COBIT 5
Information Security

Industry Trends

One small step for man...

"In 1969 NASA launched a man to the moon"

"In 2012 Launching unhappy birds into pigs"

Everything Connected

Life vest

Oxygen tank

New method

Crowding Out

Crowdsourcing Value = Mass Collaboration

Mobile is Dead (Long Live Mobile)

termination of email….

Facebook has more than 600 million active users

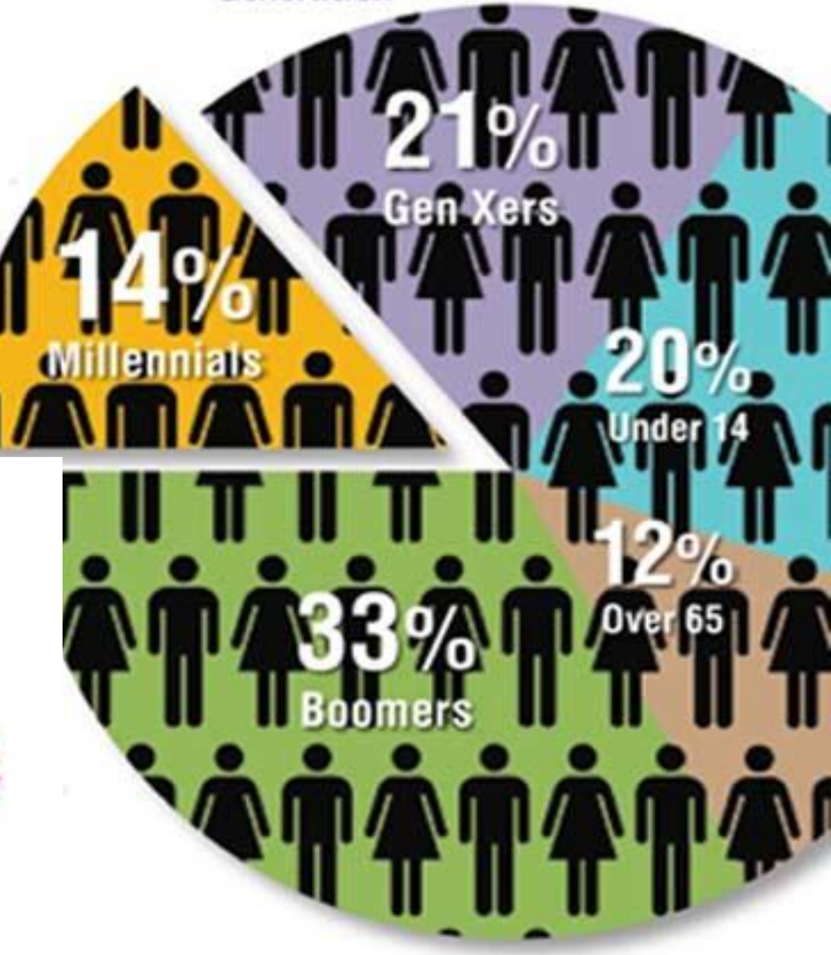
Twitter has 200 million users, generating 65 million tweets a day

LinkedIn has more than 100 million registered users, spanning more than 200 countries

"Social media has played a crucial role in the unrest in Egypt, with many of the protests organized through Facebook."
— BBC News

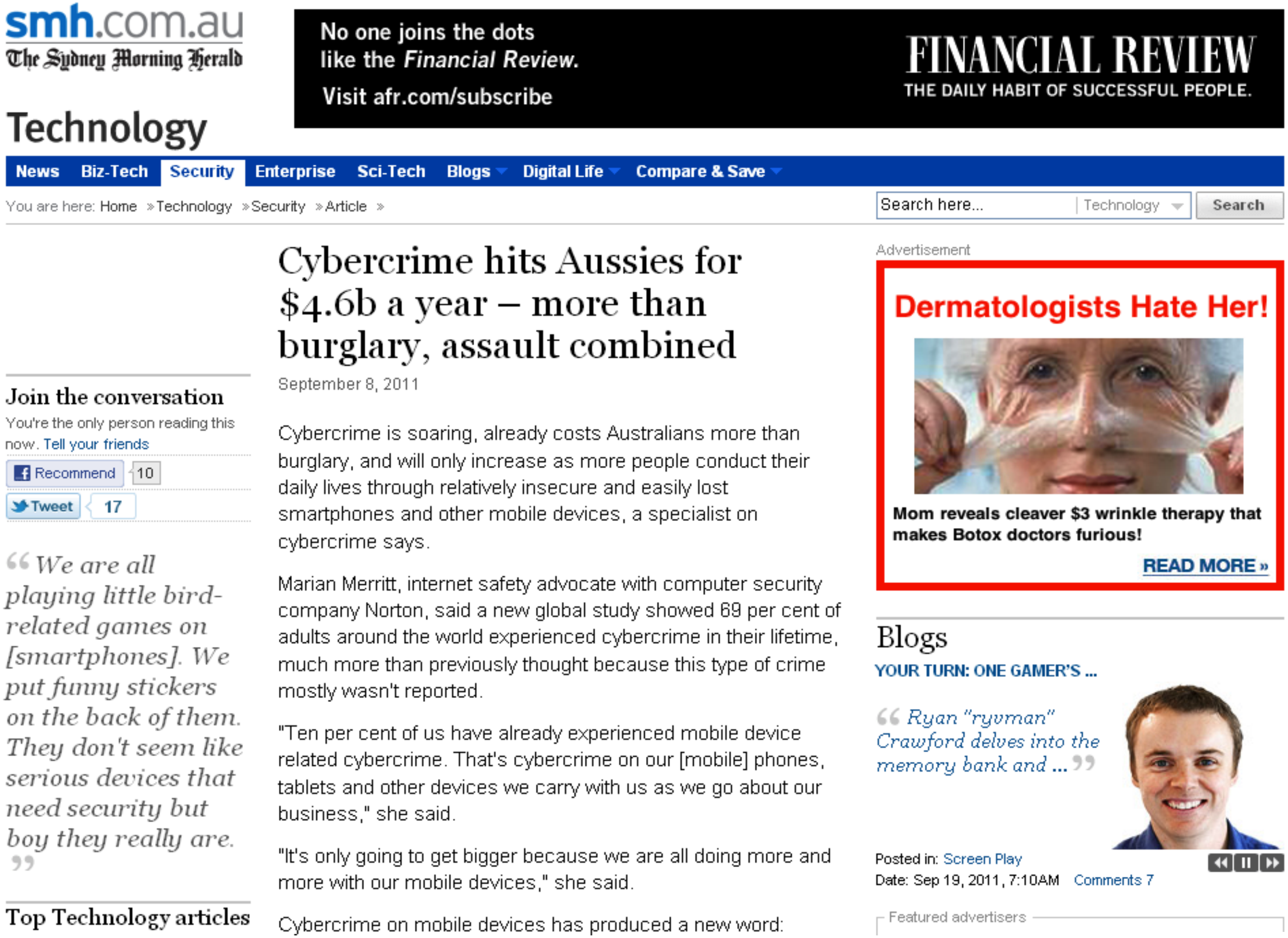
Generational differences

Population Breakdown by Generation



Source: Population Division, U.S. Census Bureau. Data released May 2007.

