



# COBIT 5: Managing Risk and Increasing Value

## Robert Stroud

Sr. Advisor, Product Management, CA Technologies

[Rob.Stroud@ca.com](mailto:Rob.Stroud@ca.com)

---

## Session Description

Your business depends on technology for its very survival. It's no longer enough to manage your governance, risk, compliance, and governance processes on the fly; they need to be part of your organization's DNA. That's where COBIT 5 comes in.

Unlike many IT frameworks, COBIT 5 is a business framework for the governance and management of enterprise IT. Encompassing the full spectrum of activities, from strategy to execution, COBIT 5 is a top-down framework that is principle-based and enabler-driven, separating governance and management in a guided implementation that ensures practitioners derive value from their IT-enabled business investments. In this session, we will use case studies to explore the critical aspects of COBIT 5 and highlight effective uses of the framework. *(Advanced)*

## Speaker Background


**Robert Stroud**, vice president of strategy and innovation at CA Technologies, is an author, speaker, innovator, and strategist in the ITSM, governance, cloud, mobility, and security space. He is dedicated to the development of industry good practices and he has contributed to many publications and best practice guides, including ISO, ITIL v3 and ITIL 2011, COBIT 4 and COBIT 5, and Basel. Robert has served on many industry boards, including ISACA, itSMF USA, and itSMF International, and he's currently the chair of the ISACA ISO Liaison subcommittee and a member of the ISACA Strategic Advisory Council.



**FUSION 13**  
**COBIT 5: MANAGING RISK AND  
INCREASING VALUE**

ROBERT E STROUD CGEIT CRISC  
@ROBERTESTROUD  
VICE PRESIDENT INNOVATION & STRATEGY CA TECHNOLOGIES  
CHAIR ISACA ISO LIAISON SUB-COMMITTEE  
& COBIT ACCELERATION TASKFORCE

WWW.SMFUSION13.COM | OCTOBER 20-23, 2013 | NASHVILLE, TN



**ABSTRACT**

Your business depends on technology for its very survival. It's no longer enough to manage your governance, risk, compliance, and governance processes on the fly; they need to be part of your organization's DNA. That's where COBIT 5 comes in. Unlike many IT frameworks, COBIT 5 is a business framework for the governance and management of enterprise IT. Encompassing the full spectrum of activities, from strategy to execution, COBIT 5 is a top-down framework that is principle-based and enabler-driven, separating governance and management in a guided implementation that ensures practitioner derive value from their IT-enabled business investments. In this session, we will use case studies to explore the critical aspects of COBIT 5 and highlight effective uses of the framework.

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

Robert E Stroud



- **Robert E Stroud CRISC CGEIT**  
VP , Strategy & Innovation IT Business Management  
CA Technologies USA

- Chair ISACA ISO Liaison Subcommittee
- Chair COBIT Acceleration Task Force
- Winner 2013 ISACA Wasserman Award
- ISACA 2013 Presidents Award for Industry Contributions
- ISACA 2012 John Kuyers Award
- ISACA 2012 ISACA Presidents Award (NJ)
- Past International Vice President ISACA/ITGI
- Contributor COBIT 4, 4.1 & 5 VALIT and RISK IT
- Past Executive Board itSMF International
- Past Board Member USA itSMF
- 15 years Banking Experience
- Author, Public Speaker & Industry Geek



COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

## Agenda

- Introduction to ISACA
- Importance of Governance
- COBIT 5
- Recommendations

- NOTE: Some of the slides reference ISACA COBIT 5.  
Recommend that you refer to the product  
([www.isaca.org](http://www.isaca.org)) or deck

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

[www.isaca.org](http://www.isaca.org)

Trust in, and value from, information systems

## Introduction to ISACA

## What Is ISACA?

- Nonprofit association for individual members
- Founded in 1969, as the EDP Auditors Association (EDPAA)
- More than 110,000 constituents worldwide
  - Members include IT auditors, IT security professionals, IT risk and compliance professionals, IT governance professionals, internal auditors, and more.
  - Nearly all industry categories: financial, public accounting, government/public sector, technology, utilities and manufacturing

## ISACA Chapters Worldwide



1 International Headquarters Office ✪  
200 Chapters Worldwide



Chapters provide:

- Access to affordable local continuing education
- Networking with professional peers
- Opportunity to make a positive impact on the local business community and the profession
- Information exchange opportunities through chapter meetings
- Leadership experience on local boards and committees

7

9/1/13

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

## ISACA Activities

- Chapter network
- Certifications
- IS auditing standards, guidelines, procedures; IS control standards
- Conferences and education
- Periodicals
- Research publications (guidance, frameworks)

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

## ISACA Certifications



...provide assurance by conducting audits and assessments of information systems...

