

Webinar Handbook

ISACA's Guide to COBIT 5 for Information Security

Premium Webinar

ISACA's Guide to COBIT 5 for Information Security

Presented by:

Christos Dimitriadis

VP

ISACA International

Robert Stroud

VP – Strategy & Innovation & ISACA Strategic Advisory Board Member

CA Technologies

From headline-making data breaches to hacktivist attacks, there never have been so many high-profile incidents, which in turn have sparked greater public awareness of information security risks.



Tom Field

Now, more than ever, regulators, board members and even customers are asking smart questions about information security, fraud and compliance. You need to be prepared to give them informed answers.

At Information Security Media Group, we've assembled a broad suite of webinar training programs aimed at giving you the latest information you need about the ever-changing threat, compliance and technology landscape. Among the benefits:

Relevant Topics – From mobile security to fraud prevention and how to conduct an effective risk assessment, we continue to produce new sessions that reflect today's top priorities.

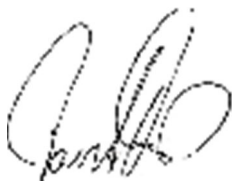
Experienced Faculty – For our virtual faculty, we draw upon industry thought-leaders, top consultants, current industry/security leaders, even federal regulators.

Convenience – You don't need to travel off-site or even to a conference room to experience our programs. They are delivered straight to your desktop.

The ROI on our training programs is three-fold:

1. Cost-effective access to education that will help you in your job today;
2. Access to world-class leaders in our virtual faculty;
3. Ability, through our Membership Program, to gain on-demand access to our training library.

Please check out our latest catalog, and be sure to offer your own suggestions for new course offerings.



Tom Field,
Vice President, Editorial
Information Security Media Group



Table of Contents

Section 1

- Workshop Overview & Background

Section 2

- The Presenter(s)

Section 3

- Workshop Handouts (slides)

Section 4

- Reference Material (if applicable)



Workshop Overview and Background

Quick Overview of Presentation:

ISACA, the global IT association, recently released COBIT 5 for Information Security - new guidance aimed at helping security leaders use the COBIT framework to reduce their risk profile and add value to their organizations. Join two ISACA leaders for an insider's look at how to use COBIT 5 for Information Security to:

- Link information security with organizational strategic goals;
- Create the appropriate governance and management framework;
- Comply with the ever-growing number of relevant laws, regulations and contractual requirements.

Background

Information is the currency of the 21st century enterprise. As such, effectively securing information is critical. To help enterprises with this challenging mission, global IT association ISACA has developed COBIT 5 for Information Security, which builds upon COBIT 5. COBIT is used by enterprises in all industries and all geographies to create trust in and value from information systems.

Among the major drivers for the development of COBIT 5 for Information Security:

- The need to describe information security in an enterprise context, including all aspects that lead to effective governance and management of information security, such as organizational structures, policies and culture.
- An ever-increasing need for the enterprise to maintain information risk at an acceptable (and regulatory compliant) level and to protect information against unauthorized disclosure, unauthorized or inadvertent modifications, and possible intrusions - all while containing the cost of IT services and technology protection.
- The need to link together all major ISACA research, frameworks and guidance, with a primary focus on Business Management for Information Security (BMIS) and COBIT.

COBIT 5 for Information Security is designed for all stakeholders of information security, from the business to IT. Leading this session are two ISACA executives, Christos K. Dimitriadis, International Vice President, and Robert E Stroud, member of the ISACA Strategic Advisory Council. They will share insights on how to use this new guidance to:

- View information security as a business enabler as well as a risk management tool;
- Ensure effective governance by combining several different standards and good practices under a common framework, avoiding overlaps and additional complexity and cost; Understand and assess the relation between information security and corporate culture;
- Ensure that services and systems are continuously available to internal and external stakeholders.

The Presenters

Robert Stroud



*VP – Strategy & Innovation, CA Technologies
Member – ISACA Strategic Advisory Council*

Stroud served a four-year term as an ISACA international vice president and now serves on the ISACA Strategic Advisory Council and is chair of the ISO Liaison Taskforce. Stroud formerly served on the itSMF International Board as treasurer and director of Audit, Standards and Compliance, the itSMF ISO liaisons to multiple working groups. He is a social media leader, author, blogger and highly regarded public speaker. As an industry veteran, Stroud has significant practical industry experience and is a recognized industry thought leader and has contributed as a global authority on governance to multiple publications, including COBIT 4.0, 4.1 and COBIT 5, Guidance for Basel II and multiple ISO standards.



*VP
ISACA International*

Dimitriadis is the head of information security at INTRALOT GROUP, a Greece-based multinational supplier of integrated gaming and transaction processing systems, where he manages information security in more than 50 countries in all continents. He has worked in information security for more than 12 years and has authored 80 security-related publications. He has provided information security services to the International Telecommunication Union, European Commission Directorate Generals, European Ministries and international organizations, as well as business consulting services to entrepreneurial companies. He is chair of ISACA's COBIT Security Task Force and has served as chair of ISACA's External Relations Committee and member of the Relations Board, Academic Relations Committee, ISACA Journal Editorial Committee and Business Model for Information Security Work Group.