“cybercrime”



smh.com.au
The Sydney Morning Herald

Technology

Cybercrime hits Aussies for $4.6b a year – more than burglary, assault combined

September 8, 2011

Cybercrime is soaring, already costs Australians more than burglary, and will only increase as more people conduct their daily lives through relatively insecure and easily lost smartphones and other mobile devices, a specialist on cybercrime says.

Marian Merritt, internet safety advocate with computer security company Norton, said a new global study showed 69 per cent of adults around the world experienced cybercrime in their lifetime, much more than previously thought because this type of crime mostly wasn't reported.

"Ten per cent of us have already experienced mobile device related cybercrime. That's cybercrime on our [mobile] phones, tablets and other devices we carry with us as we go about our business," she said.

"It's only going to get bigger because we are all doing more and more with our mobile devices," she said.

Cybercrime on mobile devices has produced a new word:

Join the conversation

You're the only person reading this now. Tell your friends

> “We are all playing little bird-related games on [smartphones]. We put funny stickers on the back of them. They don't seem like serious devices that need security but boy they really are.”

Top Technology articles

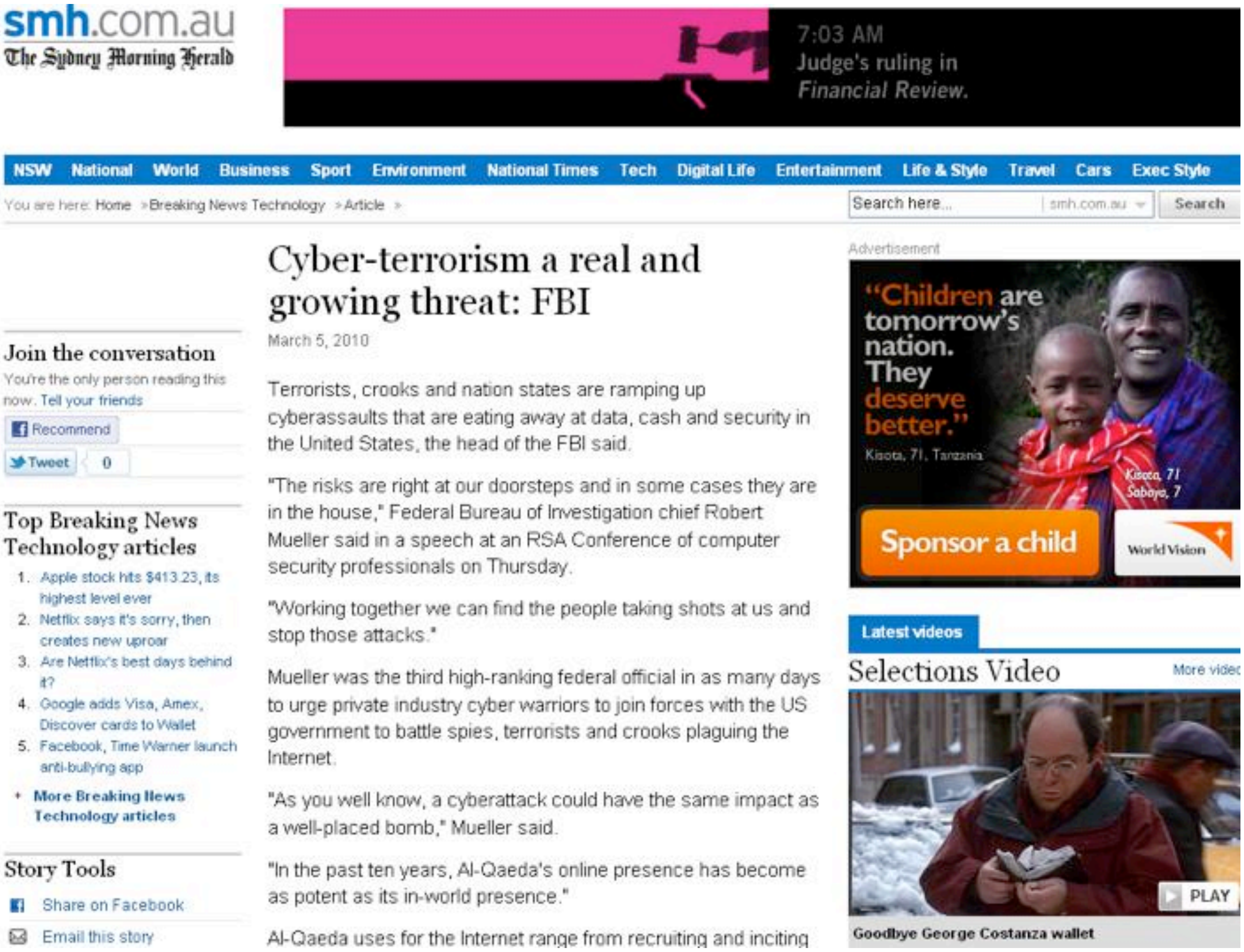
Blogs

YOUR TURN: ONE GAMER'S ...

“Ryan "ryvman" Crawford delves into the memory bank and ...”

Posted in: Screen Play
Date: Sep 19, 2011, 7:10AM Comments 7

"cyber terrorism"



smh.com.au
The Sydney Morning Herald

NSW National World Business Sport Environment National Times Tech Digital Life Entertainment Life & Style Travel Cars Exec Style
You are here: Home » Breaking News Technology » Article »
Search here... smh.com.au Search

Cyber-terrorism a real and growing threat: FBI

March 5, 2010

Terrorists, crooks and nation states are ramping up cyberassaults that are eating away at data, cash and security in the United States, the head of the FBI said.

"The risks are right at our doorsteps and in some cases they are in the house," Federal Bureau of Investigation chief Robert Mueller said in a speech at an RSA Conference of computer security professionals on Thursday.

"Working together we can find the people taking shots at us and stop those attacks."

Mueller was the third high-ranking federal official in as many days to urge private industry cyber warriors to join forces with the US government to battle spies, terrorists and crooks plaguing the Internet.

"As you well know, a cyberattack could have the same impact as a well-placed bomb," Mueller said.

"In the past ten years, Al-Qaeda's online presence has become as potent as its in-world presence."

