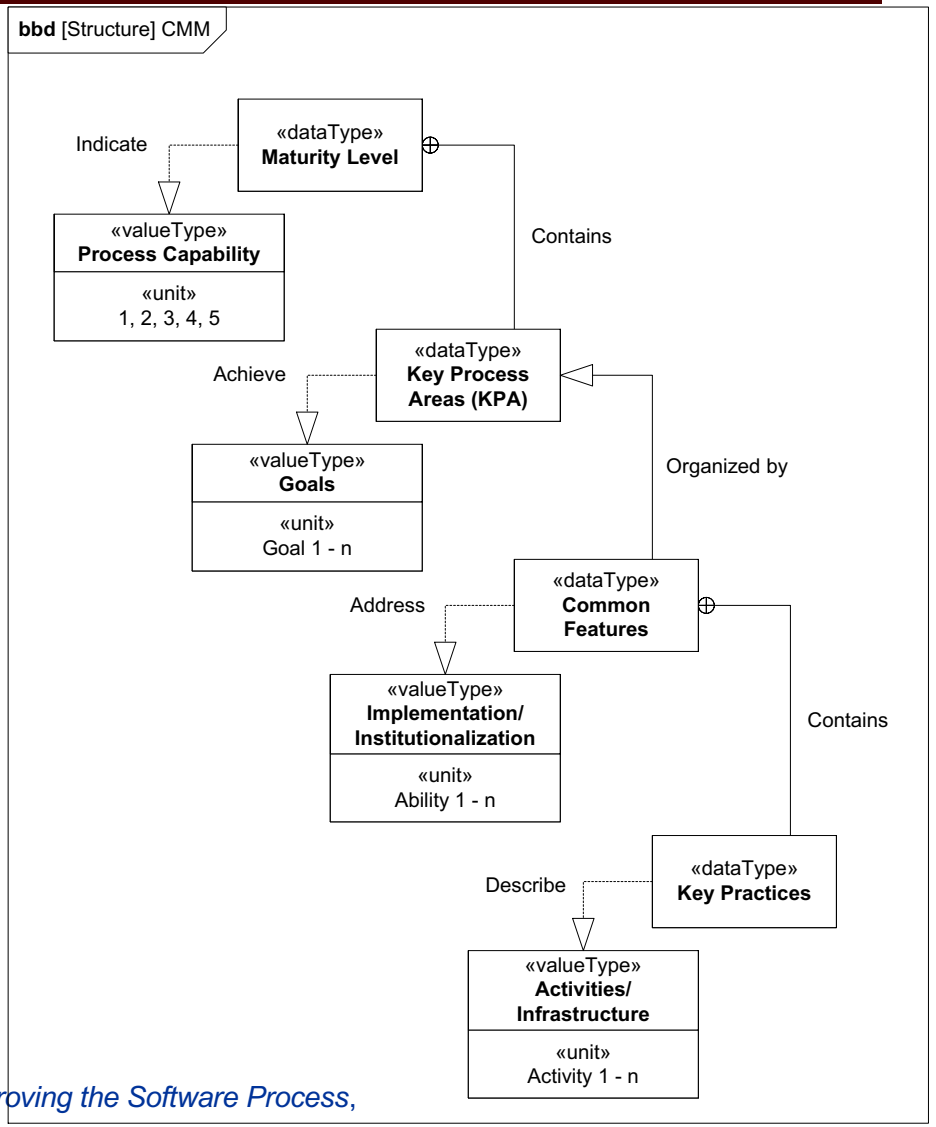
* Note: ISO/IEC 12207is identical to IEEE Std 12207

Reference: IEEE/IEC 12207:2008, *Information Technology Software Life Cycle Processes*

Capability Maturity Model (CMM) – History

In 1986, Software Engineering Institute (SEI) and MITRE began developing an assessment framework for measuring the maturity of an organization's [system/] software engineering process.

- **Process capability describes expected results.**
- **Process performance represents the actual results achieved.**
- **Process maturity is the degree which a process is explicitly defined, managed, measured, controlled, and effective.**



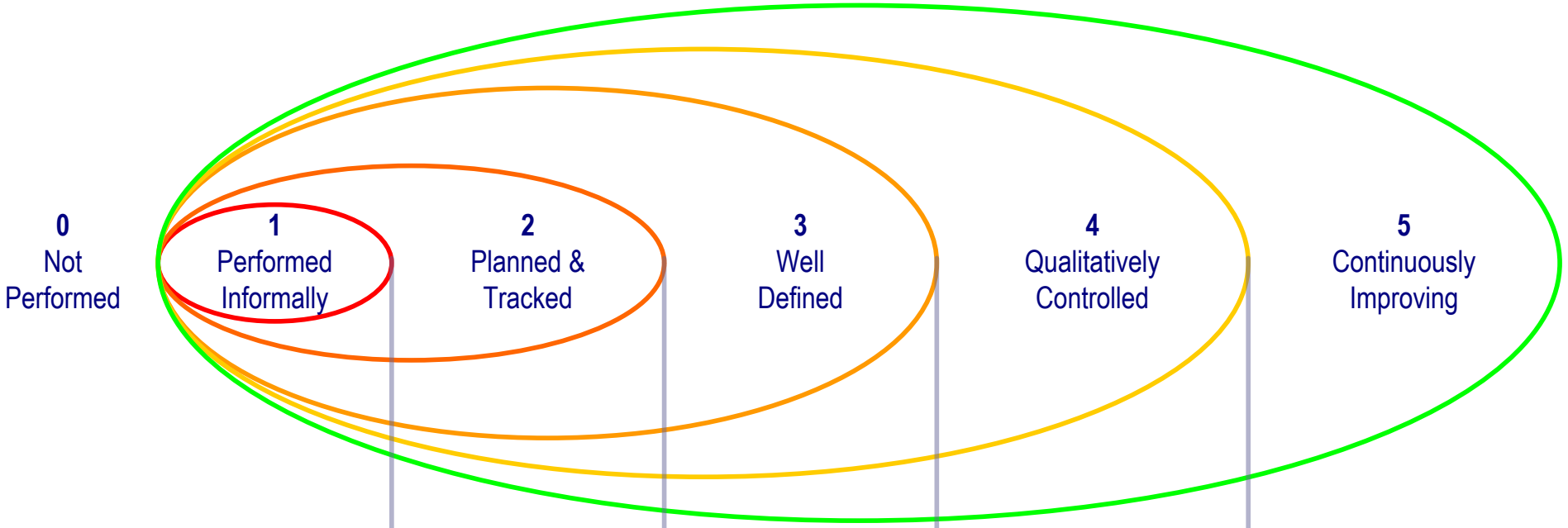
* **Reference:** M. Paulk, et al, *The Capability Maturity Model: Guidelines for Improving the Software Process*, Addison-Wesley, 1995. (ISBN: 0-201-54664-7)

Software Capability Maturity Model (SW-CMM)

- Level 1: Initial
  - The software development process is characterized as ad-hoc. Success depends on individual effort and heroics.
- Level 2: Repeatable
  - Basic project management (PM) processes are established to track performance, cost, and schedule.
- Level 3: Defined
  - Tailored software engineering and development processes are documented and used across the organization.
- Level 4: Managed
  - Detailed measures of product and process improvement are quantitatively controlled.
- Level 5: Optimizing
  - Continuous process improvement is institutionalized.

ISO/IEC 21827: SSE-CMM

- **System Security Engineering – Capability Maturity Model (SSE-CMM)**



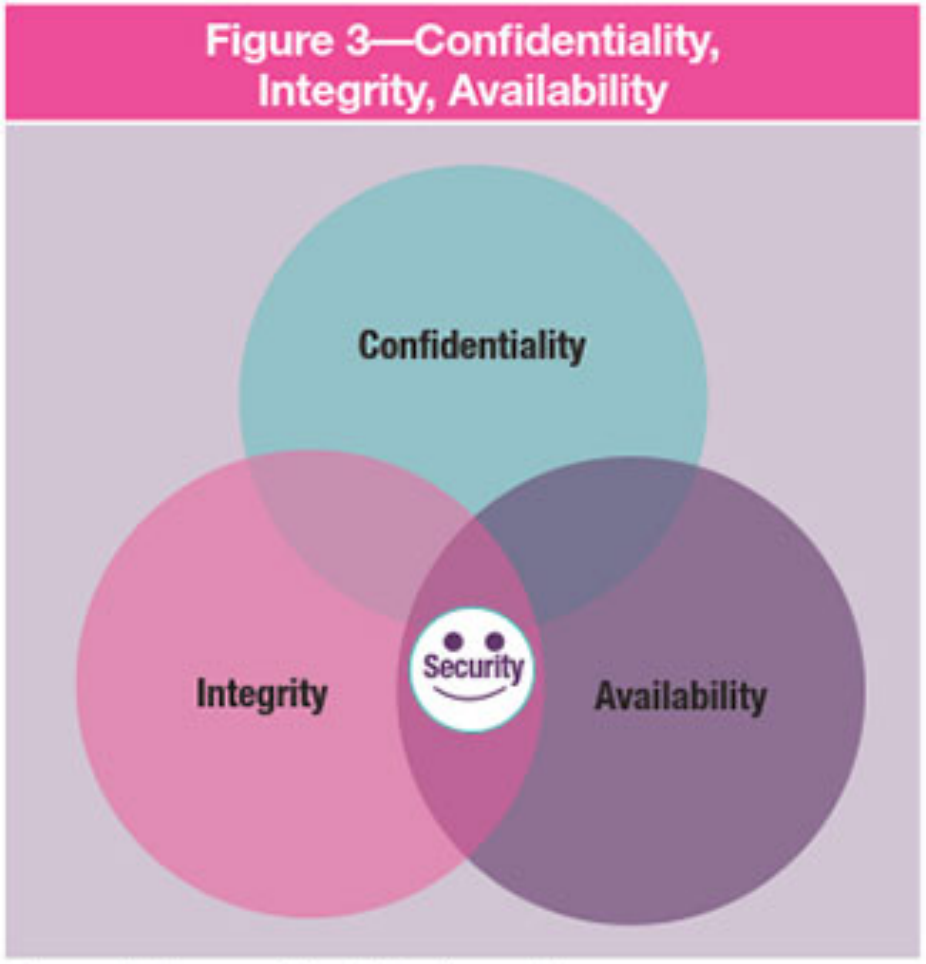
ISO/IEC 21827: SSE-CMM

- **SSE-CMM is composed of two domains:**
  - Security Base Practice (11 x Process Areas)
  - Project & Organizational Base Practice (11 x Process Areas)

- **Security Base Practices**
  - **Administer Security Controls**
  - **Assess Impact**
  - **Assess Security Risk**
  - **Assess Threat**
  - **Assess Vulnerability**
  - **Build Assurance Argument**
  - **Coordinate Security**
  - **Monitor Security Posture**
  - **Provide Security Input**
  - **Specify Security Needs**
  - **Verify & Validate Security**

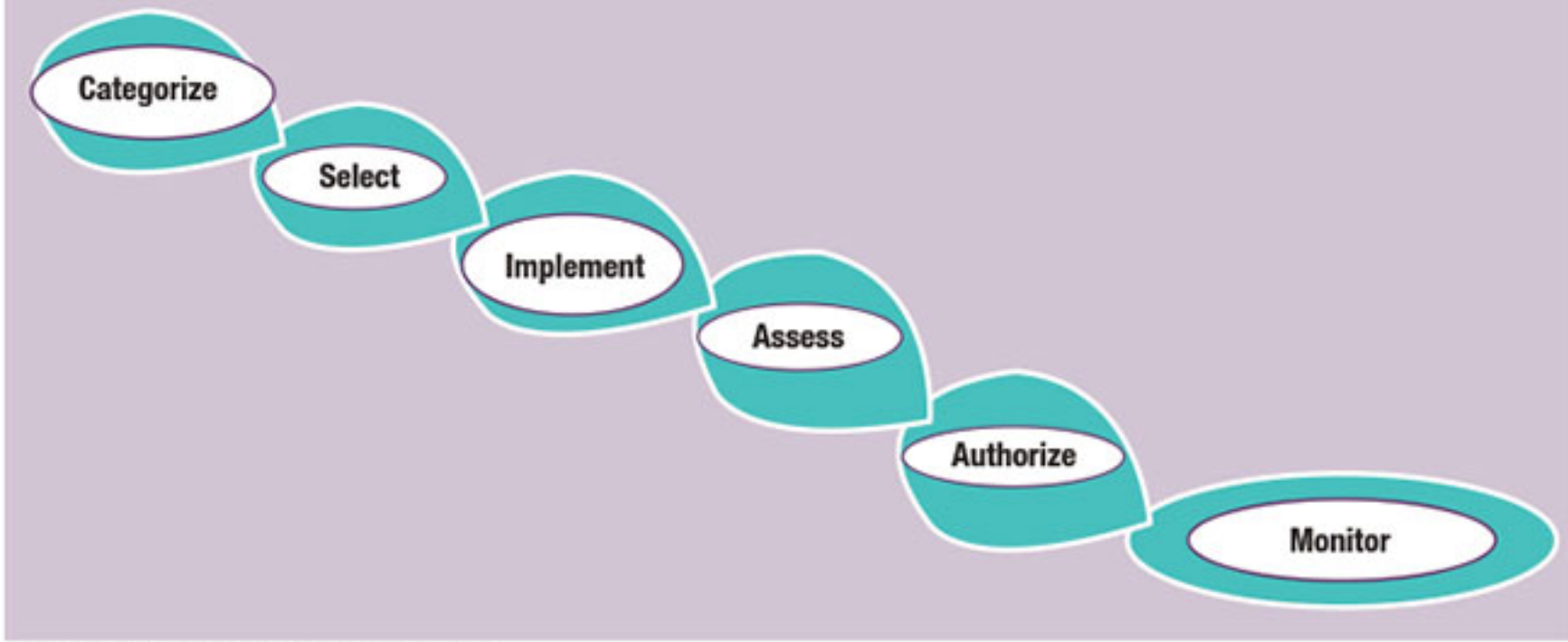
- **Project & Organizational Base Practices**
  - **Ensure Quality**
  - **Manage Configuration**
  - **Manage Project Risks**
  - **Monitor & Control Technical Effort**
  - **Plan Technical Effort**
  - **Define Organization's SE Process**
  - **Improve Organization's SE Process**
  - **Manage Product Line Evolution**
  - **Manage SE Support Environment**
  - **Provide Ongoing Skills & Knowledge**
  - **Coordinate with Suppliers**

CIA Triad (ISACA)



Risk Management Framework (ISACA)

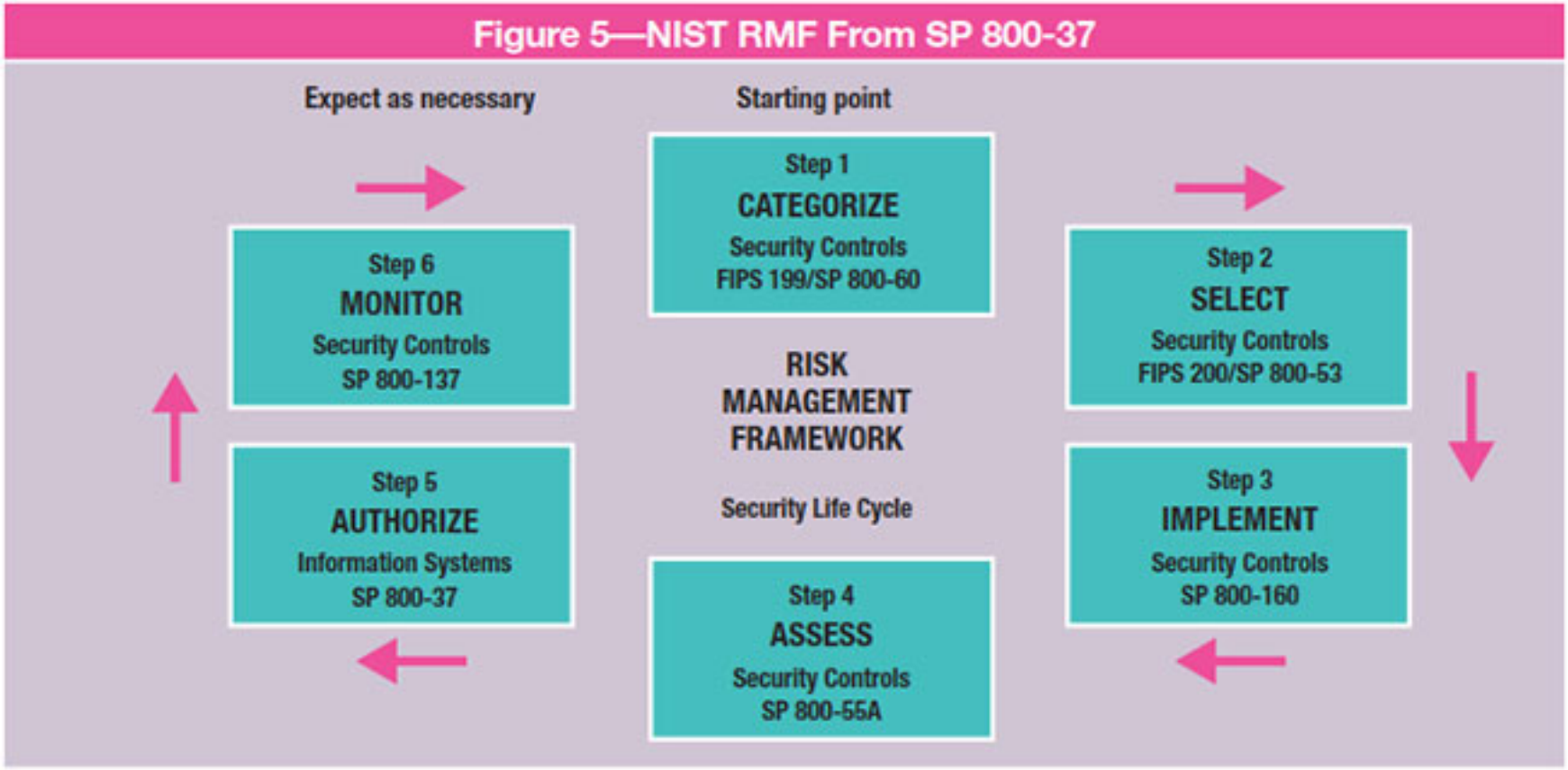
Figure 4—Six Steps in RMF



Source: J. Bennerson. Reprinted with permission

NIST Controls (ISACA)

Figure 5—NIST RMF From SP 800-37



Source: US National Institute of Standards and Technology. Reprinted with permission.