ISACA's Guide to COBIT 5 for Information Security

Presented by

Christos K. Dimitriadis, CISA, CISM, CRISC
Head of Security, INTRALOT Group (Greece)
International Vice President, ISACA

Robert E. Stroud, CGEIT, CRISC
Vice President, CA Technologies (USA)
Member, ISACA Strategic Advisory Council



About Information Security Media Group

- Creators of BankInfoSecurity, CUInfoSecurity, GovInfoSecurity, HealthcareInfoSecurity, InfoRiskToday, CareersInfoSecurity & DataBreachToday
- Unique sites in UK, EU, India and Asia
- Focused on providing content about information security specifically for unique vertical industries
- Publish new articles, interviews, blogs, regulation/guidance alerts, white papers, daily
- Educational webinars offered daily



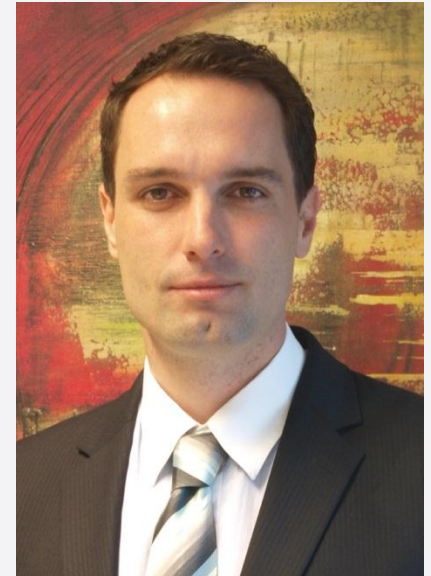
Housekeeping

- Technical Support - (609) 356-1499 x110 or x115
- Copyrighted Material
 - Used for individual study purposes only. If your institution is interested in using this or any of Information Security Media Group's presentations as part of an overall information security program, please contact us at (800) 944-0401.



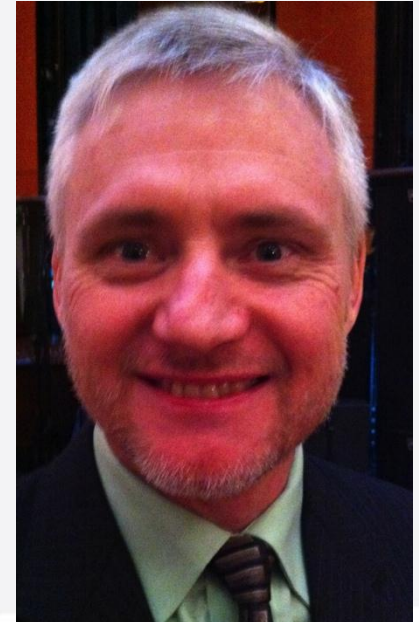
Christos K. Dimitriadis, CISM, CISA, CRISC

- ISACA International Vice President
- Head Information Security, INTRALOT Group
- Chair of COBIT 5 for Information Security Task Force
- 12 years of experience in Information Security
- Member of ENISA Permanent Stakeholder Group
- PhD in Information Security
- Over 100 Publications in the field



Robert E Stroud CRISC CGEIT

- Vice President Strategy & Innovation, CA Technologies
- Past International Vice President ISACA
- ISACA Strategic Advisory Council
- Chair ISACA ISO Liaison Subcommittee
- 15 years Banking Experience
- Contributor COBIT, VALIT and RISK IT
- Author, Public Speaker & Industry Geek
- @robertestroud



Agenda

- COBIT 5 Introduction and scope
- COBIT 5 for Information Security
- Conclusions, More Information & Discussion

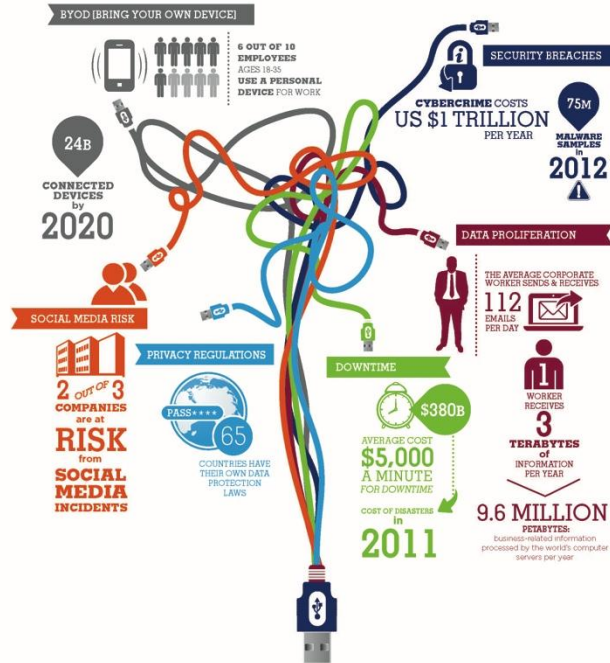


COBIT 5

Introduction & Scope

EXTRACTING VALUE FROM INFORMATION CHAOS

WHY GOOD GOVERNANCE MAKES GOOD SENSE



BUSINESS GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

Download a complimentary copy of COBIT 5 today or learn more at www.isaca.org/cobit

