ISACA®

Trust in, and value from, information systems

COBIT FOR INFORMATION SECURITY

K.Seeburn

AGENDA

1. **Quick Intro into COBIT 5**

   Information, Enterprise Benefits, Stakeholder Value, COBIT 5 Framework , COBIT 5 Principles , COBIT 5 Enablers, Governance & Management

2. **COBIT 5 for Information Security**

   - *COBIT 5 Product Family, COBIT 5 for Information Security / What does it Contain?, Drivers, Benefits, Information Security Defined, Using COBIT 5 Enablers for Implementing Information Security, Enabler: Principles, Policies & Frameworks*
   - *Information Security Principles*
   - *Information Security Policies*
   - *Enabler: Process, Enabler: Organisational Structures, Enabler: Culture, Ethics & Behaviour, Enabler: Information, Enabler: Services, Infrastructure & Applications, Enabler: People, Skills & Competencies*

3. **Implementing Information Security Initiatives**

4. **Using COBIT 5 for Information Security to connect other Frameworks, Models, Good Practices & Standards**

ISACA®
Trust in, and value from, information systems

QUICK INTRO INTO COBIT 5

— KETAN DHOLAKIA, CISM, CRISC
MANAGING PARTNER, MACLEAR
CHICAGO, ILLINOIS, USA
ISACA MEMBER SINCE 2007

MORE EMPOWERED

ISACA®
Trust in, and value from, information systems

INFORMATION

- Information is a key resource for all enterprises.
- Information is created, used, retained, disclosed and destroyed.
- Technology plays a key role in these actions.
- Technology is becoming pervasive in all aspects of business and personal life.

What benefits do information and technology bring to enterprises?

ENTERPRISE BENEFITS

Enterprises and their executives strive to:

- Maintain quality information to support business decisions.
- Generate business value from IT-enabled investments, i.e., achieve strategic goals and realise business benefits through effective and innovative use of IT.
- Achieve operational excellence through reliable and efficient application of technology.
- Maintain IT-related risk at an acceptable level.
- Optimise the cost of IT services and technology.

How can these benefits be realised to create enterprise stakeholder value?

STAKEHOLDER VALUE

- Delivering enterprise stakeholder value requires good **governance and management** of information and technology (IT) assets.
- Enterprise boards, executives and management have to **embrace IT** like any other significant part of the business.
- External **legal, regulatory and contractual compliance** requirements related to enterprise use of information and technology are increasing, threatening value if breached.