RMF Steps for ATO (ISACA)

Figure 6—RMF Steps for ATO

Security controls are the management, operational and technical safeguards or countermeasures employed within an information system to protect the confidentiality, integrity and availability of the system and its information.[22, 23]

RMF	**SP 800-37 Rev. 1**	"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"[24]
Step 1: CATEGORIZE Security impact value (low, moderate, high) for the security objectives of confidentiality, integrity or availability.		
	FIPS 199	"Standards for Security Categorization of Federal Information and Information Systems"[25]
	SP 800-60	"Guide for Mapping Types of Information and Information Systems to Security Categories"[26, 27]
Step 2: SELECT Choosing a set of baseline security controls and specifying minimum assurance requirements (safeguards or countermeasures employed), as appropriate.		
	FIPS 200	Minimum Security Requirements for Federal Information and Information Systems[28]
	SP 800-53 Rev 4	"Security and Privacy Controls for Federal Information Systems and Organizations"[29]
Step 3: IMPLEMENT Controls are: A. Implemented/Compensated/Planned B. System Specific/Inherited/Hybrid		
	SP 800-160	Draft document
Step 4: ASSESS By verification of evidence, test that the controls are in place and operating as intended.		
	SP 800-53A	"Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans"[30]
Step 5: AUTHORIZE		
	SP 800-37	"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"[31, 32]
Step 6: MONITOR POAMS		
	SP 800-137	"Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations"[33]

Source: J. Bennerson. Reprinted with permission.

Security Control Families and Management, Operational and Technical Controls (MOT) (ISACA)

Figure 7—Security Control Families and MOT

ID	Family	ID	Family
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

NIST SP 800-53 Rev. 4

18 Control Families–Comprised of three classes:

- Management controls—Normally addressed by management
- Operational controls—Primarily implemented and executed by people
- Technical controls—Focus on security controls that the computer system executes

Source: US National Institute of Standards and Technology. Reprinted with permission.

IS Governance (ISACA)

- Only 12 percent of organizations believe that information security meets the needs of the organization, and 67 percent are still making improvements.
- Sixty-nine percent noted that the information security budget should increase by as much as 50 percent to be able to protect the organization in line with the risk tolerance set by management.
  - Cited by ISACA from the 2015 Ernst and Young Global Informaton Security Survey

IS Governance Importance (ISACA) 1/2

- Addressing the increased potential for civil or legal liability.
- Providing assurance of policy compliance.
- Increasing predictability and reducing uncertainty of business operations by lowering risk to definable and acceptable levels.
- Providing the structure and framework to optimize allocations of limited security resources.
- Providing a level of assurance that critical decisions are not based on faulty information.
- Providing a firm foundation for efficient and effective risk management, process management, rapid incident response and continuity management

IS Governance Importance (ISACA) 2/2

- Providing greater confidence in interactions with trading partners
- Improving trust in customer relationships
- Protecting the organizations reputation
- Enabling new and better ways to process electronic transactions
- Providing accountability for safeguarding information during critical business activities, such as mergers and acquisitions
- Effective management of information security resources

IS Governance Outcomes 1 of 3

- **Strategic Alignment**
  - Security alignment
  - Risk Management
  - Value delivery
- **Risk Management**
  - Collective understanding of the organization's threat, vulnerability and risk profile
  - Understanding of the risk exposure and potential consequences of compromise
  - Awareness of risk management priorities based on potential consequences
  - Risk mitigation sufficient to achieve acceptable consequences from residual risk
  - Risk acceptance/deference based on an understanding of the potential consequences of residual risk.

IS Governance Outcomes (2 of 3)

- **Value delivery – Optimizing security investments**
  - A standard set of security practices
  - Information security overheads minimized while achieving mission objectives
  - A properly prioritized and distributed effort to areas with the greatest probability and highest impact and business benefit
  - Institutionalized and commoditized standards-based solutions with the greatest cost effectiveness
  - Complete solutions – organization, process, technology of the end-to-end business
  - Continuous improvement culture
- **Resource optimization**
  - Ensure that knowledge is captured and available
  - Develop security processes and practices
  - Develop security architectures to define and utilize infrastructure resources efficiently

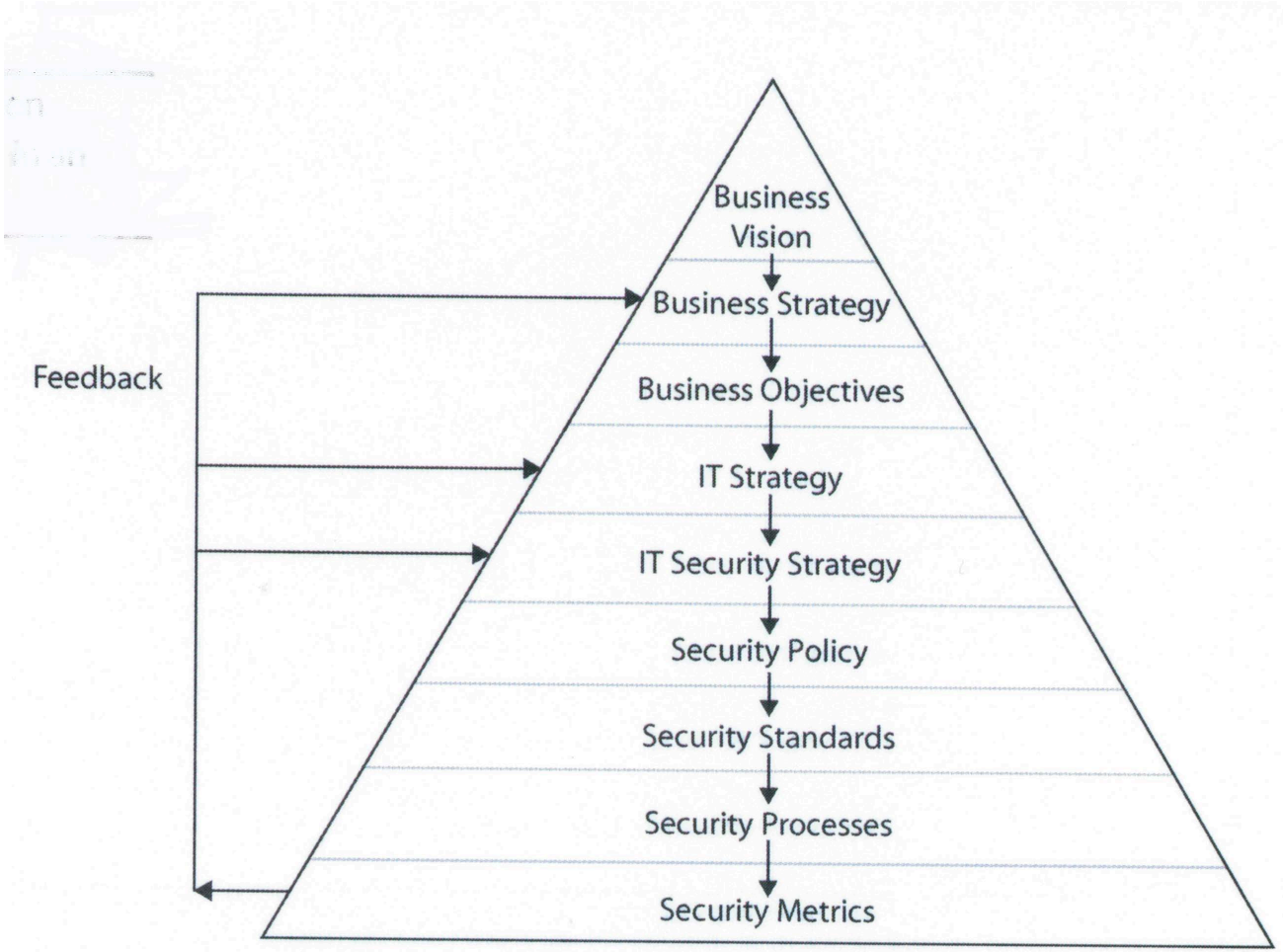
IS Governance Outcomes (3 of 3)

- **Performance measurement**
  - Metrics
  - Measurement process
  - Independent assurance by external audits/assessments
- **Assurance process integration**
  - Determine all organizational assurance functions
  - Developing formal relationships with other assurance functions
  - Coordinating all assurance functions for cost efficiency
  - Ensuring that roles and responsibilities between assurance functions overlap while avoiding gaps
  - Employing a systems approach to information security planning, deployment, metrics and management

Business Goals and Objectives

- **Six elements of a security governance framework**
  1. A comprehensive security strategy linked to business objectives
  2. Governing security policies that clearly express management intent and address each aspect of strategy, controls and regulation
  3. A complete set of standards for each policy to ensure that people, procedures, practices and technologies comply with policy requirements and set appropriate security baselines
  4. An effective security organizational structure with sufficient authority and adequate resources and no COI
  5. Defined workflows and structures that assist in defining responsibilities for information security governance
  6. Institutionalized metrics and monitoring processes to ensure compliance, provide feedback on control effectiveness and provide the basis for appropriate management decisions

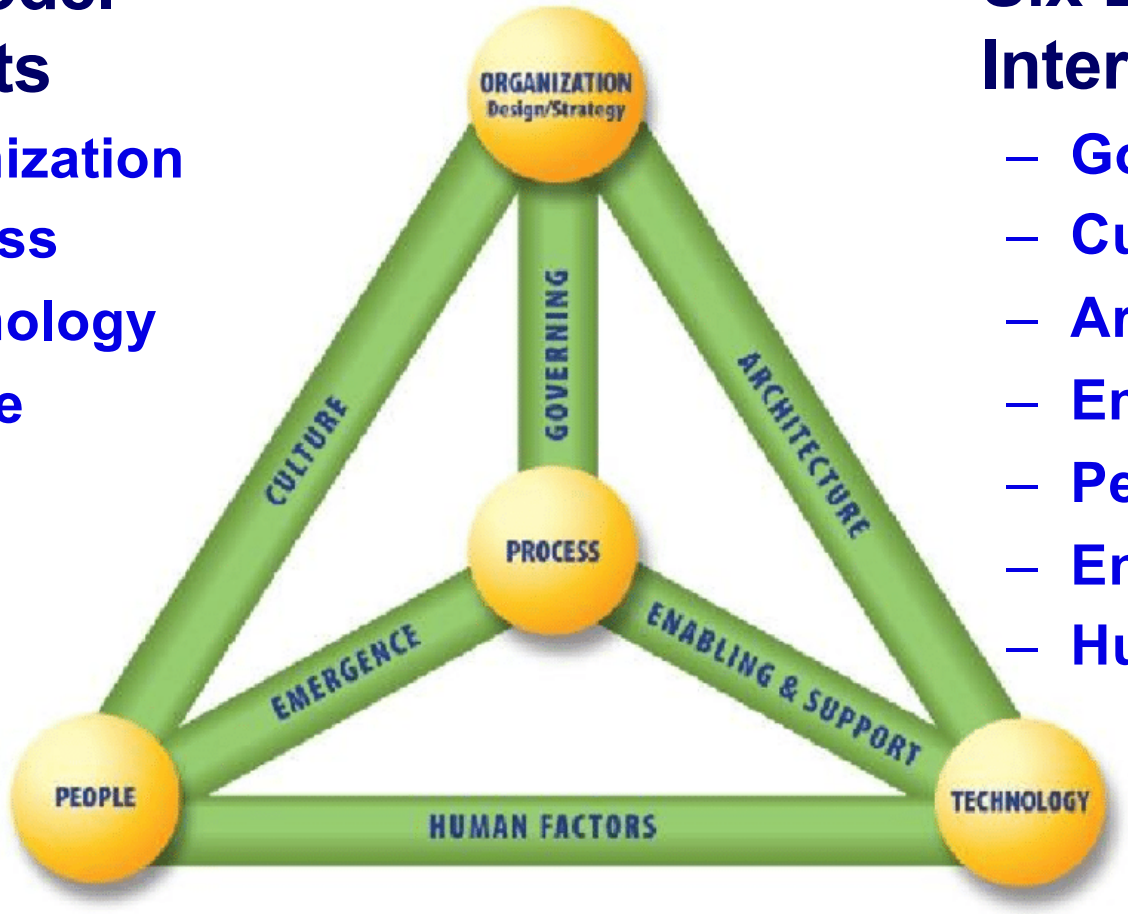
Vision Flows Downward



Source: Gregory, CISM All-in-One

Business Model for Information Security

- **Four Model Elements**
  - Organization
  - Process
  - Technology
  - People

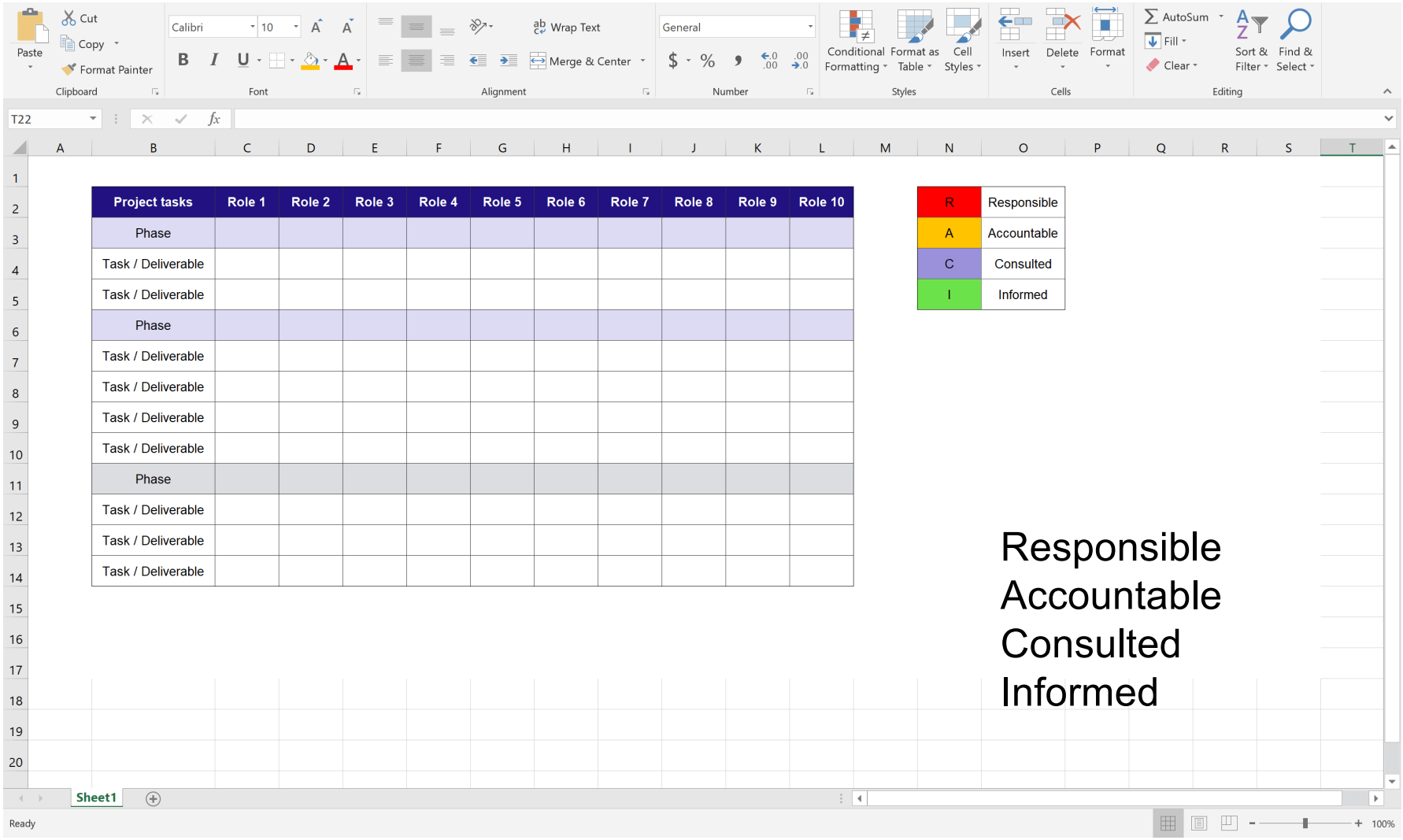


- **Six Dynamic Interconnections**
  - Governance
  - Culture
  - Architecture
  - Emergence
  - People
  - Enabling & Support
  - Human Factors