COBIT[®] 5
AN ISACA[®] FRAMEWORK

SOURCES

- <http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/ISACA-Survey-Bring-Your-Own-Device-Trend-Highlights-Cyber-Holiday-Shopping-Risk.aspx>
- <http://www.gartner.com/Articles/ID146466.aspx>
- <http://www.legal.mcafee.com/mcafee-66-the-able-report-shows-malware-surpassed-75-million-samples-in-2011>
- <http://www.mcafee.com/766004>
- <http://www.dnews.uscd.edu/news/04-08/08newsinfomation.asp>
- http://www.informationweek.com/Default.aspx?Community_Management_Development/231603279
- <http://www.isaca.org/Am/Development/Issues/News/Access/Cybersecurity-Domestic-Global-Approach.html>
- <http://www.crafo.com/privacy-44-security-44/>
- <http://www.ft.com/news/world/article/0,8599,300354,00.html>
- <http://www.zdnet.com/4/4/IT/withstructure/Topline-IT-Downtime-Cost-Cost-Per-Minute-Report-548007/>

Enterprise Benefits

Enterprises and their executives strive to:

- Maintain quality information
- Generate business value from IT-enabled investments
- Achieve operational excellence through reliable, efficient application of technology
- Maintain IT-related risk at an acceptable level
- Optimise the cost of IT services and technology

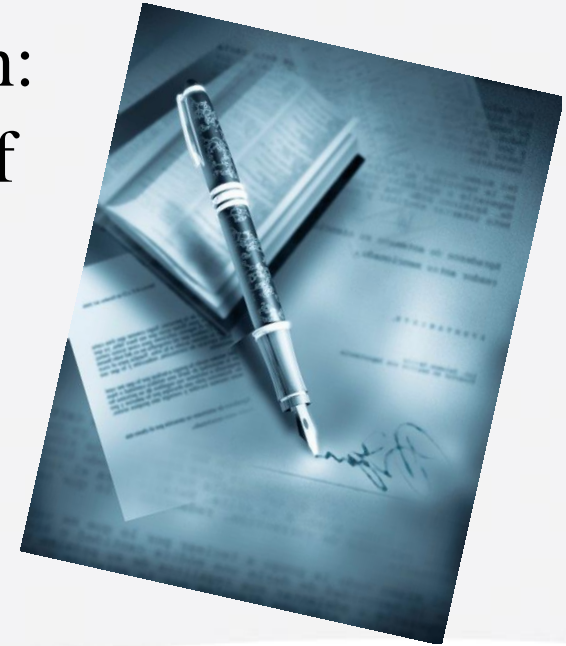


How can these benefits be realized to create value to the enterprise stakeholder?

Stakeholder Value

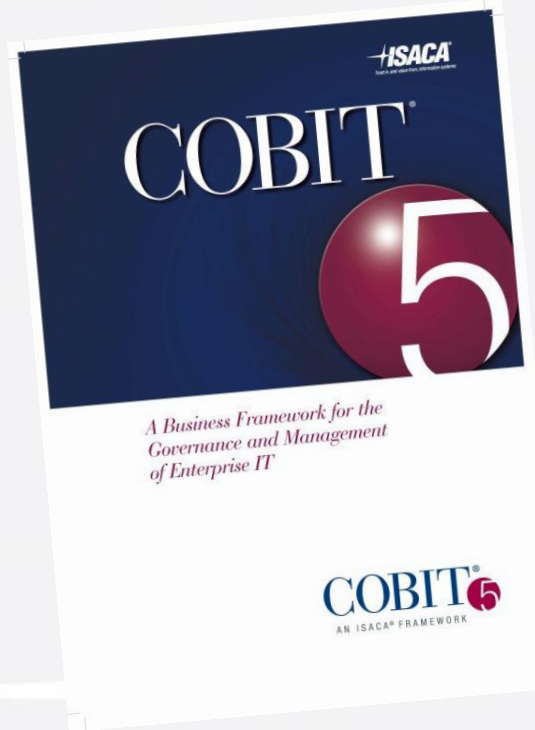
Stakeholder value can be achieved with:

- Good governance and management of information and IT assets
- Buy-in of enterprise boards, executives and management
- Legal, regulatory and contractual compliance