...oversee, direct and manage information security activities...

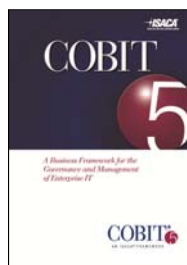
CISA | CISM  
CGEIT | CRISC

...define, establish, maintain and manage a framework of governance over IT...

...identify, evaluate and manage risk through the development, implementation and maintenance of information systems controls...

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

## COBIT



- COBIT 5 [www.isaca.org/cobit](http://www.isaca.org/cobit)
  - COBIT 5 for Information Security
  - COBIT 5 for Assurance
  - COBIT 5 Implementation
  - COBIT 5: Processes Enabler
  - COBIT Assessment Programme
  - Coming soon: COBIT 5 for Risk, COBIT 5: Information Enabler

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

## COBIT Adoption



- EU adopts COBIT for agricultural paying agencies
- COBIT adopted by Paraguayan Superintendency of Banks
- COBIT adopted in Argentina and Uruguay
- US FFIEC lists COBIT
- Lebanese banks endorse COBIT
- Auditor General of Quebec adopts COBIT
- US National Institute of Standards and Technology references COBIT
- US House of Representatives adopts COBIT/Office of Inspector General implements and uses COBIT
- Australian National Audit Office uses COBIT in IT audits
- Philippine Commission on Audit (COA) adopts COBIT
- US Department of Defense, Office of Inspector General, adopts COBIT

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

## Importance of Governance



COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud



COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

Innovation is mandatory

**FUSION 13**  
GRADUATE TO BETTER SERVICE MANAGEMENT

**BUSINESS DEMAND FOR INNOVATION**

IT Capabilities will fill this growing gap!

**IT CAPACITY FOR INNOVATION**

Are you moving for

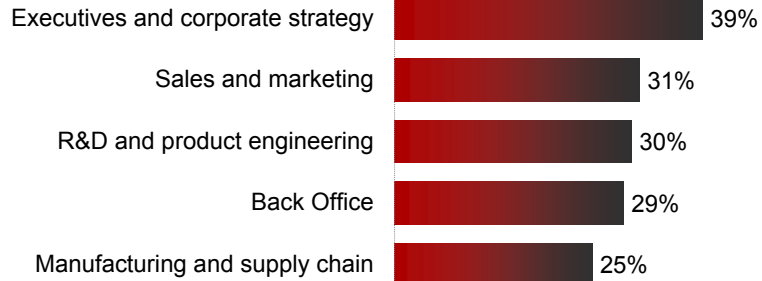
COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud



39% of corporate executives believe IT can deliver new services on time and on budget



"To what extent does the following statement describe your firm's IT organization's processes and capabilities – 'Has the ability to regularly deliver projects on time and on budget'?"\*



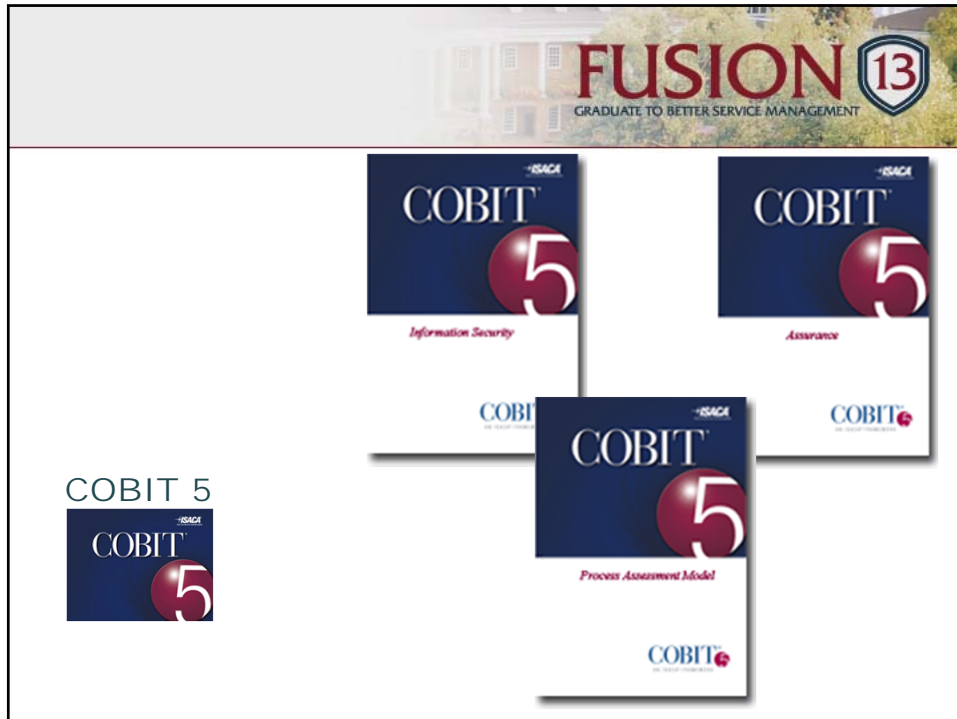
Base: North American and European business decision-makers in firms with 1,000+ employees  
\*Source: "Forrsights: Business Execs Increase Direct IT Spend to Support Systems of Engagement", Forrester Research, Inc., May 16, 2012