Al-Qaeda uses for the Internet range from recruiting and inciting

Join the conversation

You're the only person reading this now. Tell your friends

Top Breaking News Technology articles

1. Apple stock hits $413.23, its highest level ever
2. Netflix says it's sorry, then creates new uproar
3. Are Netflix's best days behind it?
4. Google adds Visa, Amex, Discover cards to Wallet
5. Facebook, Time Warner launch anti-bullying app

- More Breaking News Technology articles

Story Tools

Latest videos

Selections Video

Goodbye George Costanza wallet

Sydney Morning Herald – March 5, 2011

COBIT 5: Information Security

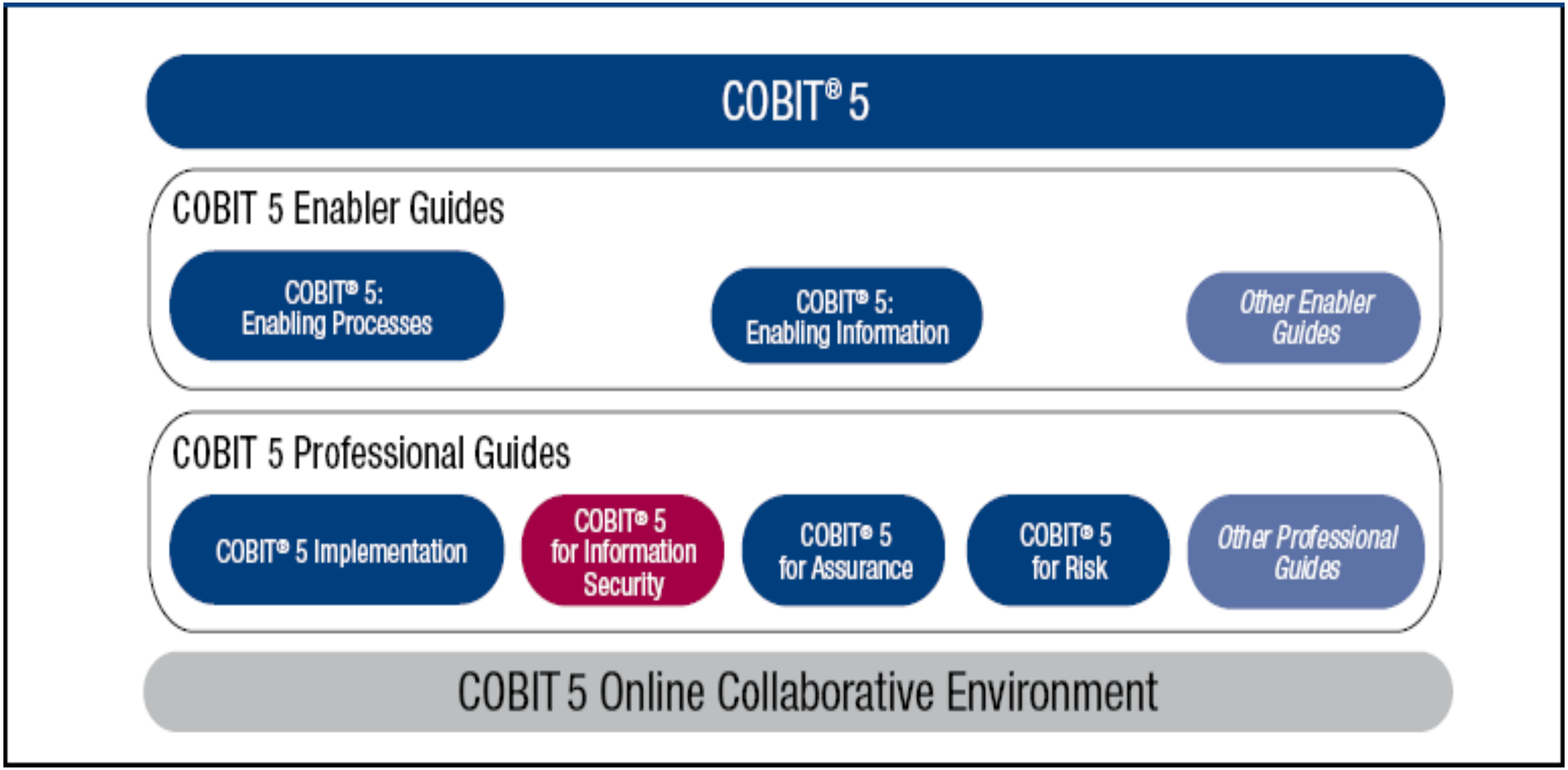
How much security is enough?

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?

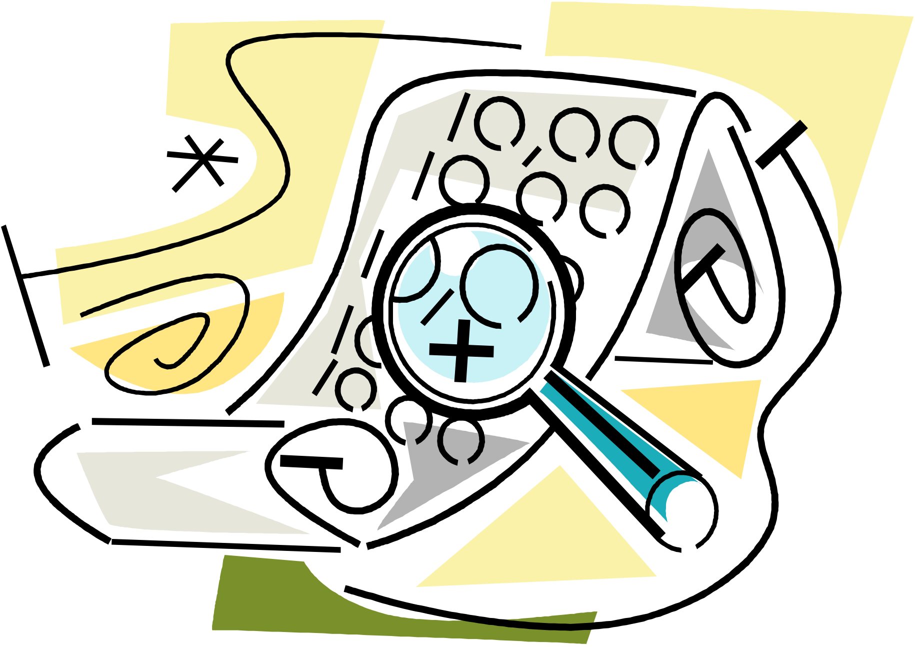
COBIT 5 Product Family


COBIT® 5
COBIT 5 Enabler Guides
COBIT® 5: Enabling Processes
COBIT® 5: Enabling Information
Other Enabler Guides
COBIT 5 Professional Guides
COBIT® 5 Implementation
COBIT® 5 for Information Security
COBIT® 5 for Assurance
COBIT® 5 for Risk
Other Professional Guides
COBIT 5 Online Collaborative Environment

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

COBIT 5 for Information Security

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



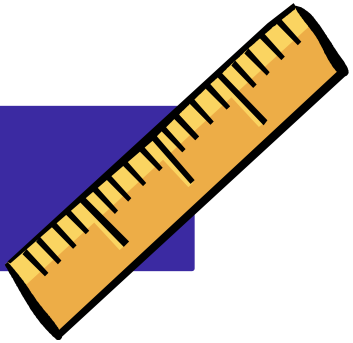
What does COBIT for Information Security contain?