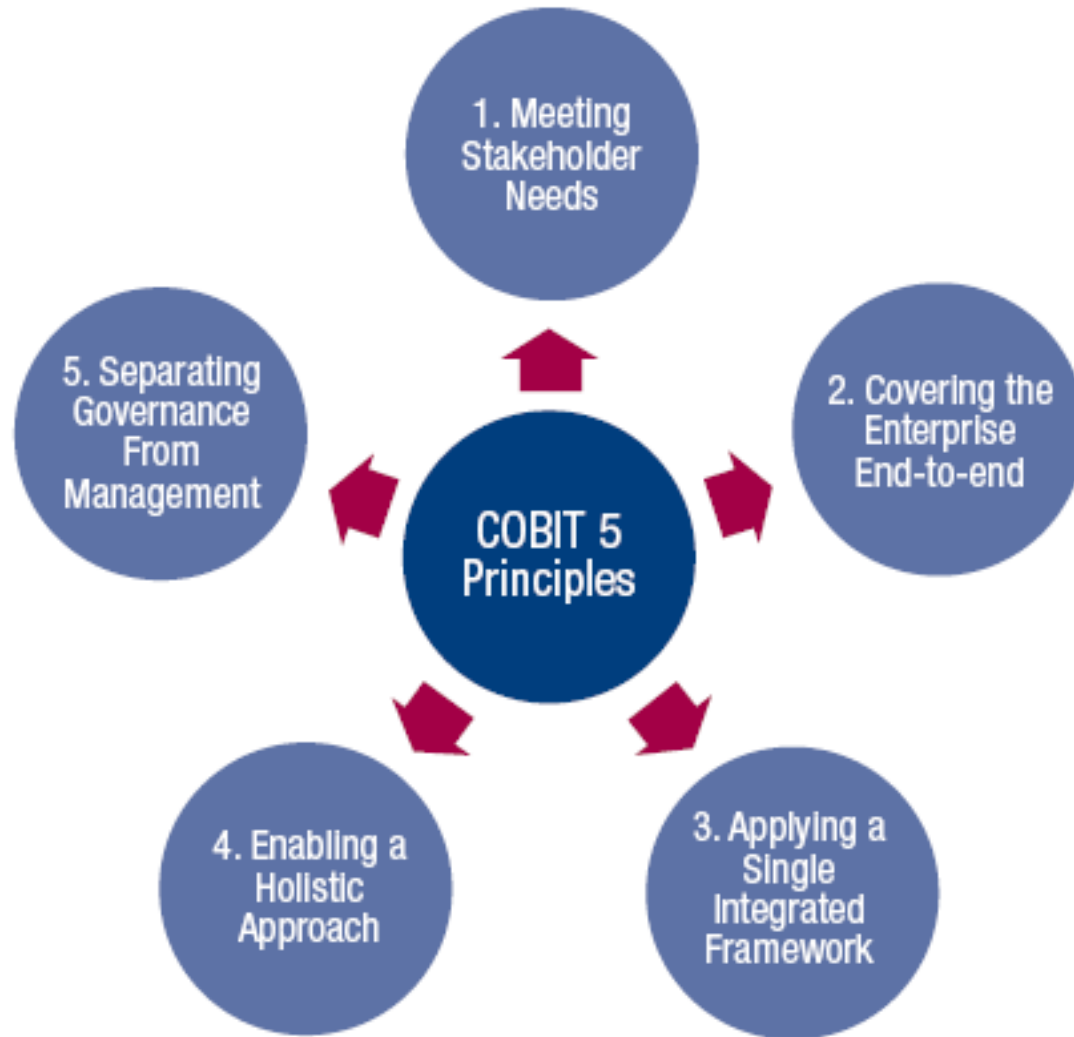
COBIT 5 provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT.