Governance, Risk and Control (GRC) Is key to solving IT Problems!



- Organizations are sacrificing money, productivity and competitive advantage by not implementing **effective GRC**
- Executives need a method to:
  - Direct IT for optimal advantage
  - Manage IT-related risks
  - Measure the value provided by IT
  - Drive business innovation leveraging technology
- COBIT 5 is the vehicle that will allow you to **DRIVE** Innovation





COBIT 5

- COBIT 5 is the business framework for the governance and management of enterprise IT
- Provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems
- Expands on COBIT 4.1 by integrating other major frameworks, standards and resources, including ISACA's Val IT and Risk IT, Information Technology Infrastructure Library (ITIL®) and related standards from the International Organization for Standardization (ISO)

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

## COBIT 5 is a 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

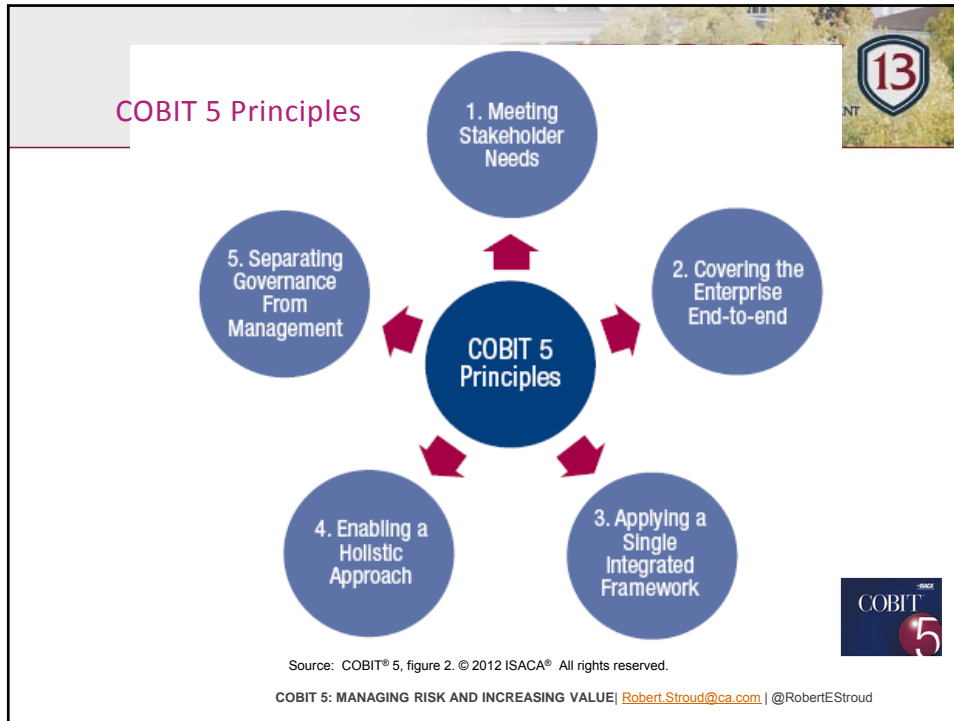
### COBIT 5 Online Collaborative Environment

Source: COBIT® 5, figure 11. © 2012 ISACA® All rights reserved.