Guidance on drivers, benefits

Principles from infosec perspective

Enablers for support

Alignment with standards



Drivers

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

Benefits

- 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

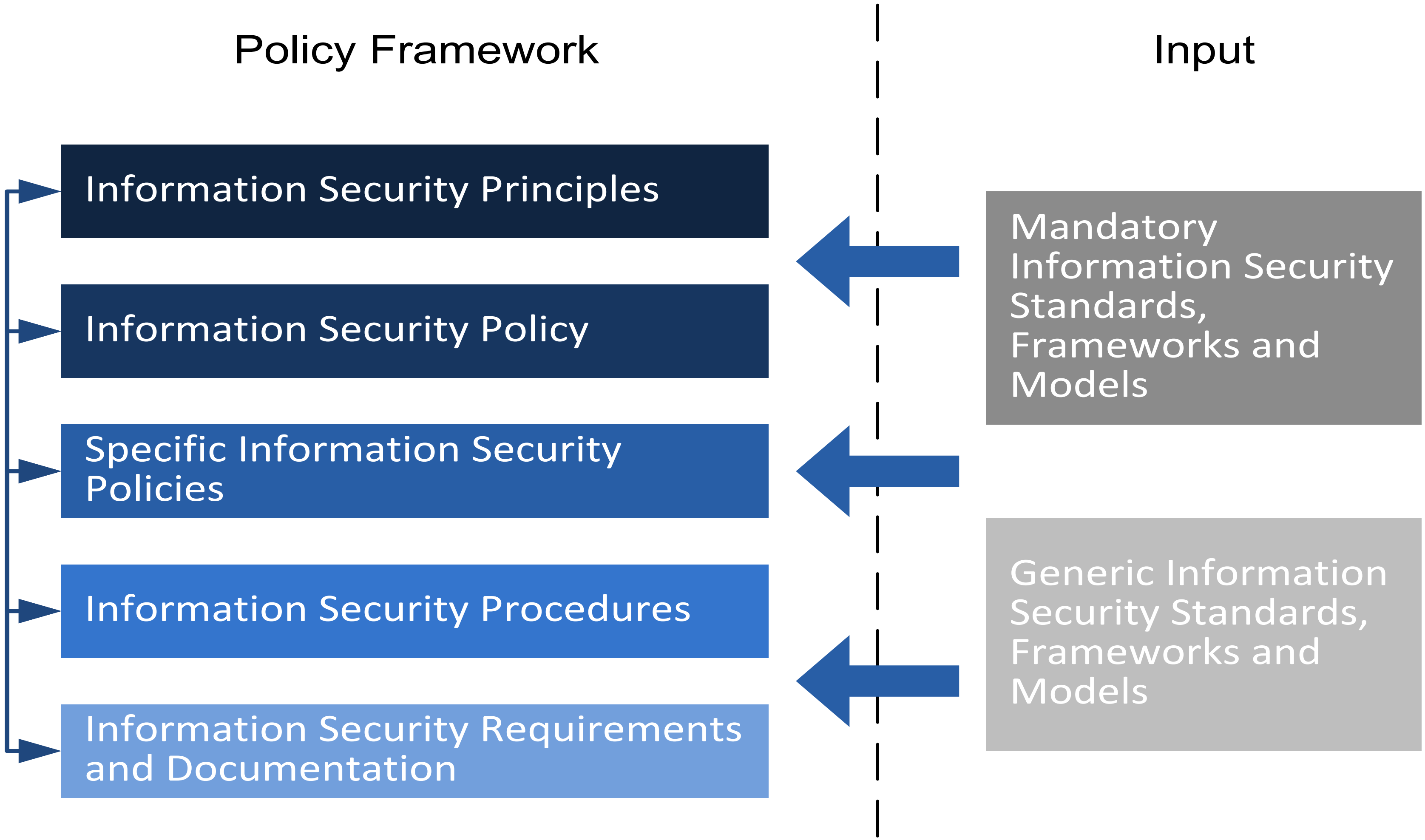
1. Information security **policies, principles, and frameworks**
2. **Processes,** including information security-specific details and activities
3. Information security-specific **organisational structures**
4. In terms of **culture, ethics and behaviour**, factors determining the success of information 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

Enabler: Principles, Policies & Frameworks

Principles, policies and frameworks refer to the communication mechanisms put in place to convey the direction and instructions of the governing bodies and management, including:

- Principles, policies and framework model
- Information security principles
- Information security policies
- Adapting policies to the enterprises environment
- Policy life cycle

Enabler: Principles, Policies & Frameworks



Policy Framework

Input

Information Security Principles

Information Security Policy

Specific Information Security Policies

Information Security Procedures

Information Security Requirements and Documentation

Mandatory Information Security Standards, Frameworks and Models

Generic Information Security Standards, Frameworks and Models

Source: *COBIT 5 for Information Security,* figure 10. © 2012 ISACA® All rights reserved

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*

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:

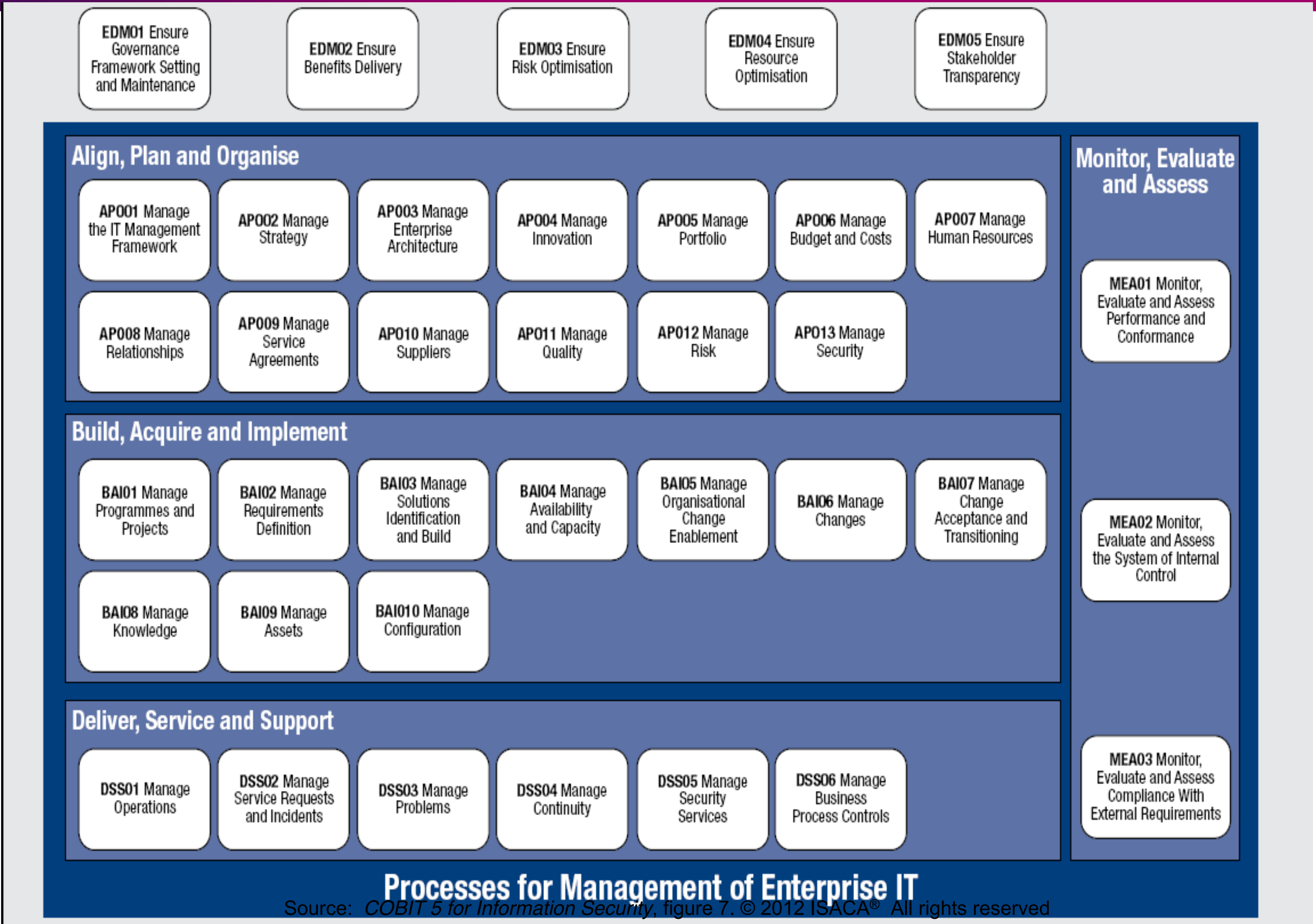
- Scope
- Validity
- Goals

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.)


EDM01 Ensure Governance Framework Setting and Maintenance
EDM02 Ensure Benefits Delivery
EDM03 Ensure Risk Optimisation
EDM04 Ensure Resource Optimisation
EDM05 Ensure Stakeholder Transparency
Align, Plan and Organise
APO01 Manage the IT Management Framework
APO02 Manage Strategy
APO03 Manage Enterprise Architecture
APO04 Manage Innovation
APO05 Manage Portfolio
APO06 Manage Budget and Costs
APO07 Manage Human Resources
APO08 Manage Relationships
APO09 Manage Service Agreements
APO10 Manage Suppliers
APO11 Manage Quality
APO12 Manage Risk
APO13 Manage Security
Build, Acquire and Implement
BAI01 Manage Programmes and Projects
BAI02 Manage Requirements Definition
BAI03 Manage Solutions Identification and Build
BAI04 Manage Availability and Capacity
BAI05 Manage Organisational Change Enablement
BAI06 Manage Changes
BAI07 Manage Change Acceptance and Transitioning
BAI08 Manage Knowledge
BAI09 Manage Assets
BAI010 Manage Configuration
Deliver, Service and Support
DSS01 Manage Operations
DSS02 Manage Service Requests and Incidents
DSS03 Manage Problems
DSS04 Manage Continuity
DSS05 Manage Security Services
DSS06 Manage Business Process Controls
Monitor, Evaluate and Assess
MEA01 Monitor, Evaluate and Assess Performance and Conformance
MEA02 Monitor, Evaluate and Assess the System of Internal Control
MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
Processes for Management of Enterprise IT

Source: *COBIT 5 for Information Security*, figure 7. © 2012 ISACA® All rights reserved