- **COBIT 5 provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT.**

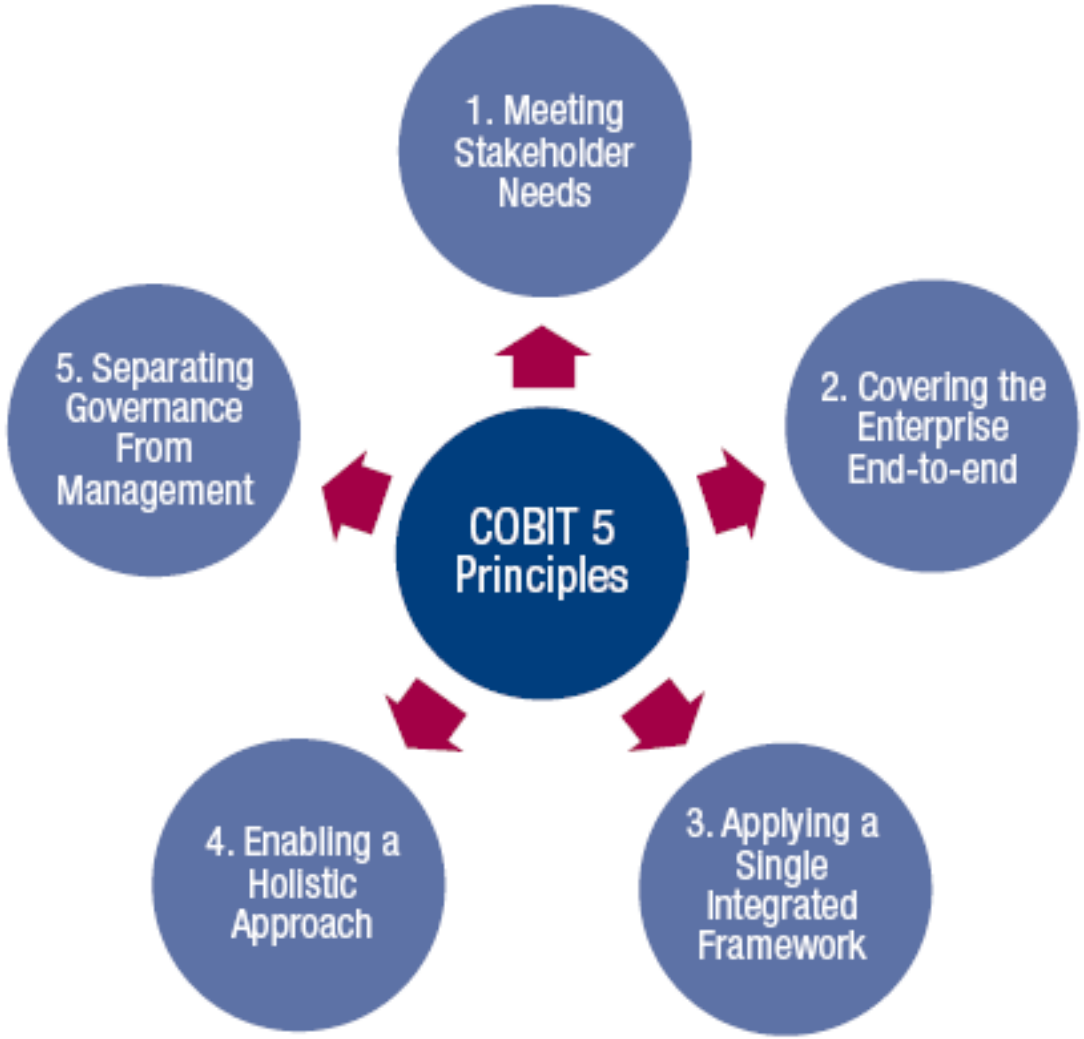
THE COBIT 5 FRAMEWORK

- Simply stated, COBIT 5 helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use.

- COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.

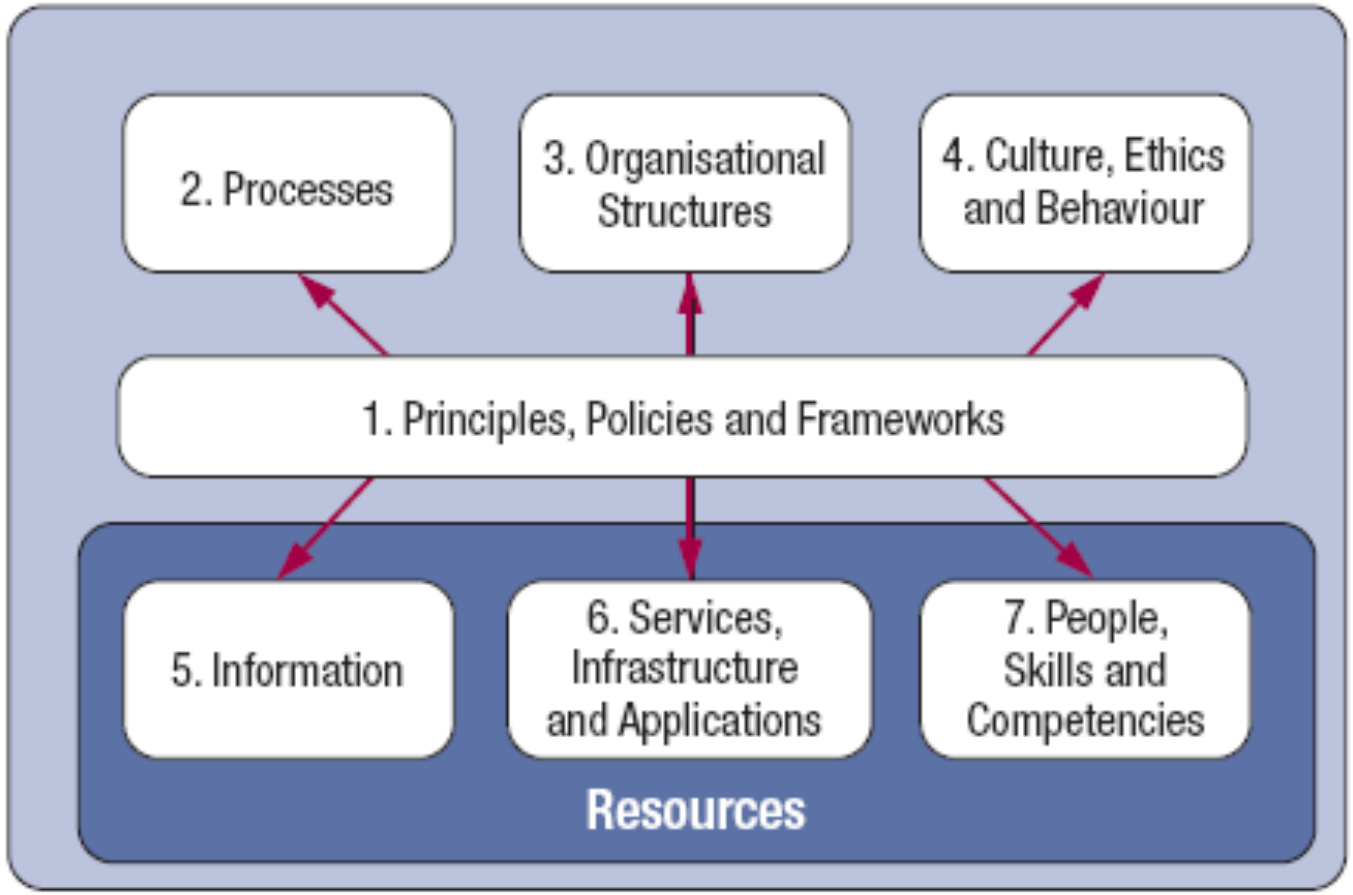
- The COBIT 5 **principles** and **enablers** are generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