Organizational Roles and Responsibilities

Domain 1
Information Security Governance

RACI Template



Project tasks	Role 1	Role 2	Role 3	Role 4	Role 5	Role 6	Role 7	Role 8	Role 9	Role 10
Phase										
Task / Deliverable										
Task / Deliverable										
Phase										
Task / Deliverable										
Task / Deliverable										
Task / Deliverable										
Task / Deliverable										
Phase										
Task / Deliverable										
Task / Deliverable										
Task / Deliverable										

R	Responsible
A	Accountable
C	Consulted
I	Informed

Responsible
Accountable
Consulted
Informed

Source: https://thedigitalprojectmanager.com/raci-chart-made-simple/

RACI Charts

- **Responsible**
- **Accountable**
- **Consulted**
- **Informed**

Source: https://thedigitalprojectmanager.com/raci-chart-made-simple/

	Frodo	Sam	Gandalf	Aragorn	Head of Elves (Elrond)
Decide on what to do with ring	C	I	A	C	R
Create Fellowship	R	C	A	C	R
Get the ring to Mt Doom	R	C	A	C	I
Distract and defeat enemies	I	R	C	R	I

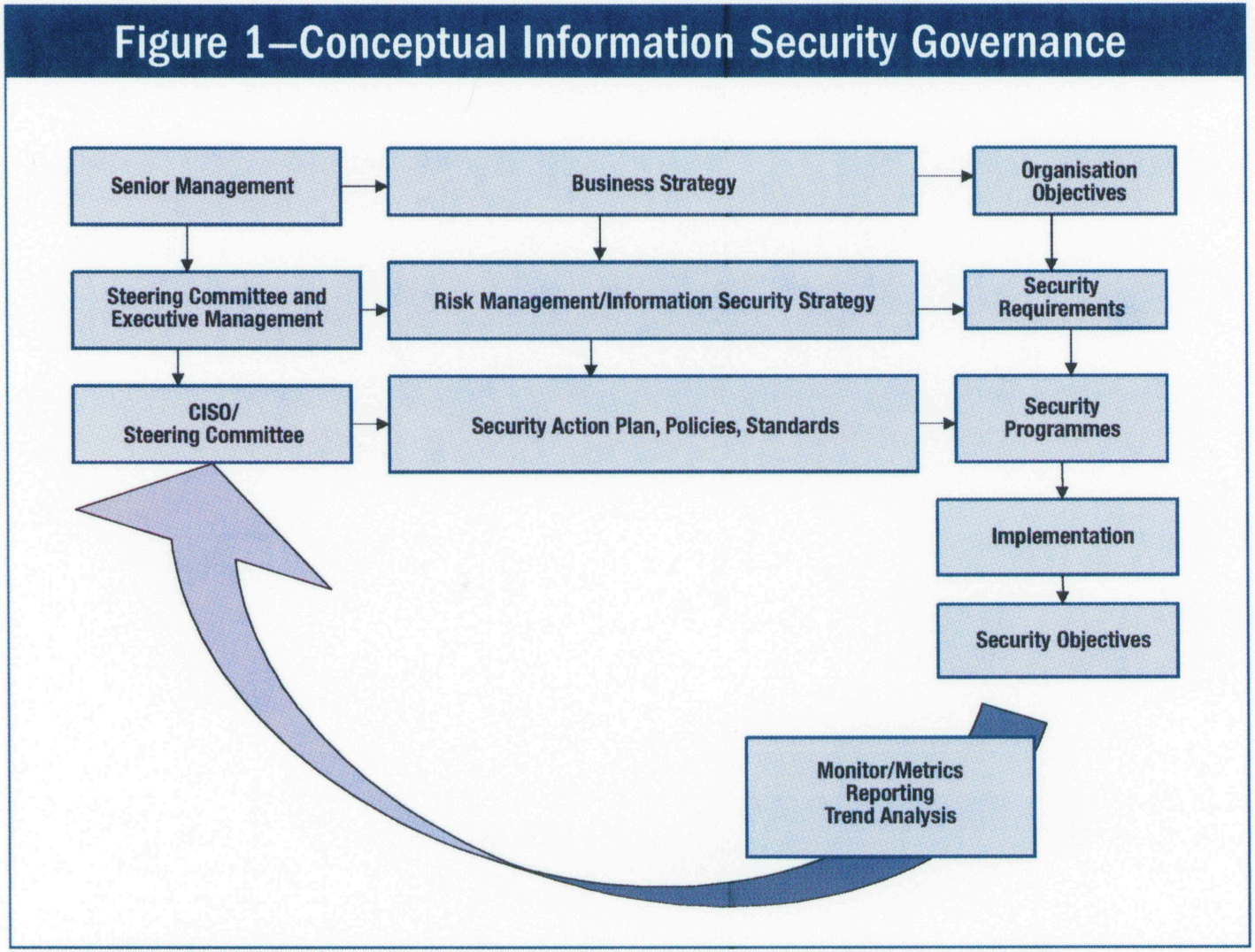
Roles and Responsibilities

- Board of Directors
  - SOX and Audit Committee
- Senior Management
  - Implements BOD security direction
- Business Process Owners
  - IS strategy integrated with Business Process Outsourcing (BPO_
- Steering Committee
  - Security strategy and integration efforts
  - Specific actions and progress relative to business unit support of ISP (and reverse)
  - Emerging risk, business unit security practices and compliance
- Chief Information Security Officer
  - CIO, CSO, CFO or CFO

Information Security Governance

- Source: IT Governance Institute (ITGI)
- ITGI is a subsidiary organization of ISACA
- Source Document for rest of this section:
- https://www.isaca.org/Knowledge-Center/Research/Documents/Information-Security-Govenance-for-Board-of-Directors-and-Executive-Management_res_Eng_0510.pdf

Conceptual Information Security Governance (IT Governance Institute)



Boards of Directors/Trustees (ITGI)

- **Senior management MUST protect the interests of the organization's stakeholders.**
  - **Understanding risks to the business to ensure that they are adequately addressed from a governance perspective.**
  - **Requires managing risks, including information security risks, by integrating information security governance in the overall enterprise governance framework of the organization.**
- **IS governance requires strategic direction and impetus.**
- **Members of the board need to be aware of the organization's information assets and their criticality to ongoing business operations.**
  - **This can be accomplished by periodically providing the board with the high-level results of comprehensive risk assessments and business impact analyses.**
  - **Can also be accomplished by business dependency assessments of information resources.**

Steering Committee (ITGI)

- **IS affects all aspects of an organization.**
  - **To ensure that all stakeholders affected by security considerations are involved, a steering committee of executives should be formed.**
  - **Members of such a committee may include, amongst others, the chief executive officer (CEO) or designee, business unit executives, chief financial officer (CFO), chief information officer (CIO)/IT director, chief security officer (CSO), CISO, human resources, legal, risk management, audit, operations and public relations.**
  - **A steering committee serves as an effective communication channel for management's aims and directions and provides an ongoing basis for ensuring alignment of the security program with organizational objectives.**

Chief Information Security Officer (ITGI)

- All organizations have a CISO whether or not anyone holds that title.
  - It may be de facto the CIO, CSO, CFO or, in some cases, the CEO, even when there is an information security office or director in place.
  - The scope and breadth of information security concerns are such that the authority required and the responsibility taken inevitably end up with an executive manager.
  - Legal responsibility, by default, extends up the command structure and ultimately resides with senior management and the board of directors.
- Failure to recognize this and implement appropriate governance structures can result in senior management being unaware of this responsibility and the attendant liability.

What Should the Senior Executives Be Doing? (ITGI)

- **Understand why IS needs to be governed**
  - Risks and threats are real and could have significant impact on the enterprise.
  - Reputational damage can be considerable.
  - Effective information security requires coordinated and integrated action from the top down.
  - IT investments can be substantial and easily misdirected.
  - Cultural and organizational factors are equally important.
  - Rules and priorities need to be established and enforced.
  - Trust needs to be demonstrated toward trading partners while exchanging electronic transactions.
  - Trust in reliability of system security needs to be demonstrated to all stakeholders.
  - Security incidents are likely to be exposed to the public.

What Should the Senior Executives Be Doing? (ITGI)

- **Take Board-level Action**
  - Become informed about information security.
  - Set direction, i.e., drive policy and strategy and define a global risk profile.
  - Provide resources to information security efforts.
  - Assign responsibilities to management.
  - Set priorities.
  - Support change.
  - Define cultural values related to risk awareness.
  - Obtain assurance from internal or external auditors.
  - Insist that management makes security investments and security
  - improvements measurable, and monitors and reports on program effectiveness.

Taking Senior Management Action (ITGI)

- Provide oversight for the development of a security and control framework that consists of standards, measures, practices and procedures, after a policy has been approved by the governing body of the organization and related roles and responsibilities assigned. (Design)
- Set direction for the creation of a security policy, with business input. (Policy Development)
- Ensure that individual roles, responsibilities and authority are clearly communicated and understood by all. (Roles and Responsibilities)
- Require that threats and vulnerabilities be identified, analyzed and monitored, and industry practices used for due care.
- Require the set-up of a security infrastructure.

More Senior Management Actions (ITGI)

- Set direction to ensure that resources are available to prioritize possible controls & countermeasure. (Implementation)
- Establish monitoring measures to detect and ensure correction of security breaches, so all actual and suspected breaches are promptly identified, investigated and acted upon, and to ensure ongoing compliance with policy, standards and minimum acceptable security practices. (Monitoring)
- Require that periodic reviews and tests be conducted.
- Institute processes that will help implement intrusion detection and incident response.
- Require monitoring and metrics to ensure that information is protected, correct skills are on hand to operate information systems securely and security incidents are responded to on a timely basis. Education in security measures and practices is of critical importance for the success of an organization's security program. (Awareness, Training and Education)
- Ensure that security is integral to the systems development life cycle

Outcomes with Management Directives

Figure 2—Relationships of Outcomes With Management Directives

Management Level	Strategic Alignment	Risk Management	Value Delivery	Performance Measurement	Resource Management	Integration
Board of directors/ trustees	Set direction for a demonstrable alignment.	Set direction for a risk management policy that applies to all activities and regulatory compliance.	Set direction for reporting of security activity costs and value of information protected.	Set direction for reporting of security effectiveness.	Set direction for a policy of knowledge management and resource utilisation.	Set direction for a policy of assuring process integration.
Senior executives	Institute processes to integrate security with business objectives.	Ensure that roles and responsibilities include risk management in all activities. Monitor regulatory compliance.	Require business case studies of security initiatives and value of information protected.	Require monitoring and metrics for reporting security activities.	Ensure processes for knowledge capture and efficiency metrics.	Provide oversight of all management process functions and plans for integration.
Steering committee	Review and assist security strategy and integration efforts, ensure that business unit managers and process owners support integration.	Identify emerging risks, promote business unit security practices, and identify compliance issues.	Review and advise adequacy of security initiatives to serve business functions and value delivered in terms of enabled services.	Review and advise the extent to which security initiatives meet business objectives.	Review processes for knowledge capture and dissemination.	Identify critical business processes and management assurance providers. Direct assurance integration efforts.
Chief information security officer	Develop security strategy, oversee the security programme and initiatives, and liaise with business unit managers and process owners for ongoing alignment.	Ensure risk and business impact assessments, develop risk mitigation strategies, and enforce policy and regulatory compliance.	Monitor utilisation and effectiveness of security resources and reputation and the delivery of trust.	Develop and implement monitoring and metrics collection and analysis and reporting approaches. Direct and monitor security activities.	Develop methods for knowledge capture and dissemination. Develop metrics for effectiveness and efficiency.	Liaise with other management process functions. Ensure that gaps and overlaps are identified and addressed.

Source: ITSG

ITGI Summary 1

Board of Directors/Executive Management

Information security governance consists of the leadership, organisational structures and processes that safeguard critical information assets.

Responsibilities		Outcomes
Boards should provide strategic oversight regarding information security, including: • Understanding the criticality of information and information security to the organisation • Reviewing investment in information security for alignment with the organisation strategy and risk profile • Endorsing the development and implementation of a comprehensive information security programme • Requiring regular reports from management on the programme's adequacy and effectiveness	**Governing boards and executive management should review:** • The scale and return of the current and future investments in information resources to ensure they are optimised • The potential for technologies to dramatically change organisations and business practices, thereby creating new opportunities and value while reducing costs	**The five basic outcomes of information security governance should include:** • Strategic alignment of information security with business strategy to support organisational objectives • Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level • Resource management by utilising information security knowledge and infrastructure efficiently and effectively • Performance measurement by measuring, monitoring and reporting information security governance metrics to ensure organisational objectives are achieved • Value delivery by optimising information security investments in support of organisational objectives

ITGI Summary 2

Benefits of good information security governance:

- Improved trust in customer relationships
- Protecting the organisation's reputation
- Decreasing likelihood of violations of privacy and potential liabilities
- Providing greater confidence when interacting with trading partners
- Enabling new and better ways to process electronic transactions
- Reducing operational costs by providing predictable outcomes—mitigating risk factors that may interrupt the process

A comprehensive security program will include:

- Development/maintenance of security policies
- Assignment of roles, responsibilities, authority and accountability
- Development/maintenance of a security and control framework that consists of standards, measures, practices and procedures
- Periodic assessments of risks and business impact analyses
- Classification and assignment of ownership of information assets
- Adequate, effective and tested controls for people, processes and technology
- Processes to monitor security elements
- Information security incident management
- Effective identity and access management process for users and suppliers of information
- Meaningful monitoring and metrics of security performance
- Education of all users, managers and board members regarding information security requirements
- Annual information security evaluations and performance reports to the board of directors
- Plan for remedial action to address information security deficiencies
- Training in the operation of security processes
- Development and testing of plans for continuing the business in case of interruption or disaster

This material is based on *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition.*

Information Security Governance Metrics

Domain 1
Information Security Governance

Characteristics of Effective Security Metrics (ISACA)

- **Specific**
  - Based on a clearly understood goal, clear and concise
- **Measurable**
  - Able to be quantified
- **Attainable**
  - Realistic, based on important goals and values
- **Relevant**
  - Directly related to a specific activity or goal
- **Timely**
  - Grounded in a specific time frame
- **KEY ACRONYM SMART**

Additional Characteristics of Effective Security Metrics (cited by ISACA)

- **Accurate**
  - At least reasonably accurate
- **Cost-effective**
  - Both collection and maintenance
- **Repeatable**
  - And reliably acquired
- **Predictive**
  - Measurements should predict outcomes
- **Actionable**
  - It should be clear what action should be taken

Major Control Networks (IV4)

- **No single framework is all encompassing and "complete" in every sense of the word.**
  - **There is no single framework that covers all aspects of providing the information services and management team with the tools and direction they need to move from regulatory requirements to implementing policy, procedure, and process controls that meet those requirements.**
- **Popular Frameworks Include:**

AICPA/CICA
Carnegie Mellon University (CMU/SEI) OCTAVE
CICA CoCo – Criteria of Control Framework
CICA IT Control Guidelines
CMMI – Capability Maturity Model Integration
CobiT
COSO
GAISP – Generally Accepted Information z Security Principles
ISF Standard of Good Practice for Information Security
ISO 9000
ITIL
Malcolm Baldridge National Quality Program
OECD Principles of Corporate Governance
OPMMM
Six Sigma
Recommended Security Controls for Federal Information Systems, NIST SP 800-53 rev.4
CIS 20 Critical Controls
ISO 17799:2005 and the ISO 27000 series

Organizational Security Model

Security planning can be broken down into three areas:

- **strategic - long term goals**
- **tactical - medium term goals**
- **operational - short term goals**

A security program is more than just having a security policy and annual network assessment.