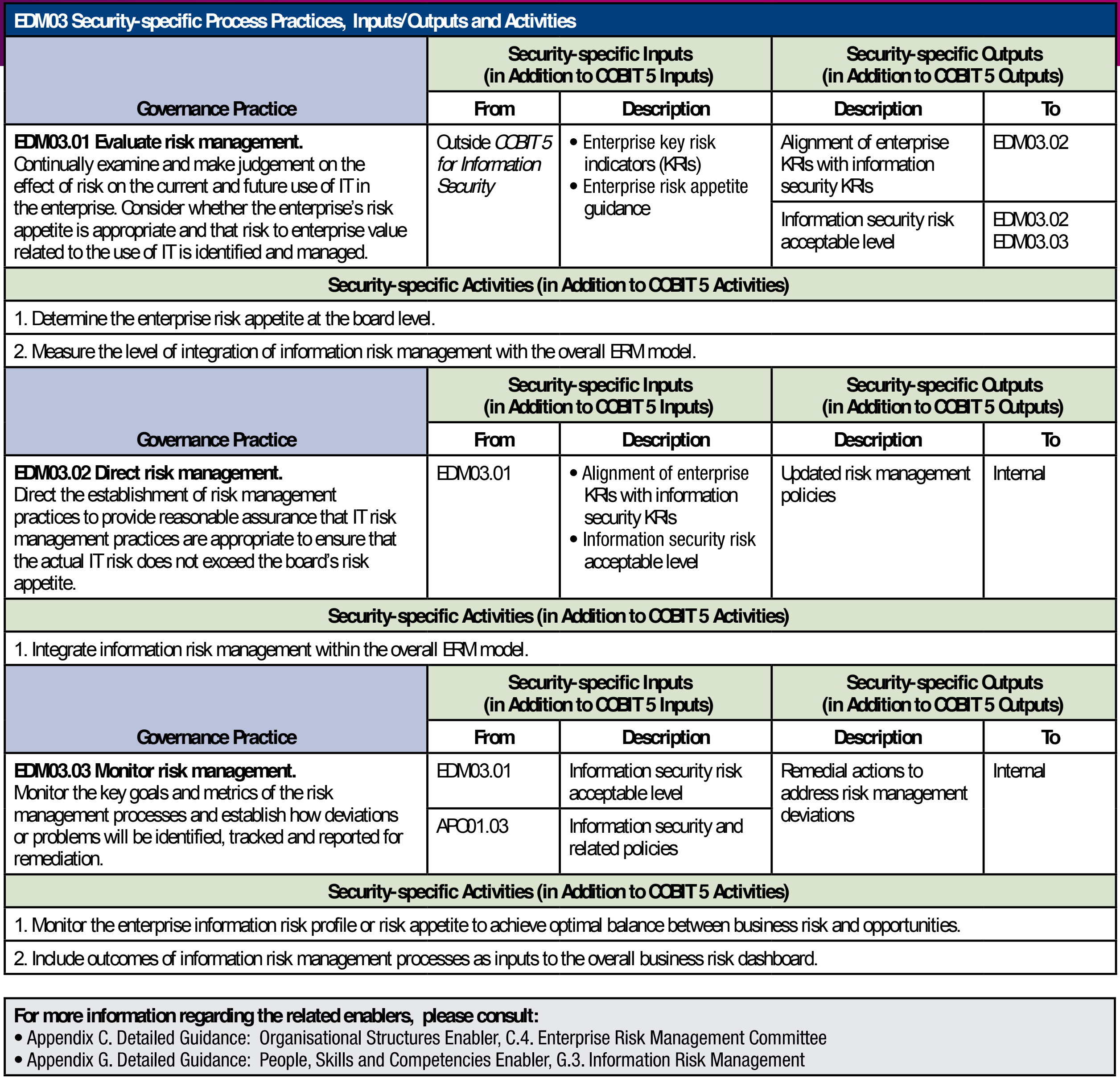
INSERT THE FOLLOWING GRAPHICS FROM APPENDIX B

- EDM03 – PAGE 75
- APO 13 MANAGE SECURITY PAGE 113 AND 114
- BAI 06 MANAGE CHANGE 131 AND 132
- DSS05 MANAGE SECURITY SERVICES 151 AND 152

Appendix B – EDM03 Ensure Risk Optomisation

<table>
<tr><th>EDM03 Ensure Risk Optimisation</th><th>Area: Governance
Domain: Evaluate, Direct and Monitor</th></tr>
<tr><td colspan="2"><b>COBIT 5 Process Description</b>
Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed.</td></tr>
<tr><td colspan="2"><b>COBIT 5 Process Purpose Statement</b>
Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.</td></tr>
<tr><td colspan="2"><b>EDM03 Security-specific Process Goals and Metrics</b></td></tr>
<tr><td><b>Security-specific Process Goals</b></td><td><b>Related Metrics</b></td></tr>
<tr><td>1. Information risk management is part of overall enterprise risk management (ERM).</td><td>• Percent of information security risk that is related to business risk
• Percent of business risk that has been effectively mitigated with information security controls</td></tr>
</table>

Appendix B – EDM03 Ensure Risk Optomisation



EDM03 Security-specific Process Practices, Inputs/Outputs and Activities

Governance Practice	Security-specific Inputs (in Addition to COBIT 5 Inputs)		Security-specific Outputs (in Addition to COBIT 5 Outputs)	
	From	**Description**	**Description**	**To**
EDM03.01 Evaluate risk management. Continually examine and make judgement on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risk to enterprise value related to the use of IT is identified and managed.	Outside *COBIT 5 for Information Security*	• Enterprise key risk indicators (KRIs) • Enterprise risk appetite guidance	Alignment of enterprise KRIs with information security KRIs	EDM03.02
			Information security risk acceptable level	EDM03.02 EDM03.03

Security-specific Activities (in Addition to COBIT 5 Activities)

1. Determine the enterprise risk appetite at the board level.

2. Measure the level of integration of information risk management with the overall ERM model.

Governance Practice	Security-specific Inputs (in Addition to COBIT 5 Inputs)		Security-specific Outputs (in Addition to COBIT 5 Outputs)	
	From	**Description**	**Description**	**To**
EDM03.02 Direct risk management. Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite.	EDM03.01	• Alignment of enterprise KRIs with information security KRIs • Information security risk acceptable level	Updated risk management policies	Internal

Security-specific Activities (in Addition to COBIT 5 Activities)

1. Integrate information risk management within the overall ERM model.

Governance Practice	Security-specific Inputs (in Addition to COBIT 5 Inputs)		Security-specific Outputs (in Addition to COBIT 5 Outputs)	
	From	**Description**	**Description**	**To**
EDM03.03 Monitor risk management. Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported for remediation.	EDM03.01	Information security risk acceptable level	Remedial actions to address risk management deviations	Internal
	APO01.03	Information security and related policies		

Security-specific Activities (in Addition to COBIT 5 Activities)