COBIT 5 PRINCIPLES



ISACA®
Trust in, and value from, information systems

COBIT 5 ENABLERS



ISACA®
Trust in, and value from, information systems

GOVERNANCE & MANAGEMENT

- **Governance** ensures that stakeholder needs, conditions and options are **evaluated** to determine balance, agreed-on enterprise objectives to be achieved; setting **direction** through prioritisation and decision making; and **monitoring** performance, compliance and compliance against agreed-on direction and objectives (**EDM**).

- **Management plans, builds, runs** and **monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives (**PBRM**).

IN SUMMARY

COBIT 5 *brings together the* ***five principles*** *that allow the enterprise to build an effective* ***governance*** *and* ***management*** *framework based on a holistic set of* ***seven enablers*** *that optimises* ***information*** *and* ***technology*** *investment and use for the benefit of stakeholders.*

ISACA®
Trust in, and value from, information systems

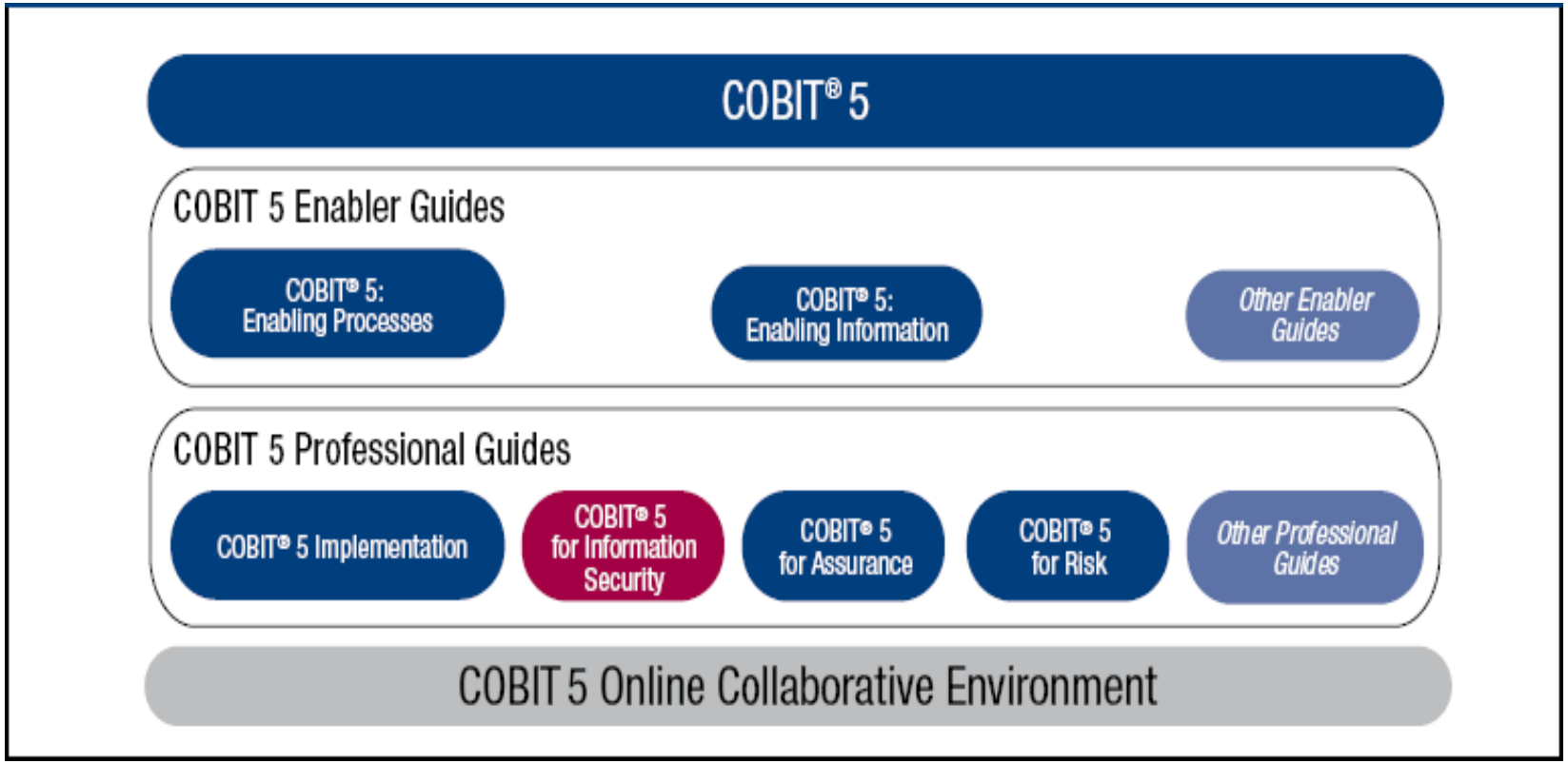
COBIT 5 FOR INFORMATION SECURITY

— **DEBBIE NEWMAN**
CONSULTANT, DELOITTE & TOUCHE LLP
CHICAGO, ILLINOIS, USA
ISACA MEMBER SINCE 2012

MORE EFFECTIVE

ISACA®
Trust in, and value from, information systems

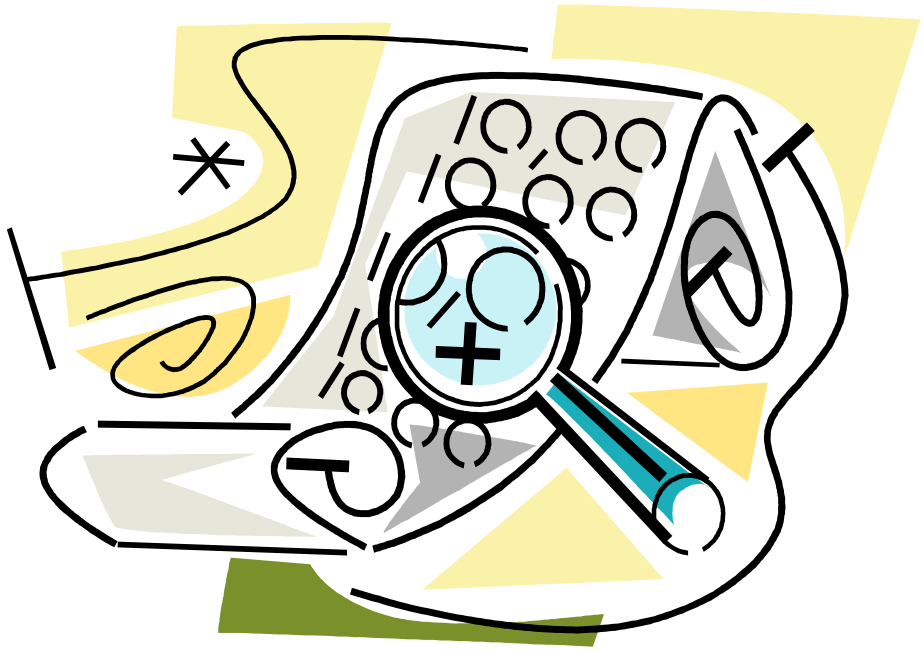
COBIT 5 PRODUCT FAMILY



Source: *COBIT® 5 for Information Security*, figure 1. © 2012 ISACA® All rights reserved.