The COBIT 5 Framework



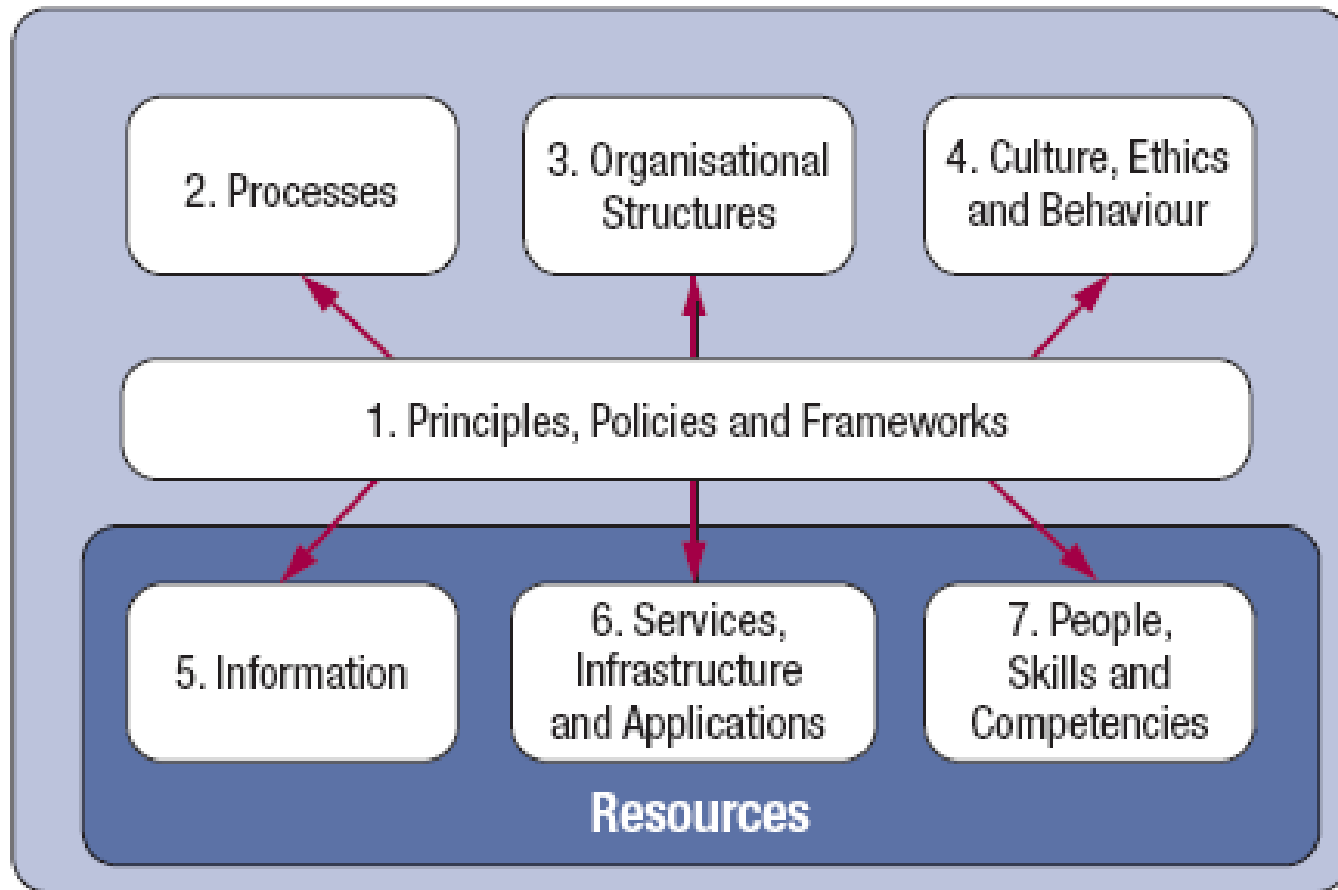
- COBIT 5 helps enterprises create value from IT by maintaining a balance between realising benefits and optimising risk levels.
- COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the entire enterprise.
- The COBIT 5 **principles** and **enablers** are generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

COBIT 5 Principles



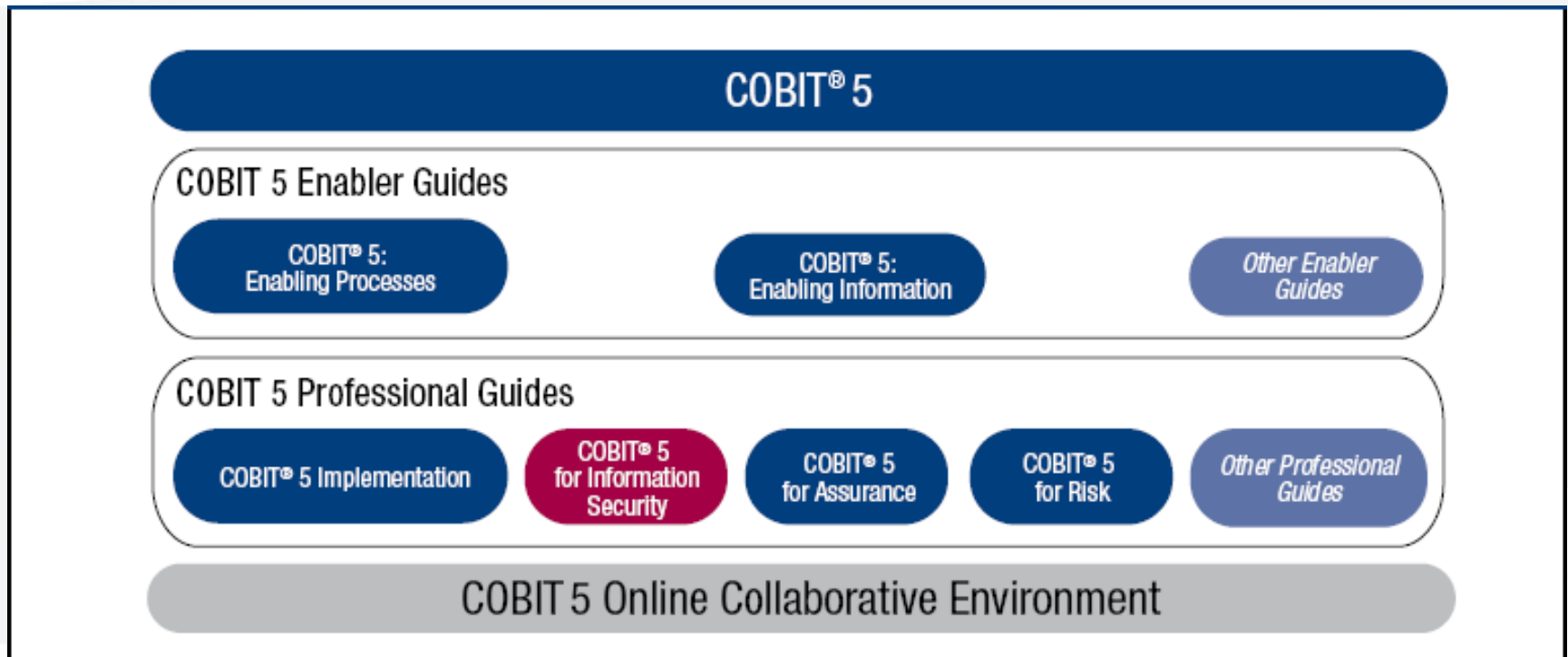
Source: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved.