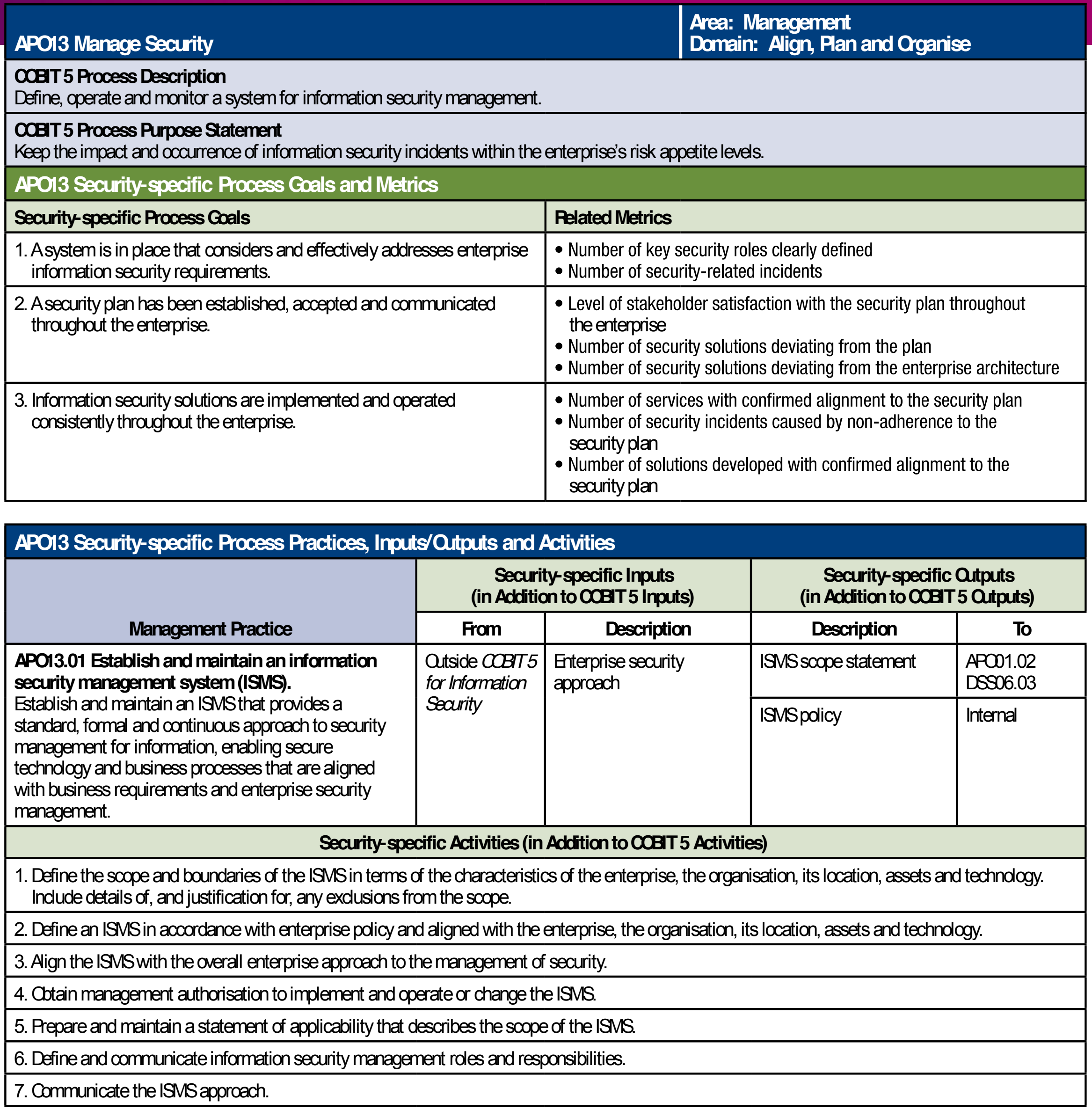
1. Monitor the enterprise information risk profile or risk appetite to achieve optimal balance between business risk and opportunities.

2. Include outcomes of information risk management processes as inputs to the overall business risk dashboard.

For more information regarding the related enablers, please consult:
- Appendix C. Detailed Guidance: Organisational Structures Enabler, C.4. Enterprise Risk Management Committee
- Appendix G. Detailed Guidance: People, Skills and Competencies Enabler, G.3. Information Risk Management

Page 75 – COBIT for Information Security

Appendix B – APO 13 MANAGE SECURITY



APO13 Manage Security	Area: Management Domain: Align, Plan and Organise

COBIT 5 Process Description
Define, operate and monitor a system for information security management.

COBIT 5 Process Purpose Statement
Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.

APO13 Security-specific Process Goals and Metrics

Security-specific Process Goals	Related Metrics
1. A system is in place that considers and effectively addresses enterprise information security requirements.	• Number of key security roles clearly defined • Number of security-related incidents
2. A security plan has been established, accepted and communicated throughout the enterprise.	• Level of stakeholder satisfaction with the security plan throughout the enterprise • Number of security solutions deviating from the plan • Number of security solutions deviating from the enterprise architecture
3. Information security solutions are implemented and operated consistently throughout the enterprise.	• Number of services with confirmed alignment to the security plan • Number of security incidents caused by non-adherence to the security plan • Number of solutions developed with confirmed alignment to the security plan

APO13 Security-specific Process Practices, Inputs/Outputs and Activities

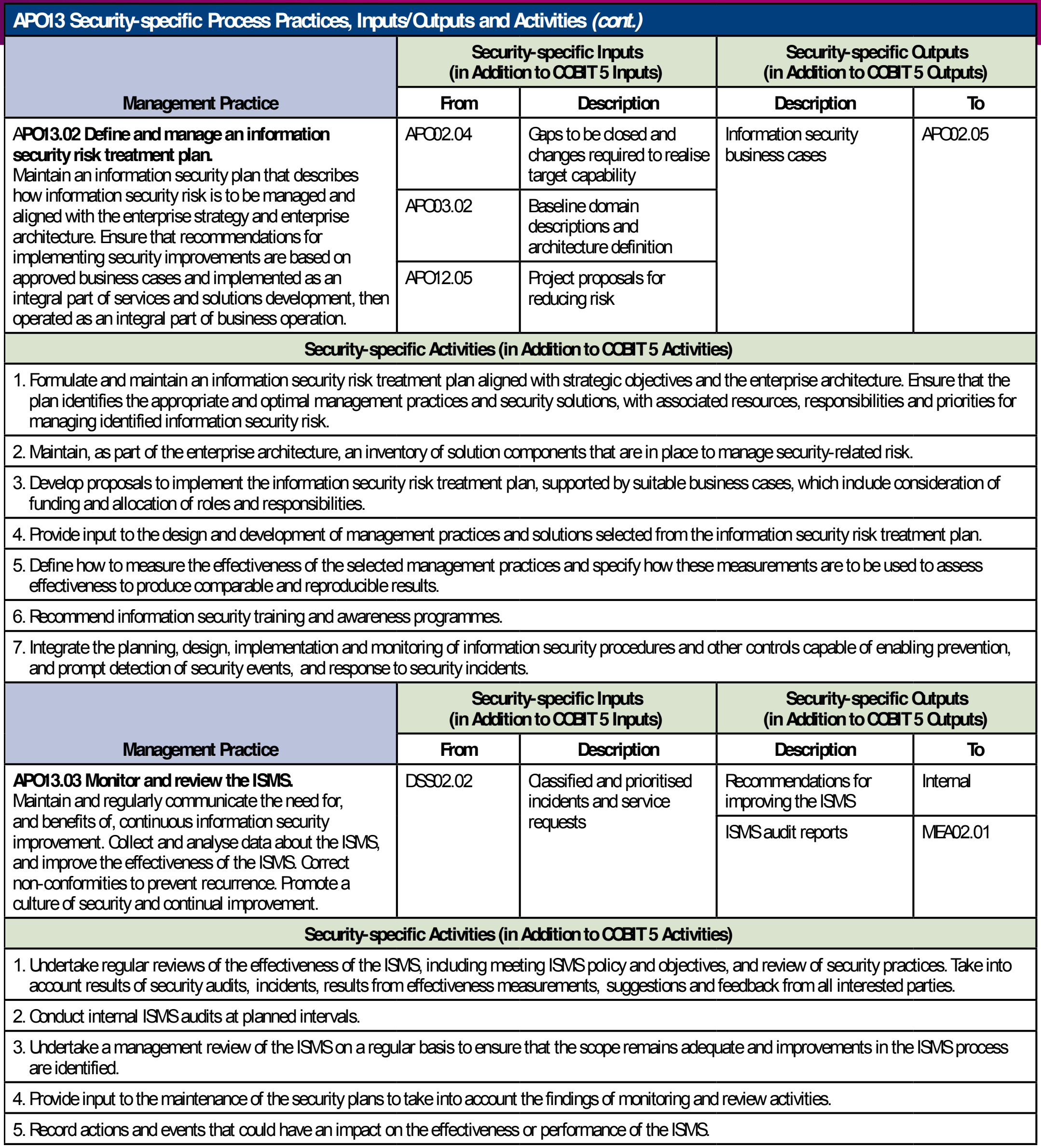
	Security-specific Inputs (in Addition to COBIT 5 Inputs)		Security-specific Outputs (in Addition to COBIT 5 Outputs)	
Management Practice	From	Description	Description	To
APO13.01 Establish and maintain an information security management system (ISMS). Establish and maintain an ISMS that provides a standard, formal and continuous approach to security management for information, enabling secure technology and business processes that are aligned with business requirements and enterprise security management.	Outside *COBIT 5 for Information Security*	Enterprise security approach	ISMS scope statement	APO01.02 DSS06.03
			ISMS policy	Internal