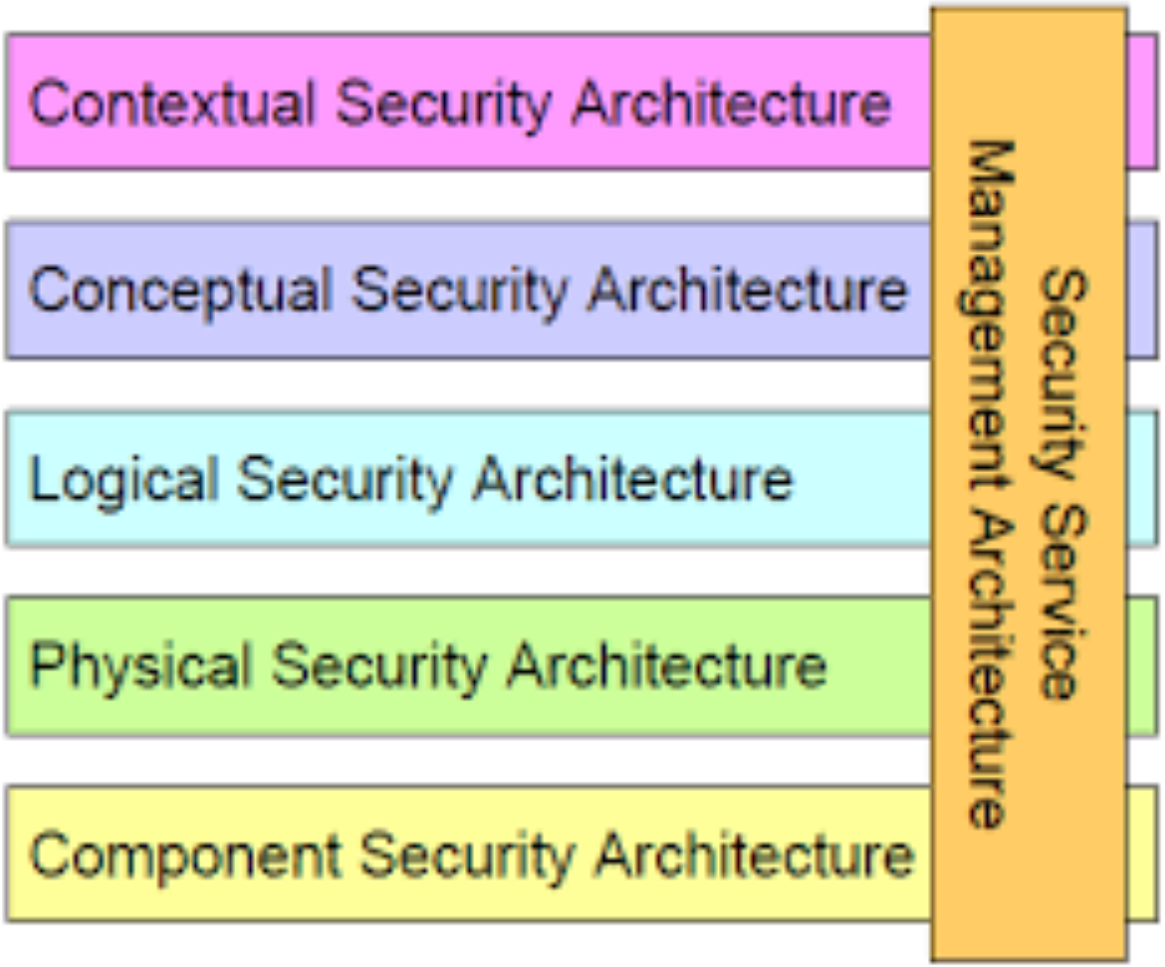
There are existing security frameworks that can be utilized:

- **ISACA's COBIT defines goals for controls for managing IT and insuring it maps to business needs. Four domains:**
  - **Plan and Organize**
  - **Acquire and Implement**
  - **Deliver and Support**
  - **Monitor and Evaluate**

Organizational Security Model

- **Security Frameworks (cont'd):**
  - **ISO 17799 - made up of 10 domains, that are similar to those in the CISSP Common Body of Knowledge**
  - **IT Infrastructure Library (ITIL)**
- **COBIT really provides "what is to be achieved," and ISO 17799 and ITIL tell you "how to achieve it.**
- **Definition:**
- ***Security Governance* - basically the same as corporate/IT governance, but as it applies to security**

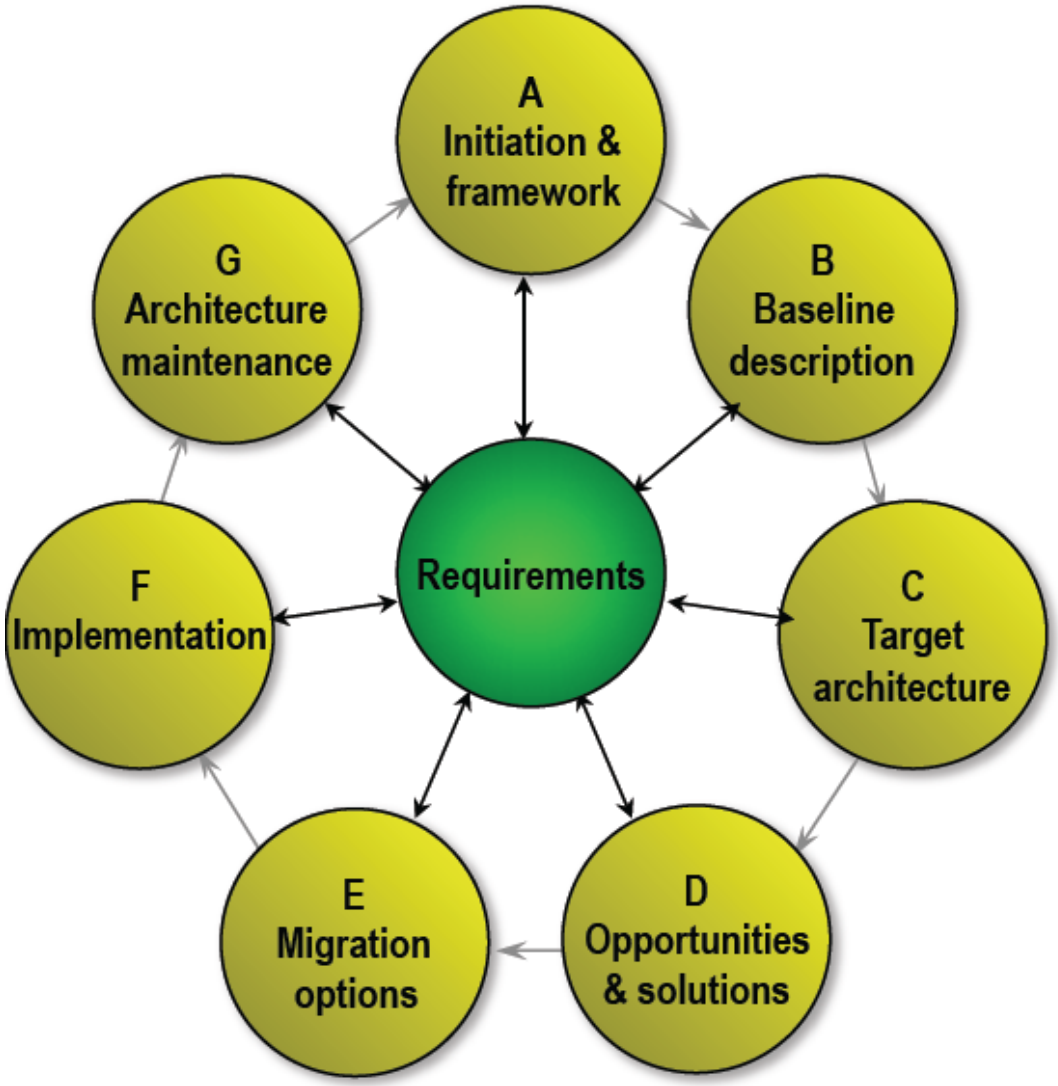
SABSA Model for Security Architecture



Sherwood Applied Business Security Architecture

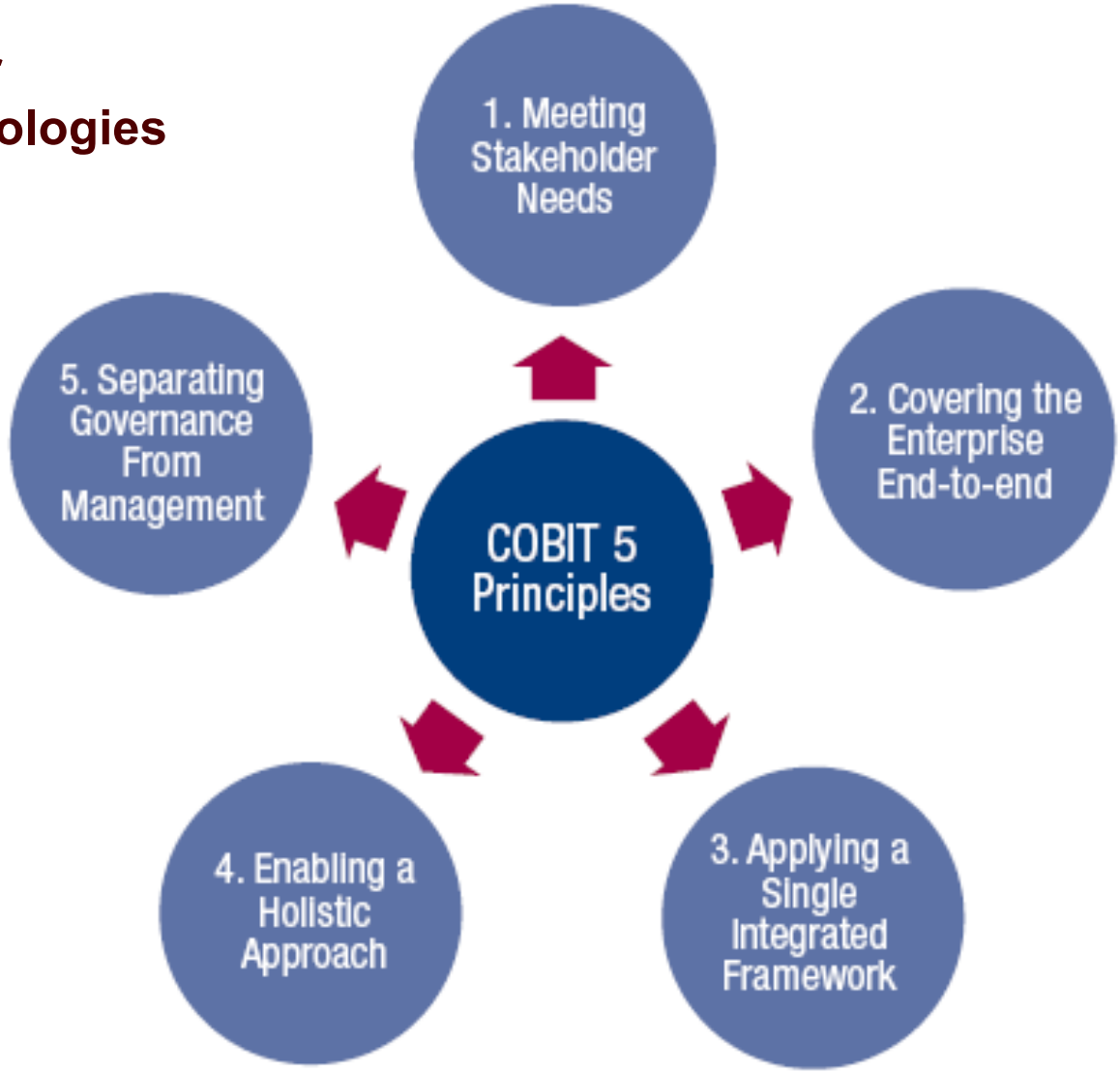
	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The business	Business risk model	Business process model	Business organization and relationships	Business geography	Business time dependencies
Conceptual	Business attributes profile	Control objectives	Security strategies and architectural layering	Security entity model and trust framework	Security domain model	Security-related lifetime and deadlines
Logical	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Physical	Business data model	Security rules, practices and procedures	Security mechanisms	Users, applications and user interface	Platform and network infrastructure	Control structure execution
Component	Detailed data structures	Security standards	Security products and tools	Identities, functions, actions and ACLs	Processes, nodes, addresses and protocols	Security step timing and sequencing
Operational	Assurance of operational continuity	Operational risk management	Security service management and support	Application and user management and support	Security of sites and platforms	Security operations schedule

The Open Group Architecture Framework (TOGAF)



COBIT 5

COBIT = Control Objectives for Information and Related Technologies

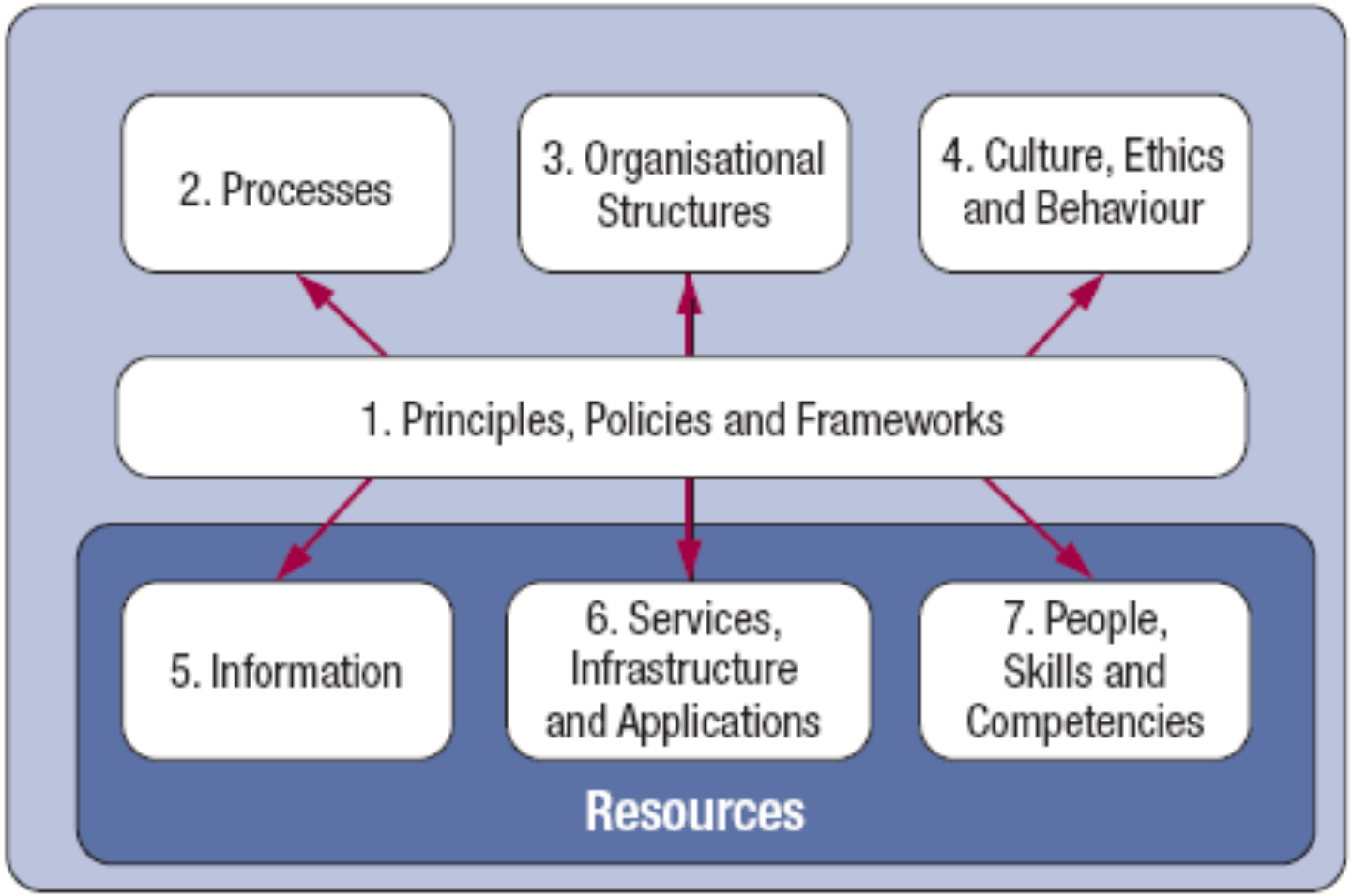


ISACA is an international professional association focused on IT Governance. Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves.

COBIT 5

- **Divided into Governance and Management domains**
  - **Governance: Contains five governance processes; within each process, evaluate, direct and monitor (EDM)**
  - **Management: Contains four domains, in line with the responsibility areas of plan, build, run and monitor (PBRM)**
    - **Align, Plan and Organize (APO)**
    - **Build, Acquire and Implement (BAI)**
    - **Deliver, Service and Support (DSS)**
    - **Monitor, Evaluate and Assess (MEA)**

COBIT 5 Enablers



Payment Card Industry Data Security Standards

- The PCI DSS represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information.
- The standard provides an actionable framework for developing a robust account data security process - including preventing, detecting and reacting to security incidents.
- Applies to any entity that stores, processes and/or transmits CHD.