ISACA®
Trust in, and value from, information systems

COBIT 5 FOR INFORMATION SECURITY



- ✓ Extended view of COBIT5
- ✓ Explains each component from info security perspective

ISACA®
Trust in, and value from, information systems

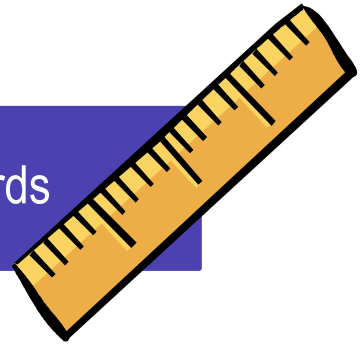
WHAT DOES IT CONTAIN?

Guidance on drivers, benefits

Principles from infosec perspective

Enablers for support

Alignment with standards



ISACA®
Trust in, and value from, information systems

DRIVERS

The major drivers for the development of *COBIT 5 for Information Security* include:

1. **The need to describe information security in an enterprise context**

2. **An increasing need for enterprises to:**
   - Keep risk at acceptable levels.
   - Maintain availability to systems and services.
   - Comply with relevant laws and regulation.

3. **The need to connect to and align with other major standards and frameworks**

4. **The need to link together all major ISACA research, frameworks and guidance**

ISACA®
Trust in, and value from, information systems

BENEFITS

Using *COBIT 5 for Information Security* can result in a number of benefits, including:

- Reduced complexity and increased cost-effectiveness due to improved and easier integration of information security standards
- Increased user satisfaction with information security arrangements and outcomes
- Improved integration of information security in the enterprise
- Informed risk decisions and risk awareness
- Improved prevention, detection and recovery
- Reduced impact of security incidents
- Enhanced support for innovation and competitiveness
- Improved management of costs related to the information security function
- Better understanding of information security

INFORMATION SECURITY DEFINED

ISACA defines information security as something that:

Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability).