Security-specific Activities (in Addition to COBIT 5 Activities)

1. Define the scope and boundaries of the ISMS in terms of the characteristics of the enterprise, the organisation, its location, assets and technology. Include details of, and justification for, any exclusions from the scope.
2. Define an ISMS in accordance with enterprise policy and aligned with the enterprise, the organisation, its location, assets and technology.
3. Align the ISMS with the overall enterprise approach to the management of security.
4. Obtain management authorisation to implement and operate or change the ISMS.
5. Prepare and maintain a statement of applicability that describes the scope of the ISMS.
6. Define and communicate information security management roles and responsibilities.
7. Communicate the ISMS approach.

COBIT for Information Security - APO 13 MANAGE SECURITY PAGE 113

Appendix B – APO 13 MANAGE SECURITY



APO13 Security-specific Process Practices, Inputs/Outputs and Activities *(cont.)*

	Security-specific Inputs (in Addition to COBIT 5 Inputs)		Security-specific Outputs (in Addition to COBIT 5 Outputs)	
Management Practice	**From**	**Description**	**Description**	**To**
APO13.02 Define and manage an information security risk treatment plan. Maintain an information security plan that describes how information security risk is to be managed and aligned with the enterprise strategy and enterprise architecture. Ensure that recommendations for implementing security improvements are based on approved business cases and implemented as an integral part of services and solutions development, then operated as an integral part of business operation.	APO02.04	Gaps to be closed and changes required to realise target capability	Information security business cases	APO02.05
	APO03.02	Baseline domain descriptions and architecture definition		
	APO12.05	Project proposals for reducing risk		

Security-specific Activities (in Addition to COBIT 5 Activities)

1. Formulate and maintain an information security risk treatment plan aligned with strategic objectives and the enterprise architecture. Ensure that the plan identifies the appropriate and optimal management practices and security solutions, with associated resources, responsibilities and priorities for managing identified information security risk.
2. Maintain, as part of the enterprise architecture, an inventory of solution components that are in place to manage security-related risk.
3. Develop proposals to implement the information security risk treatment plan, supported by suitable business cases, which include consideration of funding and allocation of roles and responsibilities.
4. Provide input to the design and development of management practices and solutions selected from the information security risk treatment plan.
5. Define how to measure the effectiveness of the selected management practices and specify how these measurements are to be used to assess effectiveness to produce comparable and reproducible results.
6. Recommend information security training and awareness programmes.
7. Integrate the planning, design, implementation and monitoring of information security procedures and other controls capable of enabling prevention, and prompt detection of security events, and response to security incidents.

	Security-specific Inputs (in Addition to COBIT 5 Inputs)		Security-specific Outputs (in Addition to COBIT 5 Outputs)	
Management Practice	**From**	**Description**	**Description**	**To**
APO13.03 Monitor and review the ISMS. Maintain and regularly communicate the need for, and benefits of, continuous information security improvement. Collect and analyse data about the ISMS, and improve the effectiveness of the ISMS. Correct non-conformities to prevent recurrence. Promote a culture of security and continual improvement.	DSS02.02	Classified and prioritised incidents and service requests	Recommendations for improving the ISMS	Internal
			ISMS audit reports	MEA02.01

Security-specific Activities (in Addition to COBIT 5 Activities)

1. Undertake regular reviews of the effectiveness of the ISMS, including meeting ISMS policy and objectives, and review of security practices. Take into account results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties.
2. Conduct internal ISMS audits at planned intervals.
3. Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified.
4. Provide input to the maintenance of the security plans to take into account the findings of monitoring and review activities.
5. Record actions and events that could have an impact on the effectiveness or performance of the ISMS.

COBIT for Information Security - APO 13 MANAGE SECURITY PAGE 114

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 and 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 and 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 and 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

Chapter 2: 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

Chapter 2: Implementing Information Security Initiatives (cont.)

- 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.

Chapter 2: Implementing Information Security Initiatives (cont.)

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

Chapter 3: Using *COBIT 5 for Information Security* to Connect Other Frameworks, Models, Practices & 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

Appendix C – Detailed organisational structure

C.1 Chief Information Security Officer

Mandate, Operating Principles, Span of Control and Authority Level

Figure 25 lists the characteristics of the CISO.

Figure 25—CISO: Mandate, Operating Principles, Span of Control and Authority Level

Area	Characteristic
Mandate	The overall responsibility of the enterprise information security programme
Operating principles	Depending on a variety factors within the enterprise, the CISO may report to the CEO, COO, CIO, CRO or other senior executive management. The CISO is the liaison between executive management and the information security programme. The CISO should also communicate and co-ordinate closely with key business stakeholders to address information protection needs. The CISO must: • Have an accurate understanding of the business strategic vision • Be an effective communicator • Be adept at building effective relationships with business leaders • Be able to translate business objectives into information security requirements
Span of control	The CISO is responsible for: • Establishing and maintaining an information security management system (ISMS) • Defining and managing an information security risk treatment plan • Monitoring and reviewing the ISMS
Authority level/decision rights	The CISO is responsible for implementing and maintaining the information security strategy. Accountability (and sign-off of important decisions) resides in the function to which the CISO reports, for example, senior executive management team member or the ISSC.
Delegation rights	The CISO should delegate tasks to information security managers and business people.
Escalation path	The CISO should escalate key information risk-related issues to his/her direct supervisor and/or the ISSC.

for Information Security

COBIT® 5
AN ISACA® FRAMEWORK

ca technologies

COBIT 5
Information Security

technologies