PCI DSS Six Goals

- Build and Maintain a Secure Network
- Protect Card Holder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

PCI DSS 12 Requirements

- 1) Install and Maintain a firewall configuration to protect Card Holder Data (CHD)
  - Firewall and Router configuration standards
  - Review Network Diagram
  - Firewall and Router connections are restricted (inbound/outbound traffic)
  - No direct internet connection to CHD (DMZ)
- 2) Do not use vendor supplied defaults
  - Attempt to sign on with defaults
  - Hardening standards and system configuration
  - Non-console admin access is encrypted

PCI DSS 12 Requirements

- 3) Protect stored CHD
  - Retention Policy and Procedures
  - Quarterly process for deleting stored CHD
  - Sample incoming transactions, logs, history files, trace files, database schemas and content
  - Do not store full track, CVV or PIN
  - Render PAN unreadable (mask/truncate)
  - Encryption and key management
- 4) Encrypt transmission of CHD
  - Verify encryption and encryption strength
  - Verify wireless is industry best practice (no WEP)

PCI DSS 12 Requirements

- 5) Use and regularly update Antivirus software
  - All system have AV
  - AV is current, actively running and logging
- 6) Develop and maintain secure systems and applications
  - Patch management – current within one month
  - ID new security vulnerabilities with risk rating
  - Custom code is reviewed prior to release
  - Change management process
  - Developers are trained in secure coding techniques

PCI DSS 12 Requirements

- 7) Restrict access to CHD by need-to-know
  - Review access policies
  - Confirm access rights for privileged users
  - Confirm access controls are in place
  - Confirm access controls default with “deny-all”
- 8) Assign a unique ID to each user
  - Verify all users have a unique ID
  - Verify authentication with ID/PW combination
  - Verify two-factor authentication for remote access
  - Verify terminated users are deleted
  - Inspect configurations for PW controls

PCI DSS 12 Requirements

- 9) Restrict physical access to CHD
  - Access to computer rooms and data centers
  - Video cameras are in place and video is secure
  - Network jacks are secure – not in visitor area
  - Process for assigning badges
  - Storage locations are secure (offsite media)
- 10) Track and monitor all access to network resources
  - Review audit trails – actions, time, date, user, etc.
  - Time server updates and distribution
  - Process to review security logs

PCI DSS 12 Requirements

- 11) Regularly test security systems
  - Test for wireless access points
  - Internal and external network vulnerability scans
  - Internal and external penetration testing annually
  - File integrity monitoring tools are used
- 12) Maintain security policies
  - Policies are reviewed at least annually
  - Explicit approval is required for access
  - Auto disconnect for inactivity-internal and remote
  - Security awareness program is in place
  - Incident Response Plan

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1 Establish firewall and router configuration standards that include the following:	**1.1** Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1** Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.			
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.			
	1.1.2.b Verify that the diagram is kept current.			
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.3.a** Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.			
	1.1.3.b Verify that the current network diagram is consistent with the firewall configuration standards.			

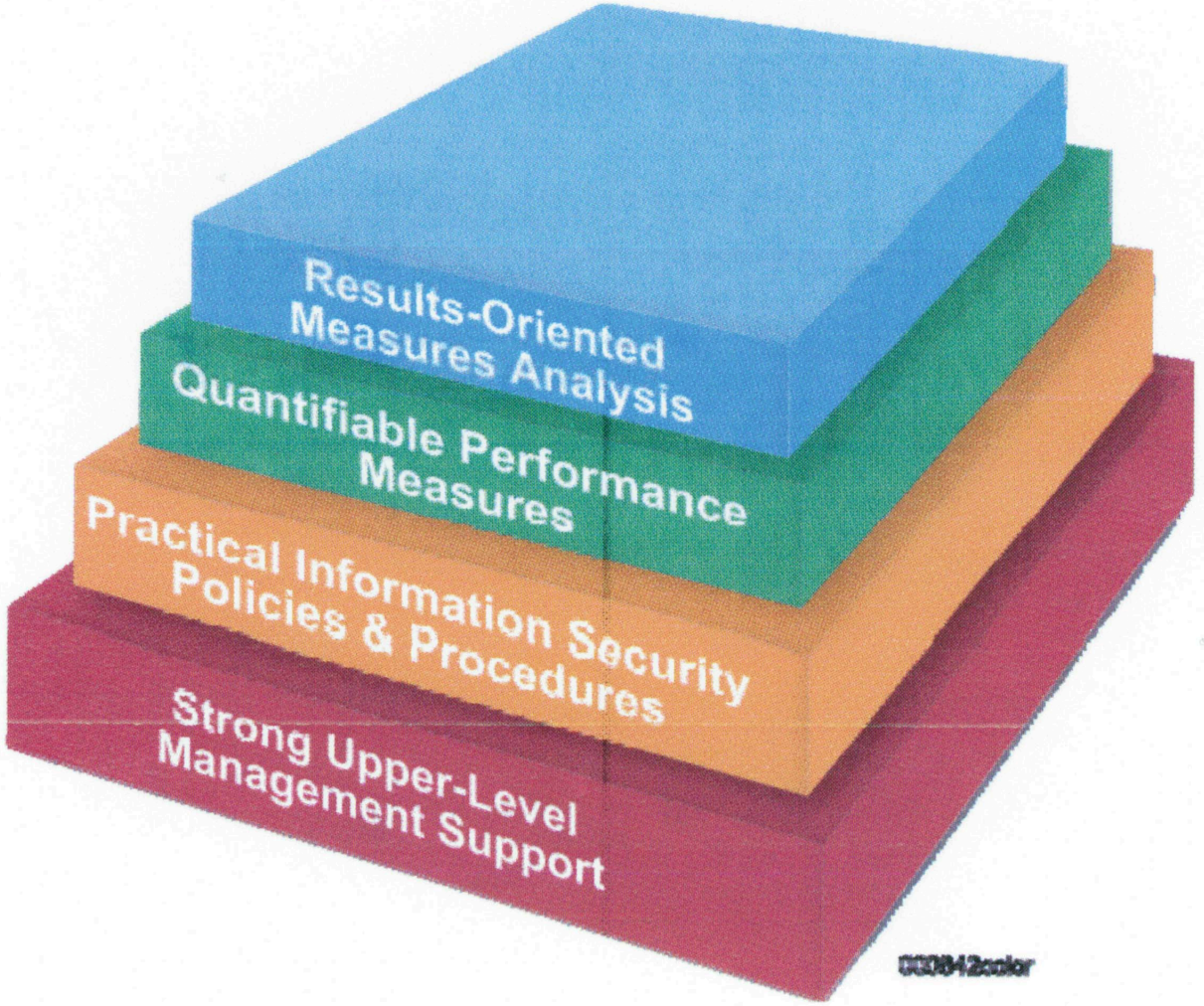
ISO/IEC 27002 (ITGI)

- **Information Technology Security Techniques**
- **The 11 major headings of ISO/IEC 27002 are:**
  1. **Information security policy**
  2. **Organizing information security**
  3. **Asset management**
  4. **Human resources (HR) security**
  5. **Physical and environmental security**
  6. **Communications and operations management**
  7. **Access control**
  8. **Information systems acquisition, development and maintenance**
  9. **Information security incident management**
  10. **Business continuity management**
  11. **Compliance**

Other Resources for Metrics (ISACA)

- ISO/IEC 27004:2009 Information Technology – Security Techniques – Information Security Management – Measurement
- COBIT 5
- The Center for Information Security (CIS)
- NIST Special Publication 800-55 Revision 1: Performance Guide for Information Security

NIST: Components of Security Metrics



Governance Implementation Metrics (ISACA)

- KGI – Key Goal Indicator
- KPI – Key Performance Indicator
- Typically used for downstream projects and initiatives
- KRI – Key Risk Indicator

Strategic Alignment Metrics (ISACA)

- The extent to which the security program demonstrably enables specific business activities
- Business activities that have not been undertaken or have been delayed because of inadequate capability to manage risk
- A security organization that is responsive to defined business requirements

Risk Management Metrics (ISACA)

- A defined organizational risk appetite and tolerance in terms relevant to the organization
- The completeness of an overall security strategy and program for achieving acceptable levels of risk
- Processes for management or reduction of adverse impacts
- Coverage of all business-critical systems by a systemic continuous risk management processes
- Periodic risk assessments indicating progress toward defined goals
- Trends in impacts
- Results from tested incident response and business continuity/disaster recovery plans
- The completeness of the asset inventory, valuation and assignment of ownership
- The percentage of BIAs of all critical or sensitive systems
- The extent of a complete an functioning asset classification process
- The ratio of security incidents from known risk compare to unidentified risk

Value Delivery Metrics (ISACA)

- **KGIs and KPIs include**
  - Security activities that are designed to achieve specific strategic objectives in a cost –effective manner
  - The cost of security being proportional to the value of the assets
  - Security resources that are allocated by degree of assessed risk and potential impact
  - Protection costs that are aggregated as a function of revenues or asset valuation
  - Controls that are well designed based on defined control objectives and are fully utilized
    - An adequate and appropriate number of controls to achieve acceptable risk impact levels
    - Control cost-effectiveness that is determined by periodic testing
    - Policies in place that require all controls to be periodically reevaluated for cost, compliance and effectiveness
    - The number of controls to achieve acceptable risk and impact levels
    - Effectiveness of controls as determined by testing

Resource Management Metrics (ISACA)

- **Indicators of effective resource management**
  - Infrequent problem solution rediscovery
  - Effective knowledge capture and dissemination
  - Extent to which security-related processes are standardized
  - Clearly defined roles and responsibilities for IS functions
  - Information security incorporated into every project plan
  - Percentage of information assets and related threats
  - Proper organizational location, level of authority and number of personnel for the information security function
  - Resource utilization levels
  - Staff productivity
  - Per-seat cost of security services

Assurance Process Integration (ISACA)

- **KGIs include**
  - No gaps in information asset protection
  - Elimination of unnecessary security overlaps
  - Seamless integration of assurance activities
  - Well-defined roles and responsibilities
  - Assurance providers understanding the relationship to other assurance functions
  - All assurance functions being identified and considered in the strategy
  - Effective communication and cooperation between assurance functions

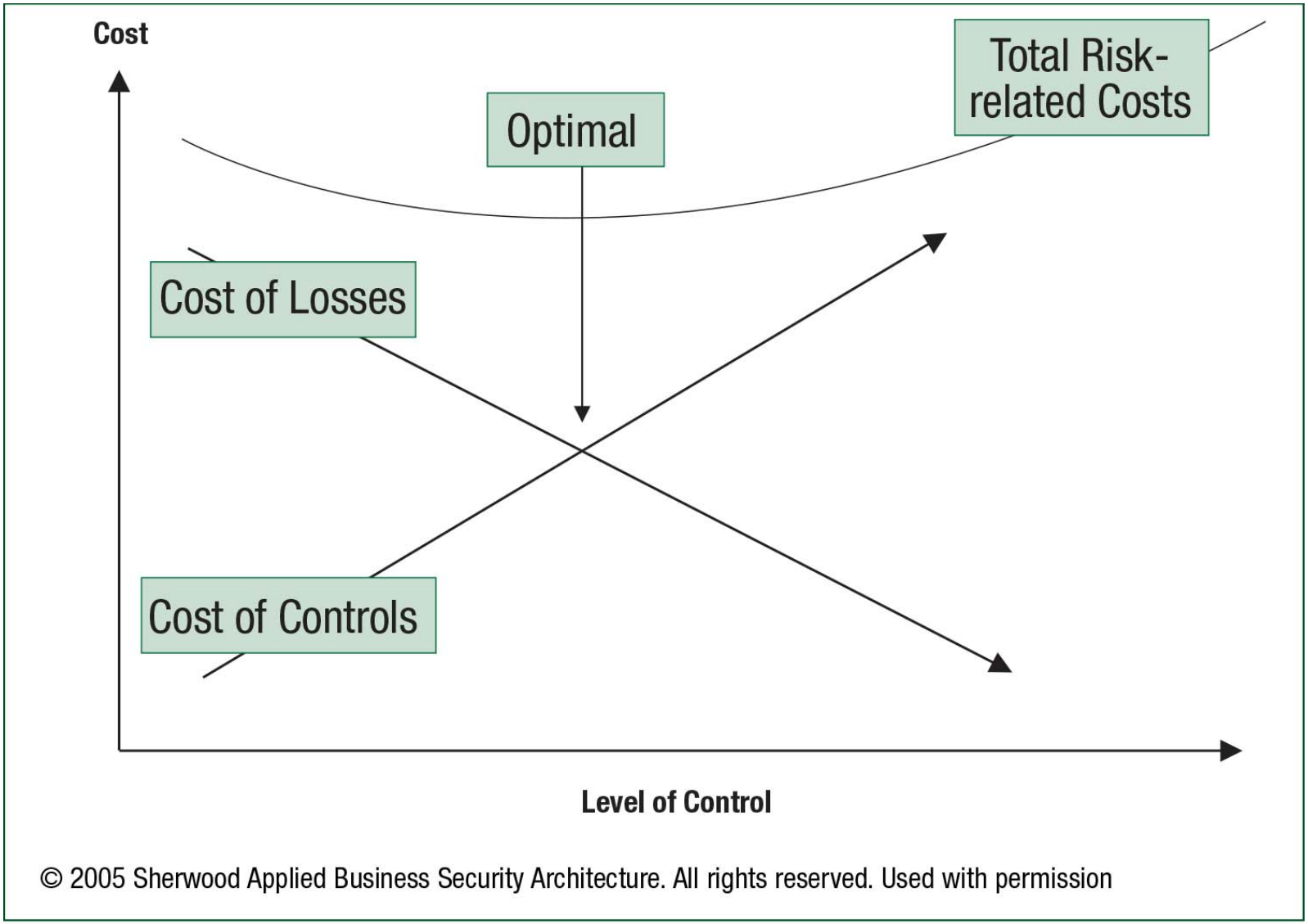
Information Security Strategy
Information Security Program Objectives

Domain 1
Information Security Governance

COBIT

Figure 3—ITGI and COBIT Maturity Scale	
Maturity Level	**Description**
0	Non-existent—No recognition by organisation of need for security
1	Initial/ad hoc—Risks considered on an ad hoc basis; no formal processes
2	Repeatable but intuitive— Emerging understanding of risk and need for security
3	Defined process—Company-wide risk management policy/security awareness
4	Managed and measurable—Risk assessment standard procedure; roles and responsibilities assigned; policies and standards in place
5	Optimized—Organization-wide processes implemented, monitored and managed

Optimizing Risk Costs



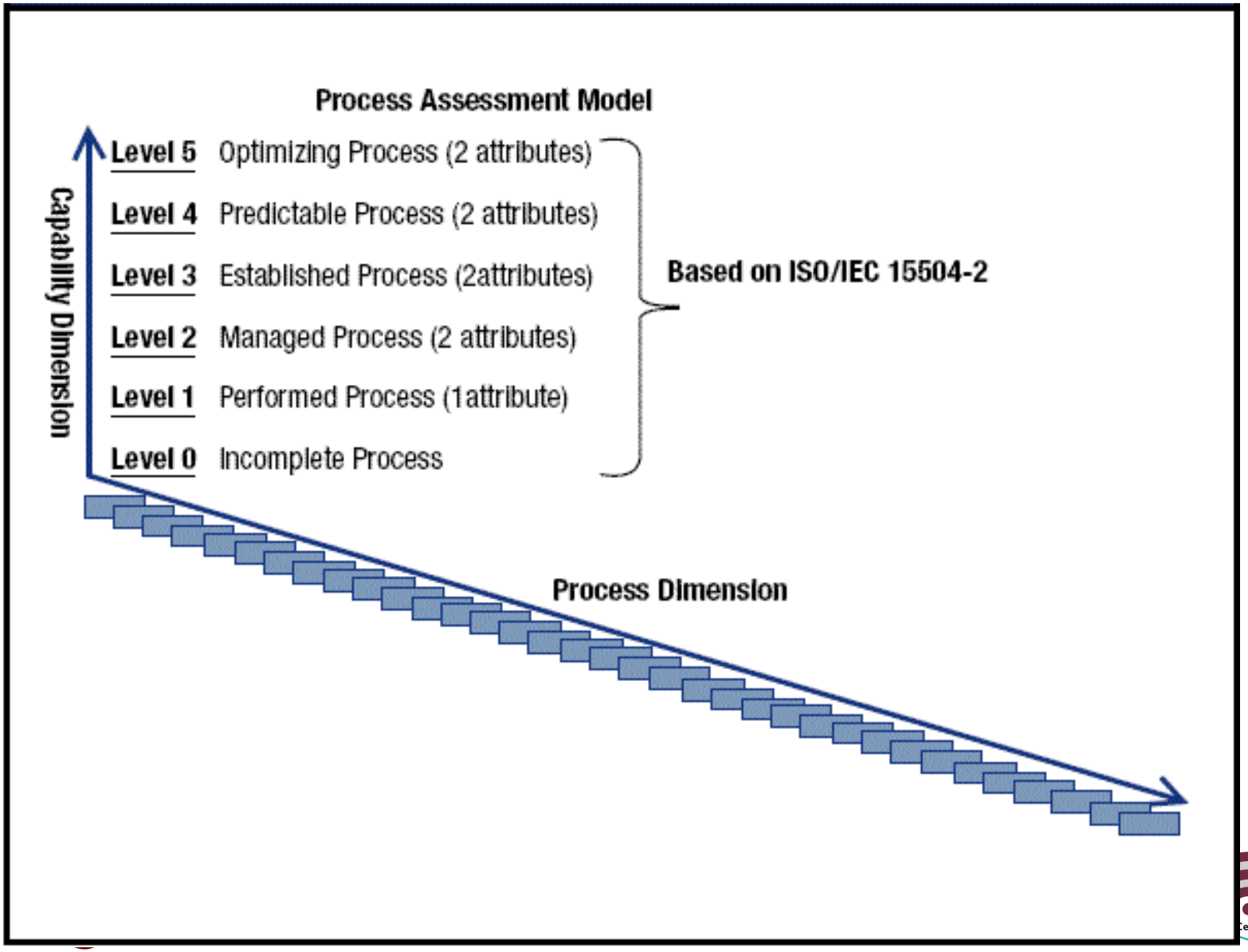
IS Strategy Objectives (ISACA)