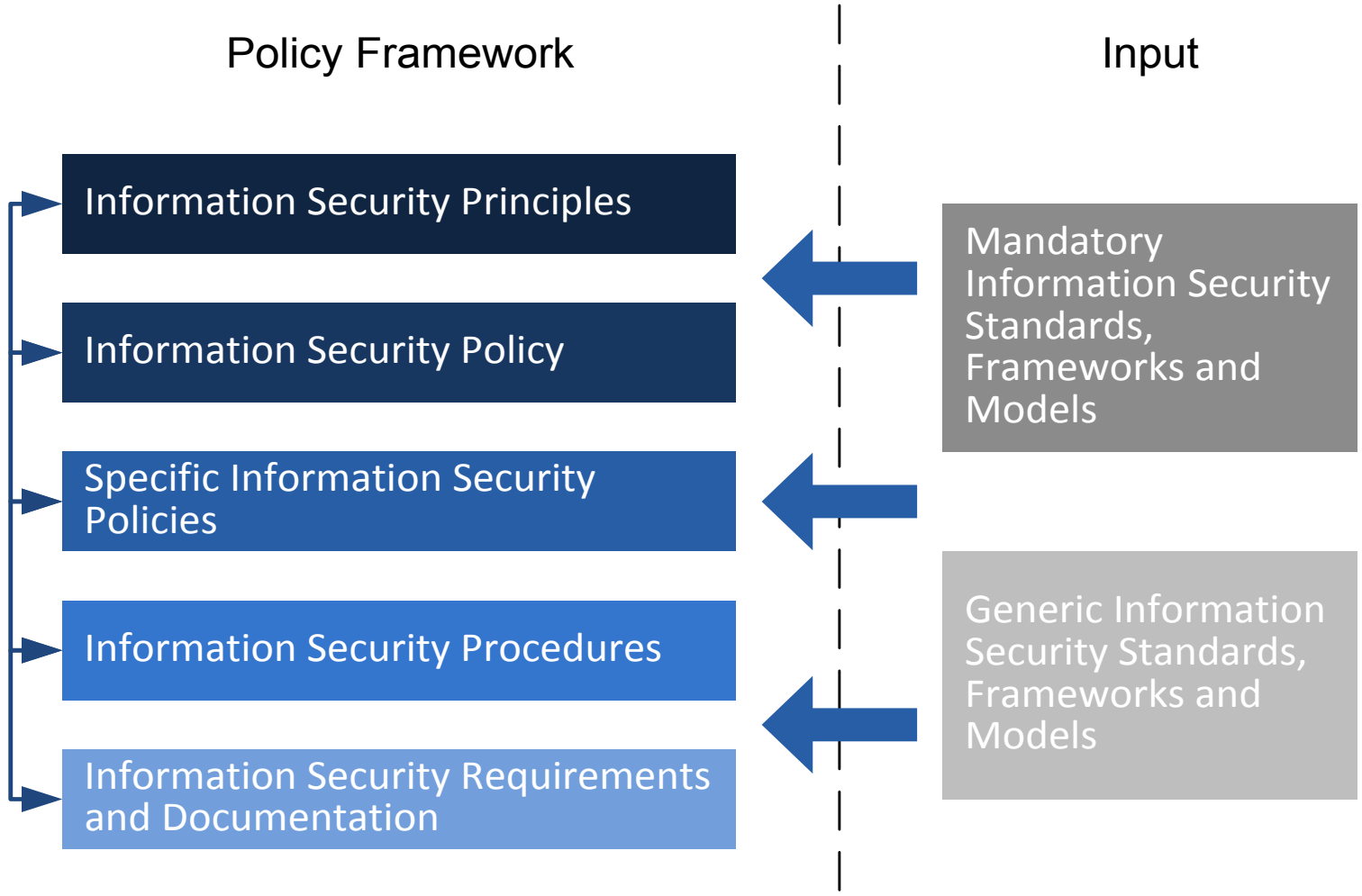
USING COBIT 5 ENABLERS FOR IMPLEMENTING INFORMATION SECURITY

***COBIT 5 for Information Security* provides specific guidance related to all enablers**

1. Information security **policies, principles, and frameworks**
2. **Processes**, including information security-specific details and activities
3. Information security-specific **organisational structures**
4. In terms of **culture, ethics and behaviour**, factors determining the success of information security governance and management
5. Information security-specific **information** types
6. **Service capabilities** required to provide information security functions to an enterprise
7. **People, skills and competencies** specific for information security

ISACA®
Trust in, and value from, information systems

ENABLER: POLICIES, PRINCIPLES & FRAMEWORKS (CONT.)



Source: *COBIT 5 for Information Security,* figure 10.

INFORMATION SECURITY PRINCIPLES

Information security principles communicate the rules of the enterprise. These principles need to be:

- Limited in number
- Expressed in simple language

In 2010 ISACA, ISF and ISC^2 worked together to create 12 principles* that will help information security professionals add value to their organisations. The principles support 3 tasks:

- Support the business.
- Defend the business.
- Promote responsible information security behaviour.

* Principles are covered in *COBIT 5 for Information Security* and can also be located at *www.isaca.org/standards*

ISACA®
Trust in, and value from, information systems

INFORMATION SECURITY POLICIES

Policies provide more detailed guidance on how to put principles into practice. Some enterprises may include policies such as:

- Information security policy
- Access control policy
- Personnel information security policy
- Incident management policy
- Asset management policy

COBIT 5 for Information Security describes the following attributes of each policy:

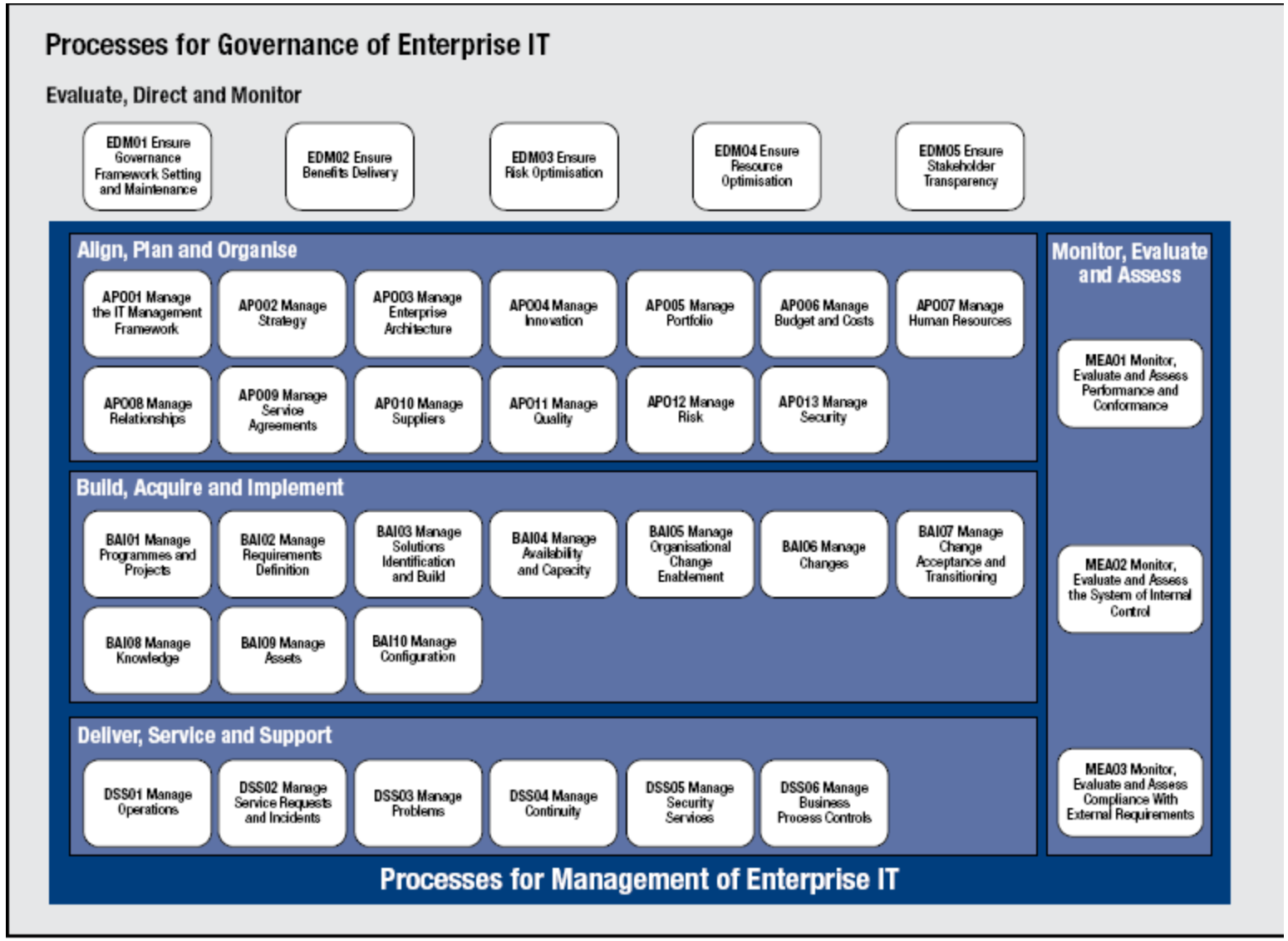
- Scope
- Validity
- Goals

ENABLER: PROCESSES

The COBIT 5 process reference model subdivides the IT-related practices and activities of the enterprise into two main areas—governance and management—with management further divided into domains of processes:

- The Governance domain contains five governance processes; within each process, evaluate, direct and monitor (EDM) practices are defined.
- The four Management domains are in line with the responsibility areas of plan, build, run and monitor (PBRM).
- *COBIT 5 for Information Security* examines each of the processes from an information security perspective.

ENABLER: PROCESSES (CONT.)



Source: *COBIT 5 for Information Security*, figure 7.

ENABLER: ORGANISATIONAL STRUCTURES

COBIT 5 examines the organisational structures model from an information security perspective. It defines information security roles and structures and also examines accountability over information security, providing examples of specific roles and structures and what their mandate is, and also looks at potential paths for information security reporting and the different advantages and disadvantages of each possibility.

ENABLER: CULTURE, ETHICS & BEHAVIOUR

Examines the culture, ethics and behaviour model from an information security perspective providing detailed security specific examples of:

1. The Culture Life Cycle –measuring behaviours over time to benchmark the security culture –some behaviours may include:
   - Strength of passwords
   - Lack of approach to security
   - Adherence to change management practices

2. Leadership and Champions –need these people to set examples and help influence culture:
   - Risk managers
   - Security professionals
   - C-level executives

3. Desirable Behaviour –a number of behaviours have been identified that will help positively influence security culture:
   - Information security is practiced in daily operations.
   - Stakeholders are aware of how to respond to threats.
   - Executive management recognises the business value of security.