COBIT 5 Enablers



Source: COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.

COBIT 5 Product Family

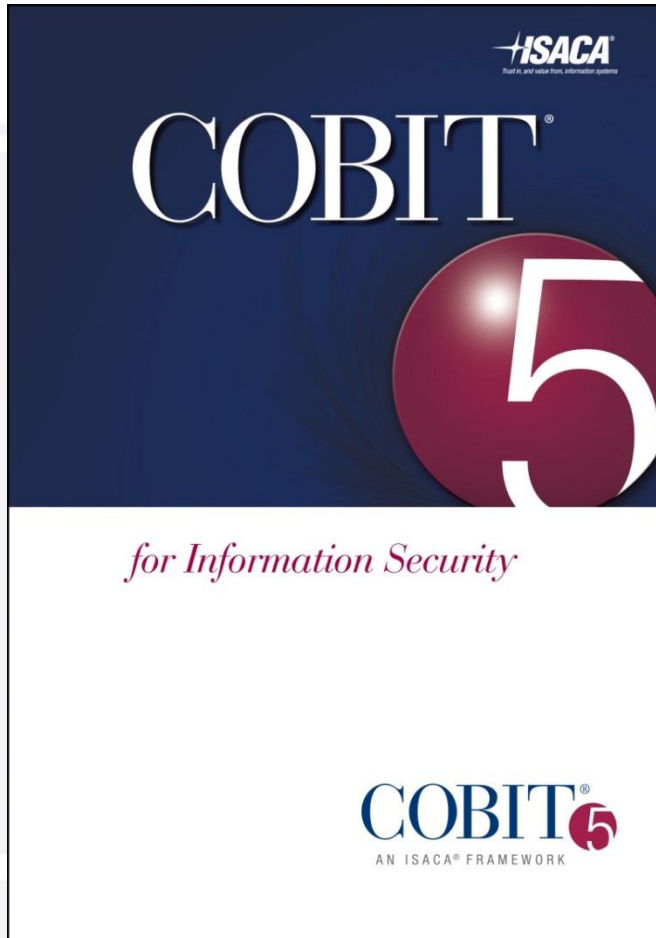


Source: *COBIT® 5 for Information Security*, figure 1. © 2012 ISACA® All rights reserved.

COBIT 5 ***for Information Security***



COBIT 5 for Information Security



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



What does it contain?



Guidance on drivers, benefits

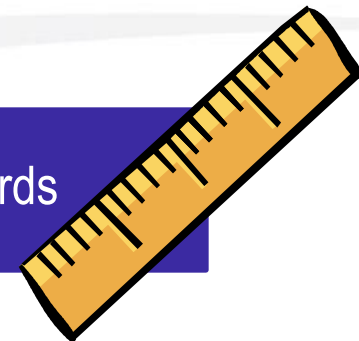
Principles from infosec perspective



Enablers for support



Alignment with standards



Drivers

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 regulations
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

Benefits of using *COBIT 5 for Information Security* include:

- Reduced complexity and increased cost-effectiveness
- Increased user satisfaction
- Improved integration of information security
- Informed risk decisions and awareness
- Improved threat prevention, detection and recovery
- Reduced impact of security incidents
- Better enterprise-wide understanding of information security



Acme Inc

- ISO 27001
- PCI DSS
- OWASP
- Privacy / PII regulation
- Contractual clauses
- ISAE 3402 / SSAE 16
- Cloud Security Alliance Guidelines



Acme SME

- 50 Employees
- 1 location
- 1M USD revenue
- Is C5Sec too heavy for small enterprises?
- NO! It helps establish security according to business needs – gives practical guidance.