- Strategic Alignment
- Effective Risk Management
- Value Delivery
- Resource Optimization
- Performance measurement
- Assurance process integration

Establishing a Desired State (ITGI)

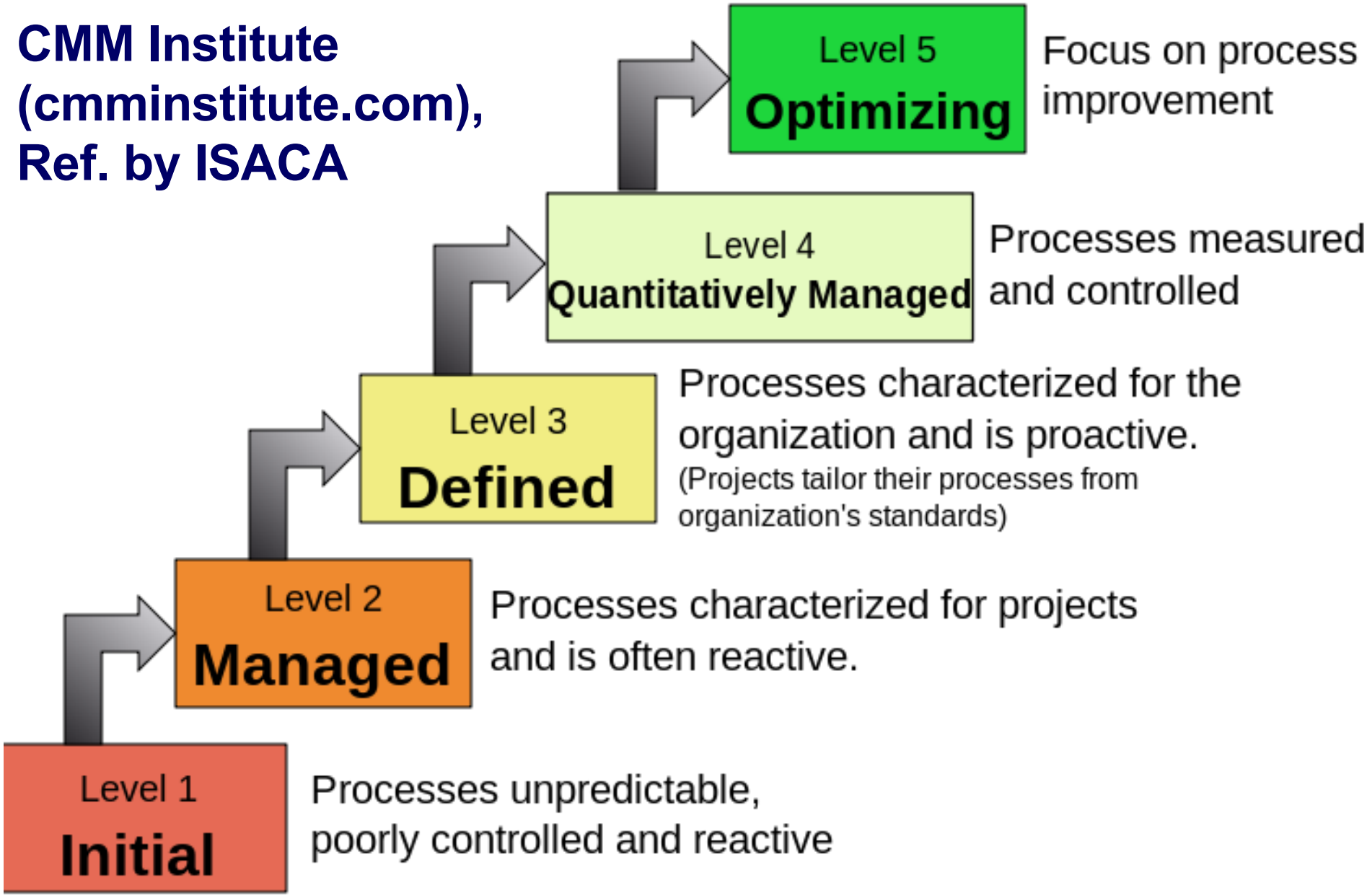
- The term ‘desired state’ is used to denote a complete snapshot of all relevant conditions at a particular point in time.
  - This includes people, processes and technologies.
- Defining a ‘state of security’ in purely quantitative terms is not possible.
  - Consequently, a ‘desired state of security’ must be defined qualitatively in terms of attributes, characteristics and outcomes.
- It can include high-level objectives such as:
  - Protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity

Overview of the Process Assessment Model (ISACA)

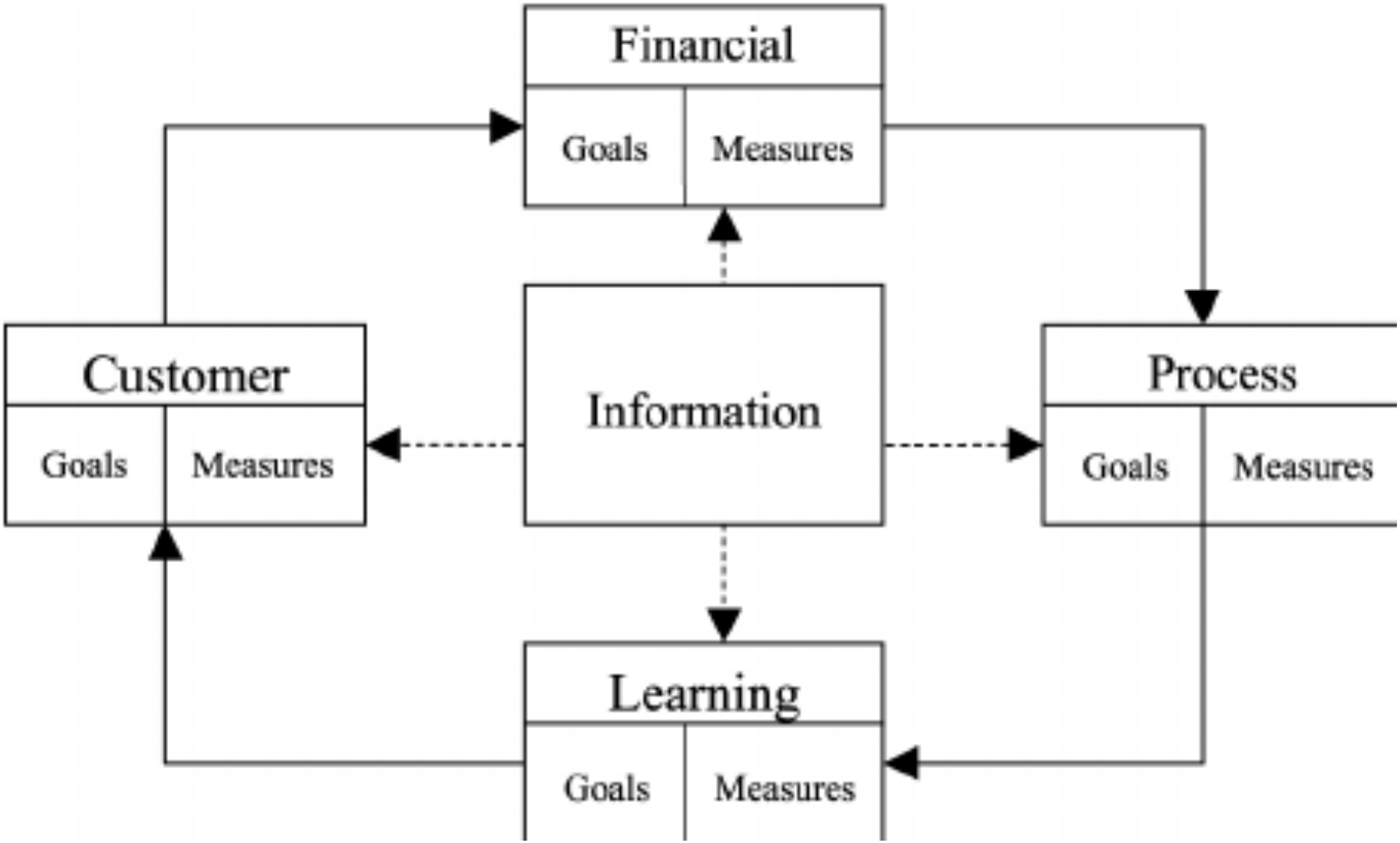


Characteristics of the Maturity levels

CMM Institute (cmminstitute.com), Ref. by ISACA



Balanced Scorecard Dimensions



Balanced Scorecard

- The balanced scorecard is a management system (not only a measurement system) that enables organizations to clarify their vision and strategy and translate them into action.
- It provides feedback around both the internal
- business processes and external outcomes in order to continuously improve strategic performance and results.
- When fully deployed, the balanced scorecard transforms strategic planning from an academic exercise into the nerve center of an enterprise.
  - Source: Balanced Scorecard Institute https://www.balancedscorecard.org

Strategy Resources

Domain 1
Information Security Governance

Elements of a Strategy (ITGI)

The available resources need to be enumerated and considered. They typically include:

- Policies
- Standards
- Processes
- Methods
- Controls
- Technologies
- People
- Skills
- Training
- Education
- Other organizational support and assurance providers

Security Architecture

- In February 2003, the White House released the National Strategy to Secure Cyber Space that responded to an urgent need for users, operators, and vendors of networked data and communications systems from both public and private sectors to work together to improve the security of the nation's information infrastructure.
- The National Strategy proposed the following goals:
  1) preventing cyber attacks against America's critical information infrastructures,
  2) reducing national vulnerability to cyber attacks, and 3) minimizing damage and recovery time from cyber attacks that may actually occur.

Security Architecture Common Elements (1/8)

1) Network security architecture:

Network security may be achieved by:

- **Eliminating network components that use shared Ethernet.**
- **Implement the concept of defense**
- **Use multiple firewalls within network.**
- **Implement intrusion detection systems at key points within network to monitor threats and attacks.**
- **Measure and report network traffic statistics for the computers on the network.**

Security Architecture Common Elements (2/8)

2) Host based security architecture:

This can be achieved through good system administration practices such as:

- **Maintain up to date virus protection.**
- **make sure that system software are configured properly, and latest patches are installed.**
- **Perform risk assessment to identify the most important computers to protect.**
- **Disable network services that are not needed and run host-based firewall on computers to block unwanted network traffic.**
- **Monitor security alerts and develop mechanism for quickly patching systems.**
- **Create centralized system logging service.**
- **Develop central authentication service to replace host-based password files**

Security Architecture Common Elements (3/8)

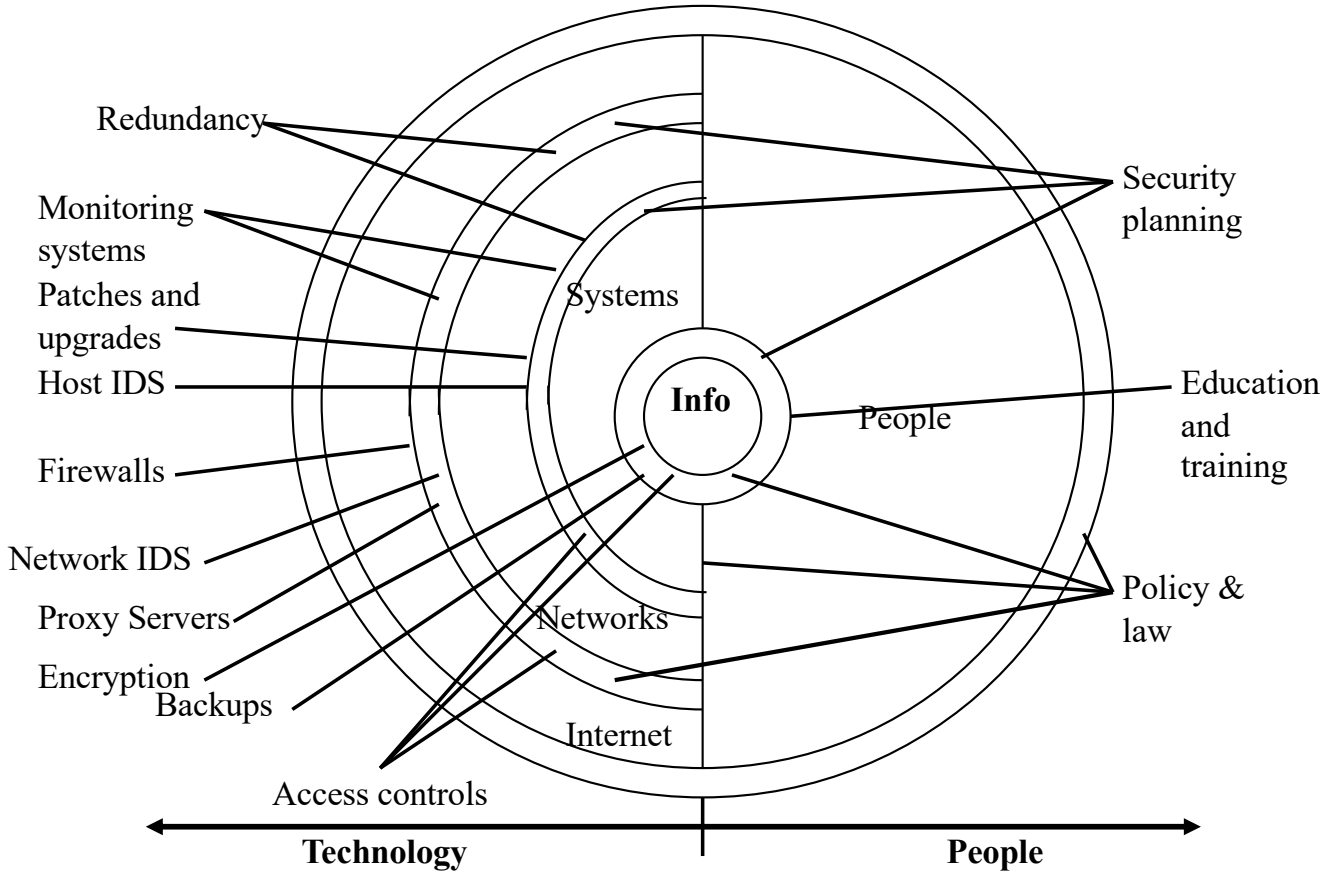
3) Application Security Architecture:

Application security deals with two main concerns:

- **Protecting the code and services running on the system, protecting who is connecting to them and protecting what is output from the programs.**
- **Delivering reusable application security services such as reusable authentication, authorization, and auditing services enabling developers to build security into their system.**

Security Architecture Common Elements (4/8)

4) Data and information Security Architecture



Sphere of use and Protection of information [Whitman and Mattord 2003]

Security Architecture Common Elements (5/8)

5) Software Security Architecture:

- Some examples of software vulnerabilities are:
  - software deletion,
  - software modifications by using Logic bomb,
  - Trojan horse,
  - viruses, worms, and Trapdoor,
  - Information leaks,
  - inserting malicious code

- There are two advantages of Software Protection:
  - Portability which ensures that a user-level software-product must coexist with a variety of operating systems. For example, it allows a browser to have platform-independent security mechanisms.
  - Performance since it offers significantly cheaper cross-domain calls whereas if they were implemented in hardware they would slow programs to an unacceptable level [Wallach et al. 1997].

Security Architecture Common Elements (6/8)

6) Hardware

Attacks against hardware:

- Since it is easy to identify and see the devices that are connected to the system, it is easy to attack by adding, changing, removing, intercepting traffic to and flooding with traffic the devices connected to the system.
- Hardware may suffer accidental acts that are not intentional "involuntary machine slaughter" where it can be drenched with water, burned, frozen, gassed or electrocuted with power surges.
- "Voluntary machine slaughter" which a person actually wants to harm the hardware of a system.