ENABLER: INFORMATION

Information is not only the main subject of information security but is also a key enabler.

1. Information types are examined and reveal types of relevant security information which can include:
    - Information security strategy
    - Information security budget
    - Policies
    - Awareness material
    - Etc.

2. Information stakeholders as well as the information life cycle are also identified and detailed from a security perspective. Details specific to security such as information storage, sharing, use and disposal are all discussed.

ENABLER: SERVICES, INFRASTRUCTURE & APPLICATIONS

The services, infrastructure and applications model identifies the services capabilities that are required to provide information security and related functions to an enterprise. The following list contains examples of potential security-related services that could appear in a security service catalogue:

- Provide a security architecture.
- Provide security awareness.
- Provide security assessments.
- Provide adequate incident response.
- Provide adequate protection against malware, external attacks and intrusion attempts.
- Provide monitoring and alert services for security related events.

ENABLER: PEOPLE, SKILLS & COMPETENCIES

To effectively operate an information security function within an enterprise, individuals with appropriate knowledge and experience must exercise that function. Some typical security-related skills and competencies listed are:

- Information security governance
- Information risk management
- Information security operations

COBIT 5 for Information Security defines the following attributes for each of the skills and competencies:

- Skill definition
- Goals
- Related enablers

IMPLEMENTING INFORMATION SECURITY INITIATIVES

— **GEORGE QUINLAN, CISA**
SENIOR CONSULTANT
CHICAGO, ILLINOIS, USA
ISACA MEMBER SINCE 2005

CONNECT MORE

ISACA®
Trust in, and value from, information systems

IMPLEMENTING INFORMATION SECURITY INITIATIVES

Considering the enterprise information security context: *COBIT 5 for Information Security* advises that every enterprise needs to define and implement its own information security enablers depending on factors within the enterprise's environment such as:

- Ethics and culture relating to information security
- Applicable laws, regulations and policies
- Existing policies and practices
- Information security capabilities and available resources

IMPLEMENTING INFORMATION SECURITY INITIATIVES

Additionally, the enterprise's information security requirements need to be defined based on:

- Business plan and strategic intentions
- Management style
- Information risk profile
- Risk appetite

The approach for implementing information security initiatives will be different for every enterprise and the context needs to be understood to adapt *COBIT 5 for Information Security* effectively.

IMPLEMENTING INFORMATION SECURITY INITIATIVES

Other key areas of importance when implementing *COBIT 5 for Information Security* are:

- Creating the appropriate environment
- Recognising pain points and trigger events
- Enabling change
- Understanding that implementing information security practices is not a one time event but is a life cycle

USING *COBIT 5 FOR INFORMATION SECURITY* TO CONNECT OTHER FRAMEWORKS, MODELS, GOOD PRACTICES AND STANDARDS

— **KATIE STETZ, CISA, CISM, CRISC**
ATO COMPLIANCE ANALYST, RISK MANAGEMENT & COMPLIANCE
CHICAGO, ILLINOIS, USA
ISACA MEMBER SINCE 2005

BE MORE

ISACA®
Trust in, and value from, information systems

USING *COBIT 5 FOR INFORMATION SECURITY* TO CONNECT OTHER FRAMEWORKS, MODELS, GOOD PRACTICES AND STANDARDS

COBIT 5 for Information Security aims to be an umbrella framework to connect to other information security frameworks, good practices and standards.

COBIT 5 for Information Security describes the pervasiveness of information security throughout the enterprise and provides an overarching framework of enablers, but the others can be helpful as well because they may elaborate on specific topics. Examples include:

- Business Model for Information Security (BMIS)–ISACA
- Standard of Good Practice for Information Security (ISF)
- ISO/IEC 27000 Series
- NIST SP 800-53a
- PCI-DSS

QUESTIONS ?

— **NATHAN ANDERSON, CISA, CRISC**
INTERNAL AUDIT DIRECTOR
CHICAGO, ILLINOIS, USA
ISACA MEMBER SINCE 2010

MORE | **CAPABLE**

ISACA®
Trust in, and value from, information systems