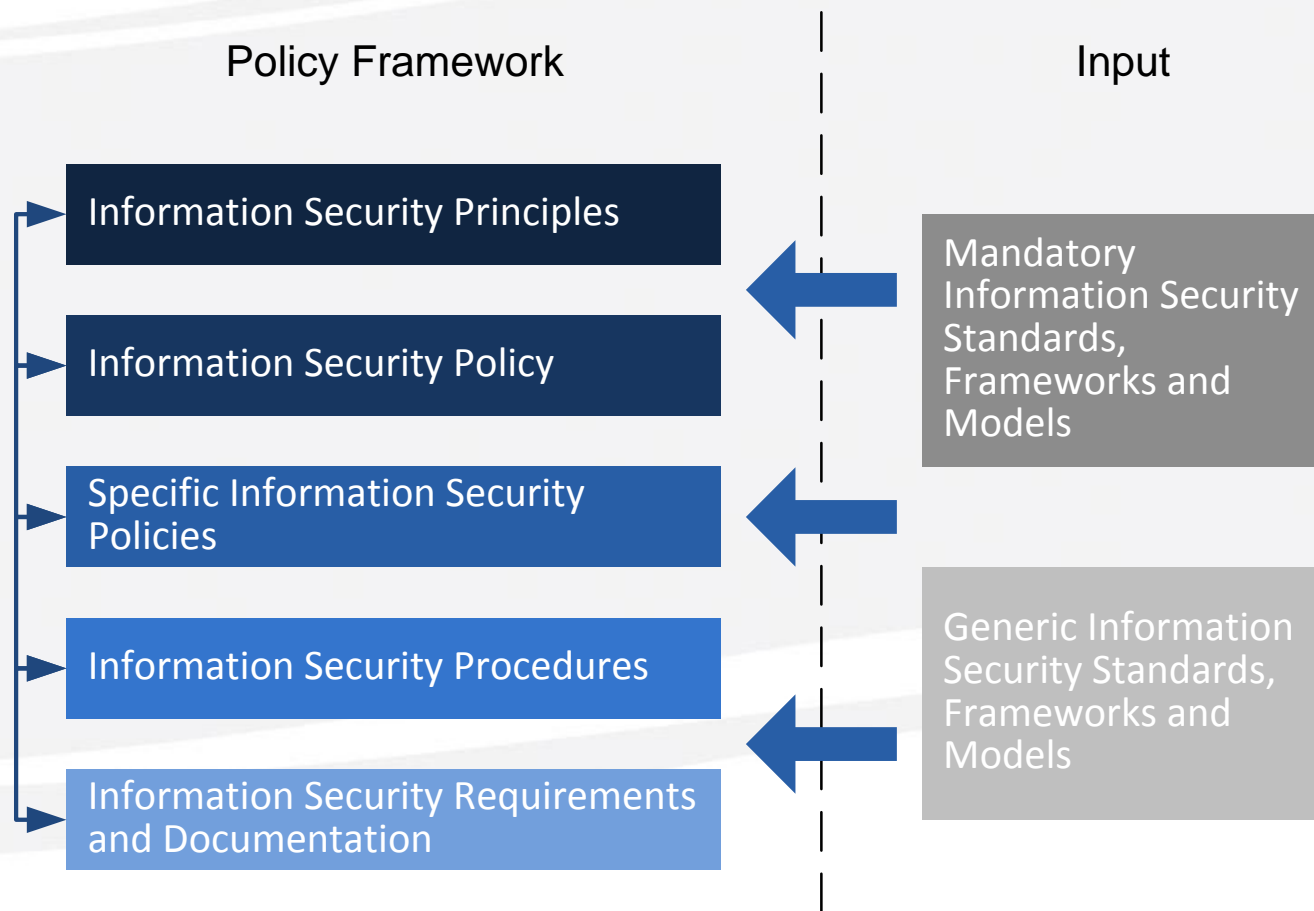
Implementing Information Security

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

- Policies, principles, and frameworks
- Processes
- Organisational structures
- Culture, ethics and behaviour
- Information types
- Service capabilities
- People, skills and competencies



Principles, Policies and Frameworks



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, expressed in simple language.

In 2010, ISACA, ISF and ISC² worked together to create 12 principles* that will help information security professionals add value to their organisations. The principles support three 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

Guidance on how to put principles into practice 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 attributes of each policy: Scope, Validity, Goals



Processes

The COBIT 5 process reference model:

- Governance domain—five governance processes; within each process, evaluate, direct and monitor (EDM) practices are defined
- Management domains—in line with the responsibility areas of plan, build, run and monitor (PBRM)



Processes

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

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

AP001 Manage the IT Management Framework

AP002 Manage Strategy

AP003 Manage Enterprise Architecture

AP004 Manage Innovation

AP005 Manage Portfolio

AP006 Manage Budget and Costs

AP007 Manage Human Resources

AP008 Manage Relationships

AP009 Manage Service Agreements

AP010 Manage Suppliers

AP011 Manage Quality

AP012 Manage Risk

AP013 Manage Security

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

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

BAI10 Manage Configuration

Deliver, Service and Support

DSS01 Manage Operations

DSS02 Manage Service Requests and Incidents

DSS03 Manage Problems

DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

Processes for Management of Enterprise IT

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



EDM03 Ensure Risk Optimisation

EDM03 Ensure Risk Optimisation		Area: Governance Domain: Evaluate, Direct and Monitor
COBIT 5 Process Description 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.		
COBIT 5 Process Purpose Statement 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.		
EDM03 Security-specific Process Goals and Metrics		
Security-specific Process Goals	Related Metrics	
1. Information risk management is part of overall enterprise risk management (ERM).	<ul style="list-style-type: none"> • Percent of information security risk that is related to business risk • Percent of business risk that has been effectively mitigated with information security controls 	