Security Architecture Common Elements (7/8)

7) Database

Security can be addressed by:

- **Operating system integrity control and recovery procedures.**
- **Element integrity is achieved by using the proper access control to protect a specify data element from being changed or written by unauthorized users.**
- **Element accuracy is ensured by using checks on the values of elements that can be used to prevent the insertion of improper values.**
- **Constraint conditions can be used to detect incorrect values.**
- **Two-phase update is used to ensure that an update operation is performed on the complete record and that no part of the data was updated before the operation is aborted for what ever reason.**
- **The database recover data by maintaining a log of users' accesses and what they have changed.**
- **The concurrency/consistency problem resulting from many users accessing or sharing the same database can be solved by using different kinds of locks.**
- **In multilevel databases, two levels of security for individual elements that are sensitive and non-sensitive are inadequate; therefore, each element should be associated with a related sensitivity level.**

Security Architecture Common Elements (8/8)

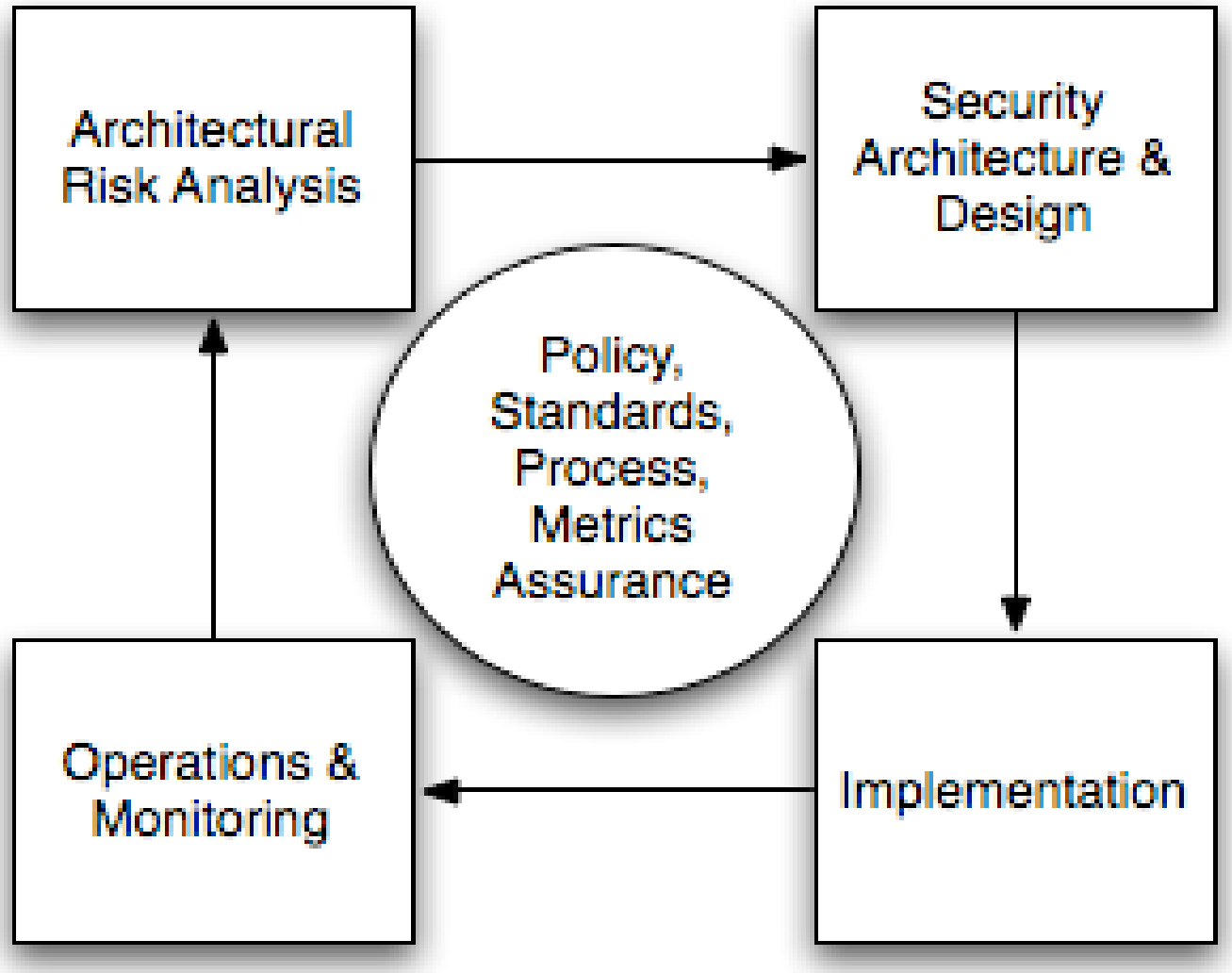
8) Physical Security

- It is in general used to describe the security needed outside the computer system.
- Some examples of the natural disasters that may affect a system are flood and fire.
- Damage may also result from power loss that can be because of an uninterruptible power supply or surge suppressors.
- Human vandals may physically attack systems which can be easily prevented by employing guards or using locks.

Principles of Security Architecture

- Set a security policy for the system and know what's on it.
- Verify actions.
- Always give the least privilege practical.
- Practice defense in depth and not rely on one form of security precaution.
- Auditing the system and keep (and review) system logs.
- Build the system to contain intrusions and minimize the consequences when a system is cracked.
- A system is only as strong as its weakest link and the more defenses a system has, the less likely that the weakest one will leave it vulnerable.
- The only way to be reliably certain that the system is secure after being successfully attacked is to reinstall the BIOS, reformat the hard drive, and restore files from a backup taken before the system was compromised.
- Practice full disclosure. When a system is successfully attacked, or is known to be vulnerable, let users know as soon as possible.

Security Architecture Process



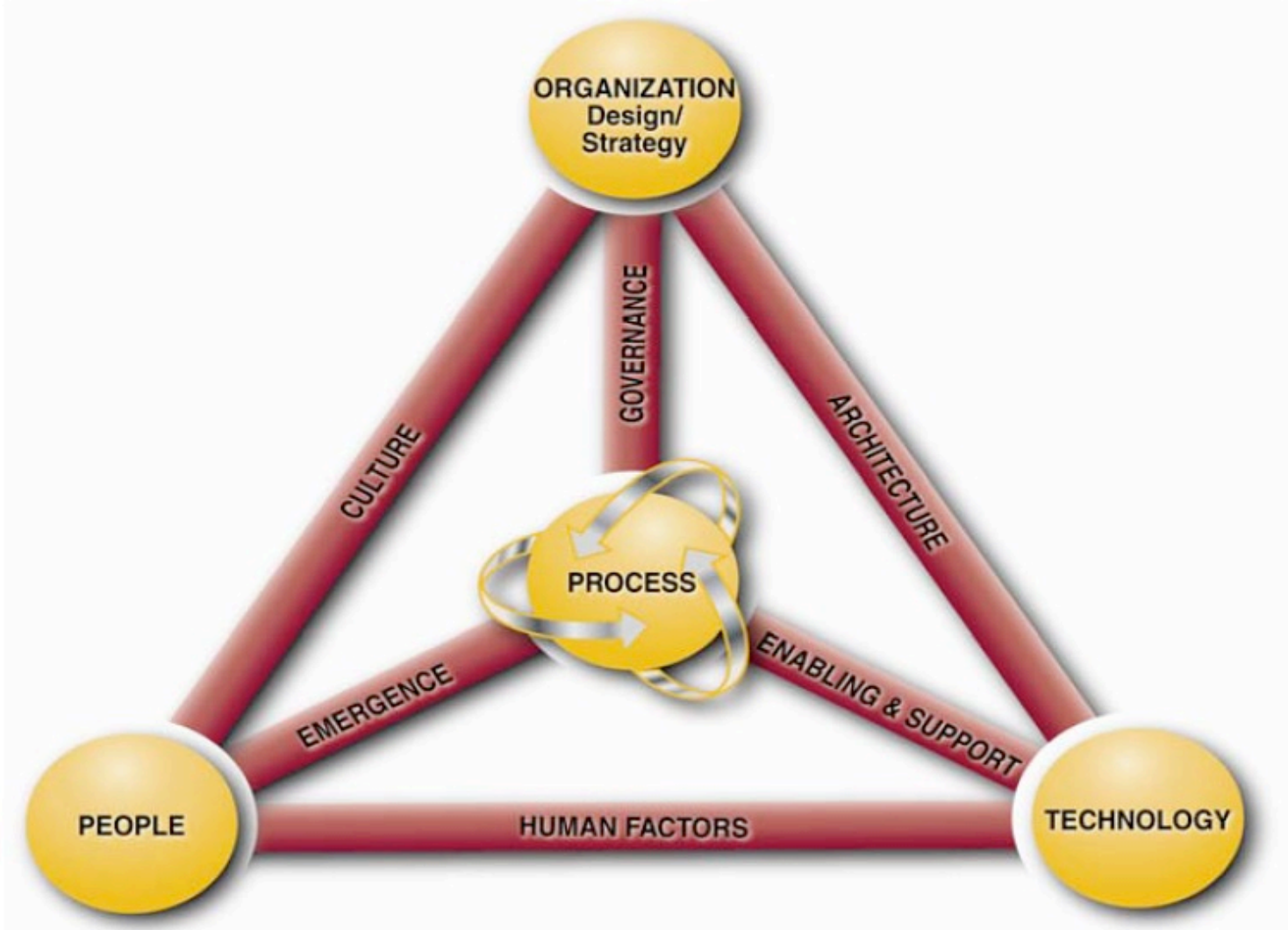
Models Capturing Security Architecture

- Designing a security architecture requires capturing the architecture in an appropriate way.
- The representation should be clear, concise and consistent to facilitate easy analysis and comparison of architectures.

Models for capturing architecture:

1) The Domain Approach is easy to understand and would allow a concise representation of an organization's discrete information sets along with any appropriate physical elements such as buildings, server rooms, and printers.
2) The Defense Architecture Framework (DoDAF) does not deal specifically with information security, and is likely too broad to be ideally suited to architecture capture.
3) 3) The International Common Criteria's Protection Profiles are formal documents that could certainly capture security architecture, but perhaps at an unnecessary level of detail.

The Institute for Critical Information Infrastructure Protection (ICIIP) MODEL



Security Architecture Comparison and Assessment

Techniques used to compare among and assess different security architectures:

- **Bayesian networks allow considering the effect of countermeasures on potential attacks. However, justifying the data used in Bayesian networks is a serious issue that needs to be considered.**
- **Simulation has dynamic nature, giving decision-makers knowledge of the architecture. However, it relies on the existence of an accurate model, which is hard to obtain in the information security domain. With risk analysis, unavailable or inaccurate data can reduce their effectiveness.**
- **The IATF robustness strategy provides minimum requirements on architectures, but the incompleteness of the strategy and its US specific requirements are issues to be considered.**
- **Game theory could theoretically provide optimal designs for security architectures. Unfortunately, it is not well developed enough for the information security domain to be relied upon.**
- **Survivability analysis techniques are useful for architecture assessment, but are restricted to architectures containing networks.**
- **Economic models have practical, non-technical uses, incorporating a human factors and system view into the security architecture analysis. However, they do not provide the most important answers for government and Defense information systems.**

SABSA (Wikipedia) (1/2)

- SABSA is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives.
- The primary characteristic of the SABSA model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited.
- The process analyzes the business requirements at the outset, and creates a chain of traceability through the strategy and concept, design, implementation, and ongoing 'manage and measure' phases of the lifecycle to ensure that the business mandate is preserved.

SABSA (Wikipedia) (2/2)

- **The model is layered, with the top layer being the business requirements definition stage.**
  - **At each lower layer a new level of abstraction and detail is developed, going through the definition of the conceptual architecture, logical services architecture, physical infrastructure architecture and finally at the lowest layer, the selection of technologies and products (component architecture).**
- **The SABSA model itself is generic and can be the starting point for any organization, but by going through the process of analysis and decision-making implied by its structure,**
  - **`it becomes specific to the enterprise, and is finally highly customized to a unique business model. It becomes in reality the enterprise security architecture, and it is central to the success of a strategic program of information security management within the organization.**

SABSA (ISACA)

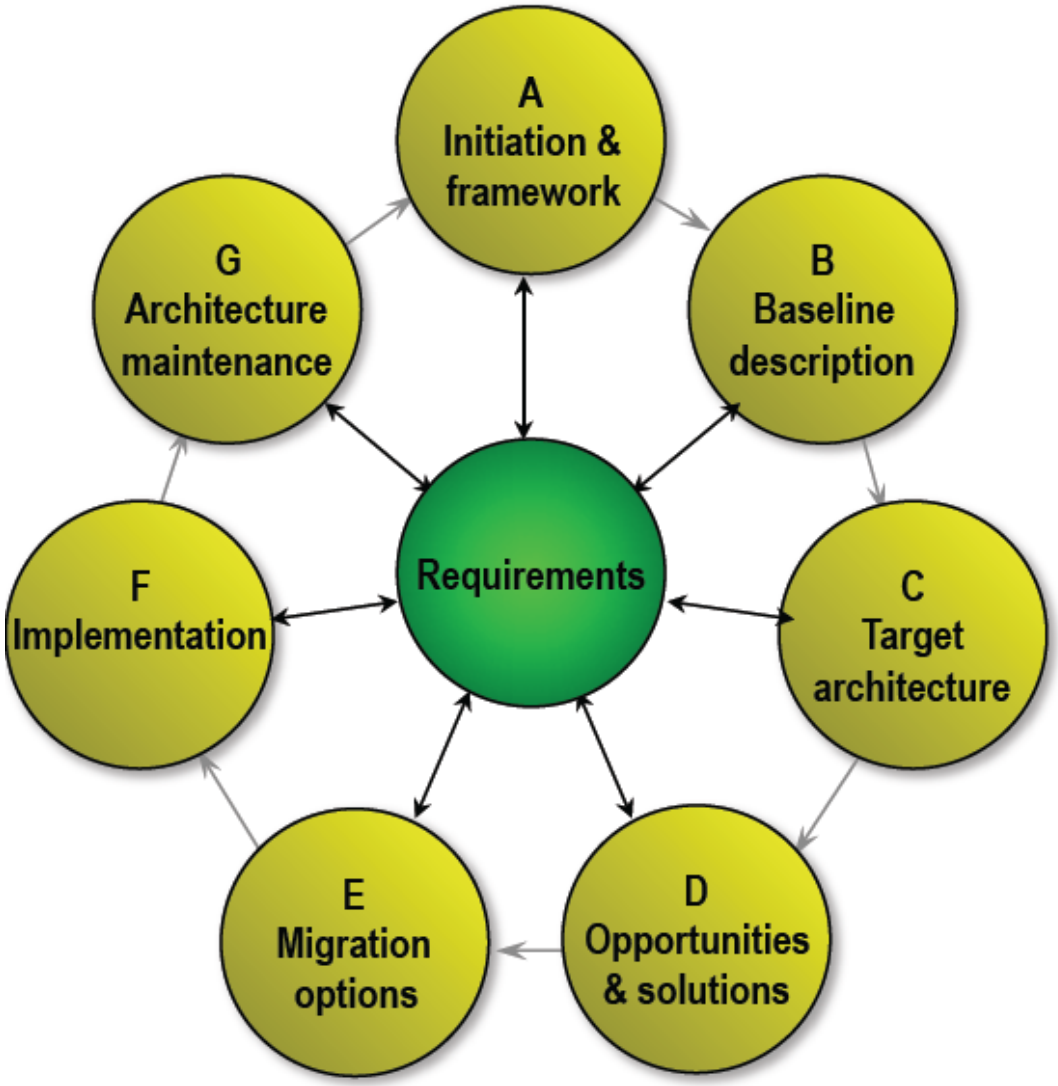
	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The business	Business risk model	Business process model	Business organisation and relationships	Business geography	Business time dependencies
Conceptual	Business attributes profile	Control objectives	Security strategies and architectural layering	Security entity model and trust framework	Security domain model	Security-related lifetimes and deadlines
Logical	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Physical	Business data model	Security rules, practices and procedures	Security mechanisms	Users, applications and the user interface	Platform and network infrastructure	Control structure execution
Component	Detailed data structures	Security standards	Security products and tools	Identities, functions, actions and ACLs*	Processes, nodes, addresses and protocols	Security step timing and sequencing
Operational	Assurance of operational continuity	Operational risk management	Security service management and support	Application and user management and support	Security of sites, networks and platforms	Security operations schedule

*Access control lists

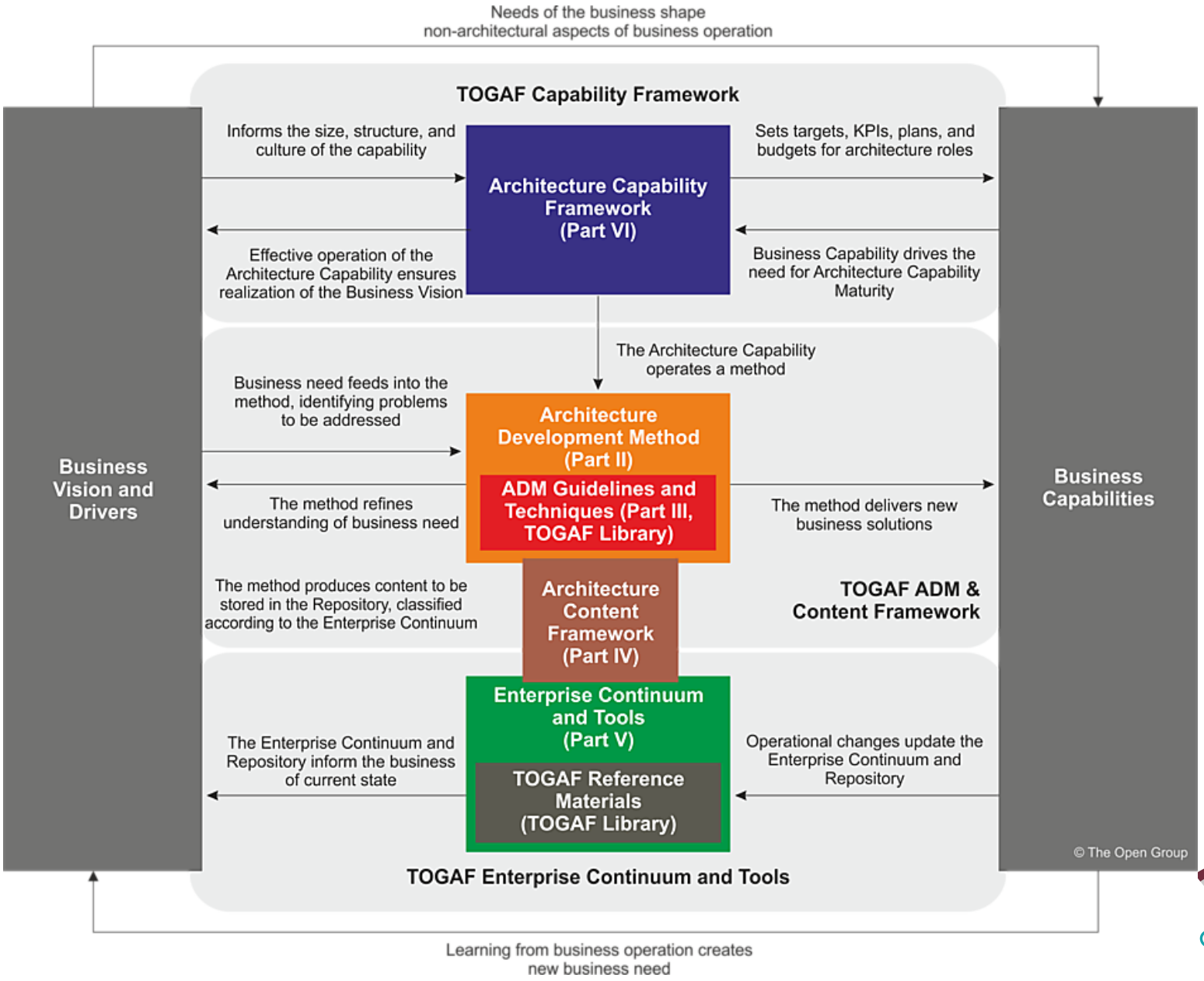
TOGAF & The Open Group

- The TOGAF standard is a framework for Enterprise Architecture. It may be used freely by any organization wishing to develop an Enterprise Architecture for use within that organization.
- The TOGAF standard is developed and maintained by members of The Open Group, working within the Architecture Forum.
  - The original development of TOGAF Version 1 in 1995 was based on the Technical Architecture Framework for Information Management (TAFIM), developed by the US Department of Defense (DoD).
  - The DoD gave The Open Group explicit permission and encouragement to create Version 1 of the TOGAF standard by building on the TAFIM, which itself was the result of many years of development effort and many millions of dollars of US Government investment.

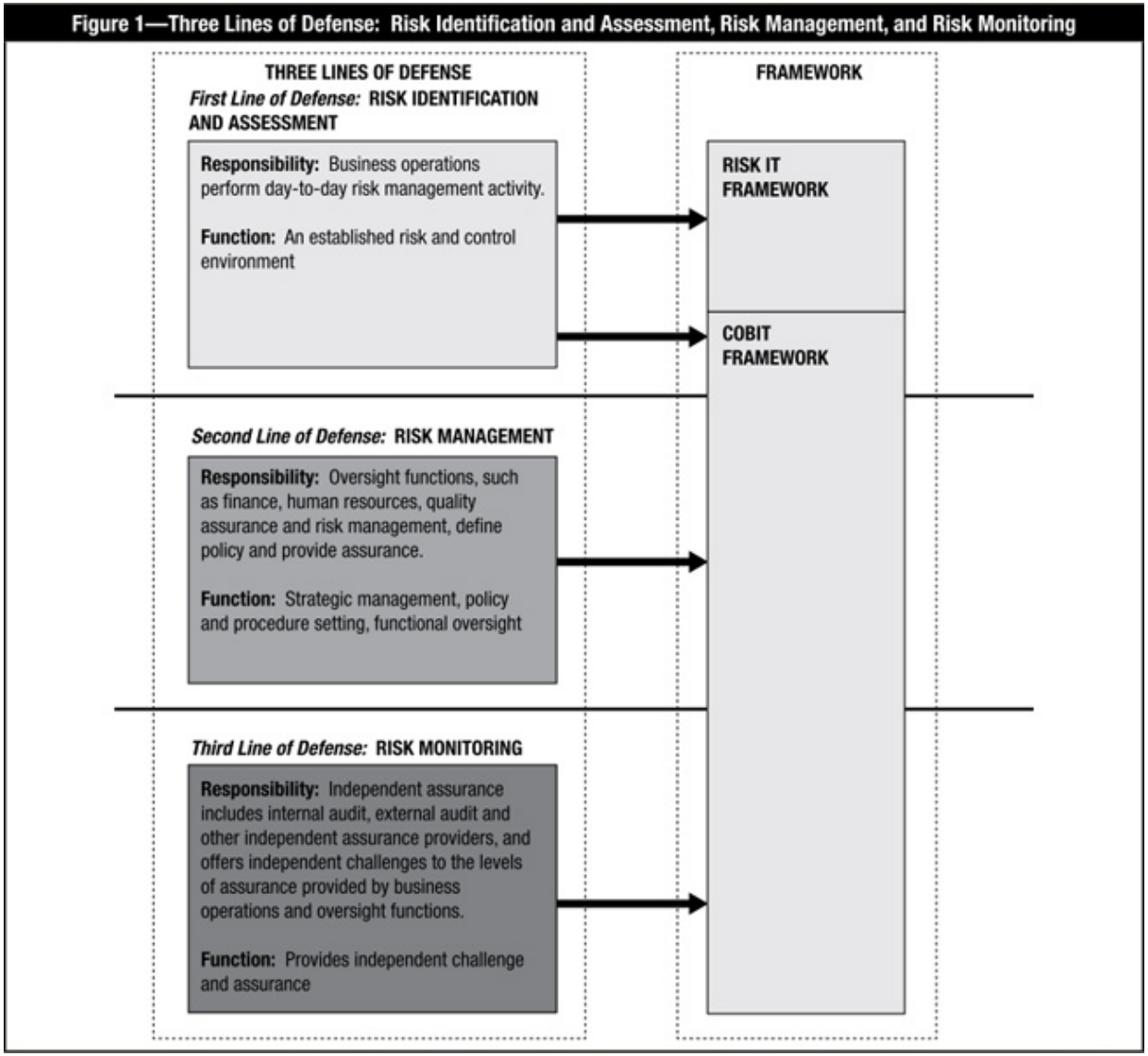
The Open Group Architecture Framework (TOGAF)



The Open Group Architecture Framework



3 Lines of Defense (ISACA)



Strategy Constraints and Action Plan for Strategy Implementation

Domain 1
Information Security Governance

Strategy Constraints (ITGI)

- **Constraints to a strategy and subsequent action plan.**
  - Law —Legal and regulatory requirements
  - Physical —Capacity, space and environmental constraints
  - Ethics —Appropriate, reasonable and customary
  - Culture —Both inside and outside the organization
  - Costs —Time and money
  - Personnel —Resistance to change; resentment against new constraints
  - Resources —Capital, technology and people
  - Capabilities —Knowledge, training, skills and expertise
  - Time —Window of opportunity; mandated compliance
  - Risk tolerance —Threats, vulnerabilities and impacts

Gap Analysis—Basis for an Action Plan (ITGI)

- **Establishing a strategy will require one or more actions, projects or plans.**
  - **An analysis of the gap between the current state and the desired state for each defined metric will identify the requirements and priorities for a plan of action.**
  - **Gap analysis will be required for various components of the strategy previously discussed, such as maturity levels, control objectives, and risk and impact objectives.**
  - **This exercise may need to be repeated annually, or more frequently, to provide performance and goal metrics and information on possible corrections needed in response to changing environments or other factors.**
  - **A typical approach to gap analysis is to work backward from the end point to the current state and determine the intermediate steps needed to accomplish the objectives.**

Action Plan (ITGI)

- An action plan to execute the strategy must create or modify policies and standards as needed.
  - Policies are the constitution of governance;
  - Standards are the law.
  - Policies must capture the intent and direction of management.
- As a strategy evolves, it is vital that supporting policies be developed to articulate the strategy.
  - For example, if the objective is to become ISO/IEC 27001-compliant over a three-year period, the strategy must consider
    - which elements are addressed first,
    - what resources are allocated,
    - how the elements of the standard can be accomplished, etc.
  - The road map will show the steps and the sequence, dependencies and milestones.
- The action plan is essentially a project plan to implement the strategy following the road map.

Policy Definitions (ITGI) 1/3

- **Policies—High-level statements of management intent, expectations and direction.**
  - **An example of a policy statement on access control is: 'Information resources shall be controlled in a manner that effectively prevents unauthorized access'.**
  - **Policy can be considered the 'constitution' of security governance.**
- **Standards—Metrics, allowable boundaries or the process used to determine whether procedures meet policy requirements.**
  - **An example of a standard for passwords used for access control is: 'Passwords for medium- and low-security domains must be comprised of no fewer than eight characters consisting of a mixture of upper- and lower-case letters, at least one number and one punctuation mark**

Policy Definitions (ITGI) 2/3

- **Procedures—The portion of an information security policy that states the general process that will be performed to accomplish a security goal.**
  - **Procedures can be the responsibility of operations but can also include security-specific activities intended to support operational aspects of the information security program.**
    - **Procedures must be unambiguous and include all necessary steps needed to accomplish specific tasks.**
    - **Procedures must define expected outcomes and displays as well as dependencies and conditions required for execution.**
    - **Procedures must also contain the steps required when unexpected results occur.**
    - **Procedures must be clear and unambiguous &terms must be exact.**
      - **For example, the words 'must', 'shall' and 'will' shall be used for any task that is mandatory. The word 'should' must be used only to mean a preferred action that is not mandatory. The terms 'may' or 'can' must be used only to denote a purely discretionary action.**
      - **Procedures for passwords should include the detailed steps for setting up password accounts & for changing or resetting passwords.**

Policy Definitions (ITGI) 3/3

- **Guidelines—A description of a particular way of accomplishing something that is less prescriptive than a procedure.**
  - **Guidelines are often the responsibility of operations but can also be used within business units to provide guidance for management, who is defining department-specific procedures.**
  - **Guidelines should contain information that will be helpful in executing procedures. Information can include suggestions and examples, narrative clarifying the procedures, useful background information, and tools.**

Attributes of Good Policies (ITGI)

- Information security policies should be an articulation of a well-defined information security strategy and capture the intent, expectations and direction of management.
  - Each policy should state only one general security mandate.
  - Policies must be clear and easily understood by all affected parties.
  - Policies should rarely be more than a few sentences long.

Standards (ITGI)

- **Standards are a powerful information security management tool.**
  - **They set the permissible bounds for procedures and practices of technology and systems and for people & events.**
  - **Properly implemented, they are the law to policy's constitution.**
  - **They provide the measuring stick for policy compliance and a sound basis for audits.**
  - **They govern the creation of procedures and guidelines.**
  - **Standards serve to create information security baselines, i.e., the minimum level of security across the enterprise.**
    - **It is, therefore, important that all information security policies be expressed through a complete set of standards to ensure there are no significant gaps or 'weak links'.**
  - **Regular, systematic standards, compliance monitoring and enforcement processes are critical to ensure that the intentions of policies are met, and should themselves be the subject of a set of policies and standards.**

Action Plan Intermediate Goals
ITGI Example for ISO/IEC 27002 Compliance

- Assign each business unit to identify current applications in use and their criticality and sensitivity
- Review 25 percent of stored information to determine ownership, criticality and sensitivity
- Assign each business unit to complete a BIA to identify critical resources
- Develop metrics and a reporting system tied to business objectives
- Define and document all security roles and responsibilities
- Develop a process to ensure business process linkages
- Perform a comprehensive risk assessment for each business unit
- Educate all users on the acceptable use policy
- Review all policies for strategic alignment and revise as necessary
- Develop standards for all policies for each business unit

Action Plan Metrics (ITGI)

- The plan of action to implement the strategy will require methods to monitor and measure progress and the achievement of milestones.
- Possible methodologies
  - Capability Maturity Model (CMM)
  - Balanced Scorecard (BSC)
  - COBIT (Controlled Objective for Information and Related Technologies)
- Each plan of action will benefit from an appropriate set of KPIs, defining critical success factors (CSFs) and setting KGIs.

Action Plan KGIs (ITGI)

- **Key Goal Indicators (KGIs)—Defining clear objectives and achieving consensus on the goals are essential to developing meaningful metrics.**
- **Key goals could include:**
  - **Achieving Sarbanes-Oxley controls testing compliance mandates**
  - **Completing independent controls testing, compliance validation and attestation**
  - **Preparing a required statement of control effectiveness**
    - **Sarbanes-Oxley requires that, for organizations publicly traded in the US, all financial controls be tested for effectiveness within 90 days of reporting.**
    - **The results of testing must be signed by the CEO and CFO, and be attested to by the organization's auditors.**
    - **The results then must be included in the organization's public filings to the US Securities Exchange Commission (SEC).**

Action Plan CSFs (ITGI)

- **Critical Success Factors (CSFs)—To achieve Sarbanes-Oxley compliance, certain steps must be accomplished to achieve the required objectives:**
  - **Identifying, categorizing and defining controls**
  - **Defining appropriate tests to determine effectiveness**
  - **Committing resources to accomplish required testing**
    - **Large organizations may have hundreds (or more) of controls that usually have been developed over a period of time. In many cases, these controls are ad hoc and have not been subject to formal processes.**
  - **It is necessary to identify control processes, procedures, structures and technologies so that an appropriate testing regime can be developed.**
  - **Determining the necessary resources and testing procedures is critical to accomplish the required tests.**

Action Plan KPIs (ITGI)

- **Key Performance Indicators (KPIs)**
  - **Control effectiveness testing plans**
  - **Progress in control effectiveness testing**
  - **Results of testing control effectiveness**
- **For management to track progress in the testing effort, appropriate testing plans must be developed, consistent with the defined goals and encompassing the CSFs.**
- **Because of the limited time (90 days) available to perform the required tests, management needs reports on the progress and results of testing.**

General Metrics Considerations (ITGI)

- Considerations for information security metrics include ensuring the relevance of what is being measured.
- Because information security is difficult to measure in any objective sense, relatively meaningless metrics are often used simply because they are readily available.
- Different metrics will be more or less useful for different parts of the organization and should be determined in collaboration with business process owners.

General Metrics Considerations (ITGI)

- Senior management typically is not interested in detailed technical metrics
  - number of virus attacks thwarted
  - passwords reset.
- Senior management typically wants a summary or 'roll up' of information important from a management perspective—information that typically excludes detailed technical data.
- This summary may include:
  - Progress according to plan and budget
  - Significant changes in risk and possible impacts to business objectives
  - Results of disaster recovery testing
  - Audit results
  - Regulatory compliance status

General Metrics Considerations (ITGI)

- The information security manager may want more detailed information, including such data as:
  - Policy compliance metrics
  - Significant process, system or other changes that may affect risk profile
  - Patch management status
  - Exceptions and variances to policy or standards
- In organizations that have an IT security manager, it is likely that all available technical security data can be useful. These data may include:
  - Vulnerability scan results
  - Server configuration standards compliance
  - IDS monitoring results
  - Firewall log analysis

Metrics Summary (ITGI) 1 / 2

- Useful information security metrics are often difficult to design and implement.
  - Since a standard predictive security yardstick does not exist, most measures are just indicative of possible risks and potential impacts.
  - The lack of predictive value often results in the collection of vast amounts of data to try to ensure nothing significant is overlooked.
- The result can be that the sheer volume of data makes it difficult to see the big picture, and efforts should be made to develop processes to distill data into useful information.
  - A collaborative effort with various constituencies may help determine which security information is useful and what it means.

Metrics Summary (ITGI) 2 / 2

- The focus is often on IT vulnerabilities, regardless of whether a threat exists or the potential impact is significant.
- Simply knowing the number of open vulnerabilities provides no information on risk, threats or impacts, and, by itself, is of little use.
- Metrics design and monitoring activities should take into consideration:
  - What is important to information security operations
  - The requirements of IT security management
  - The needs of business process owners
  - The requirements of senior management