EDM03 Ensure Risk Optimisation

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.	<i>Outside COBIT 5 for Information Security</i>	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Alignment of enterprise KRIs with information security KRIs Information security risk acceptable level 	Updated risk management policies	Internal



Appendix B – APO 13 MANAGE SECURITY

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

Management Practice	Security-specific Inputs (in Addition to COBIT 5 Inputs)		Security-specific Outputs (in Addition to COBIT 5 Outputs)	
	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.	<i>Outside COBIT 5 for Information Security</i>	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



APO 13 MANAGE SECURITY

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

Management Practice	Security-specific Inputs (in Addition to COBIT 5 Inputs)		Security-specific Outputs (in Addition to COBIT 5 Outputs)	
	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.



Organisational Structures

COBIT 5 defines information security roles and structures.

It also examines accountability over information security, providing examples of specific roles and structures and what their mandate is, and looks at potential paths for information security reporting.



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	<p>Depending on a variety factors within the enterprise, the CISO may report to the CEO, COO, CIO, CRO or other senior executive management.</p> <p>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.</p> <p>The CISO must:</p> <ul style="list-style-type: none"> • 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	<p>The CISO is responsible for:</p> <ul style="list-style-type: none"> • 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	<p>The CISO is responsible for implementing and maintaining the information security strategy.</p> <p>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.</p>
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.



Culture, Ethics and Behaviour

1. The Culture Life Cycle –behaviours to benchmark the security culture include:
 - Strength of passwords
 - Lack of approach to security
 - Adherence to change management practices
2. Leadership and Champions to influence culture:
 - Risk managers
 - Security professionals
 - C-level executives
3. Desirable Behaviour to 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.



BYOD

- 2009 security Reaction: NO!
- 2012 security Reaction: HELP!
- C5Sec:
 - Study trends
 - Understand behaviors / culture
 - Update framework: protect / monitor – look ahead – be proactive



Information Types

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

Types of relevant security information include:

- Information security strategy and budget
- Policies
- Awareness material

Information stakeholders, the information life cycle and details specific to security, such as information storage, sharing, use and disposal, are all discussed in *COBIT 5 for Information Security*.



Know your enterprise

- Incidents
- Audit results
- Monitoring reports
- Threats, vulnerabilities, risks, controls
- Feedback from stakeholders
- Customer requirements
- Legal requirements



Services, Infrastructure and Applications

Examples of potential security-related services:

- 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



People, Skills and Competencies

Security-related skills and competencies are needed, including:

- 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

Enterprises should define and implement information security enablers depending on factors within the enterprise's own 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

Define the enterprise's information security requirements 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

More key considerations for implementing *COBIT 5 for Information Security*:

- Create the appropriate environment
- Recognise pain points and trigger events
- Enable change
- Understand that implementing information security practices is not a one-time event but is a life cycle



Acme in the Cloud

- Understand needs
- Know current security level
- Review Cloud contract
- Compare current situation with Cloud Security
- Incorporate in overall assessment criteria
- Make a decision



Connect Other Frameworks, Models, Good Practices and Standards



COBIT 5 for Information Security is an umbrella framework to connect to other information security frameworks, practices and standards, including:

- 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



Conclusions, More Information & Discussion



Next Steps

- Now:
 - Visit www.isaca.org/cobit and download COBIT 5
 - Read COBIT 5 for Information Security
- 90 Days
 - Assess your Information Security requirements
- 180 Days
 - Implement an effective Information Security program

Relevant Links

- Join the COBIT communities in ISACA' s Knowledge Center: www.isaca.org/Knowledge-Center
- Follow ISACA on Twitter: <https://twitter.com/ISACANews>
- Learn about COBIT training: <http://www.isaca.org/cobittraining>



Frequently Asked Questions

Please use the following form for any questions or comments:

<http://www.inforisktoday.com/webinar-feedback.php>

Or contact us at: (800) 944-0401

Thank You for Participating!

Please use the following form for any questions or comments:

<http://www.inforisktoday.com/webinar-feedback.php>

Or contact us at: (800) 944-0401



BANK  INFO SECURITY®

 Just for Credit Unions
CU INFO SECURITY®

 GOV  INFO SECURITY®

 HEALTHCARE  INFO SECURITY®

 infoRisk.
TODAY

 CAREERS  INFO SECURITY®

Data Breach.
Prevention. Response. Notification. TODAY

 **SMG**
INFORMATION SECURITY
MEDIA GROUP

4 Independence Way • Princeton, NJ • 08540 • www.ismgcorp.com