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud



COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

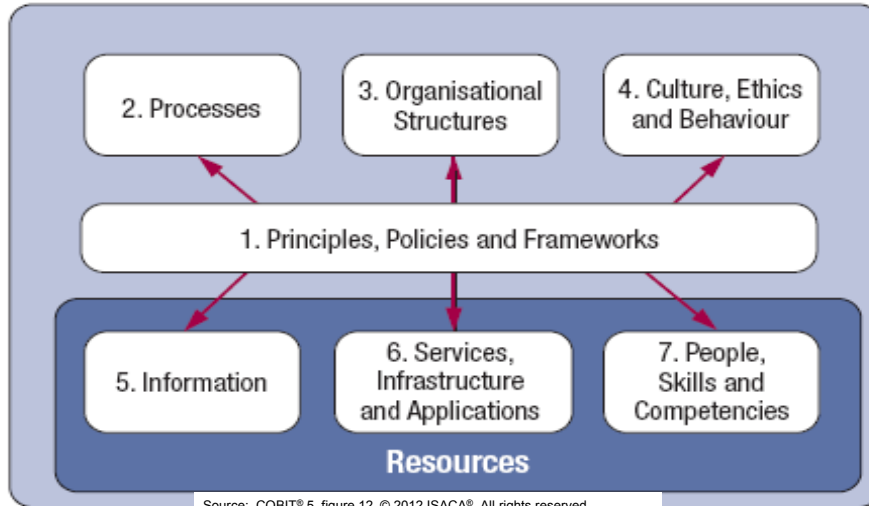


## Stakeholder Value and Business Objectives

BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

Source: COBIT® 5, figure 5. © 2012 ISACA® All rights reserved.  
 COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

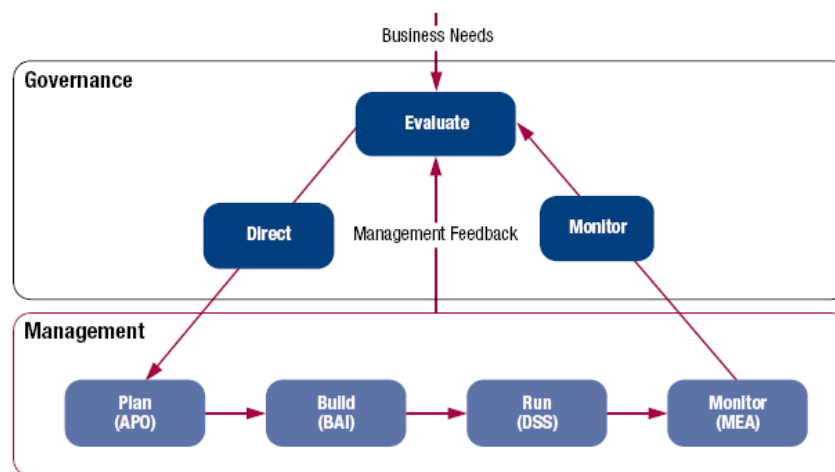
## COBIT 5 Enablers



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

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

## Governance and Management are not the same



Source: COBIT® 5, figure 15. © 2012 ISACA® All rights reserved.

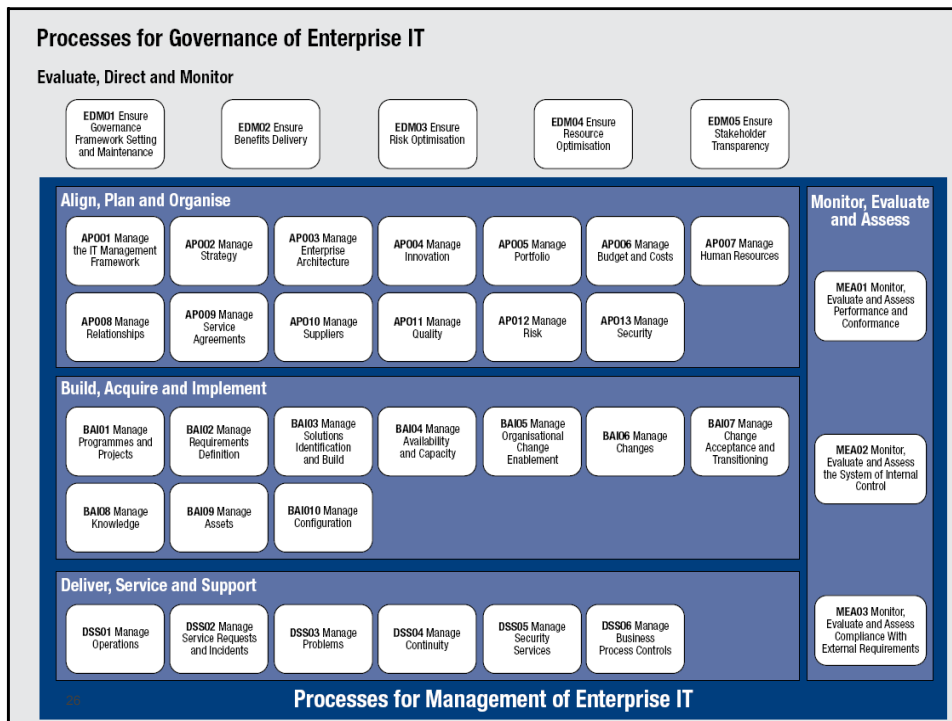
COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

## Separating Governance and Management



- Governance ensures stakeholders needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives are achieved; setting direction through prioritisation, decision making; and monitoring performance 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).

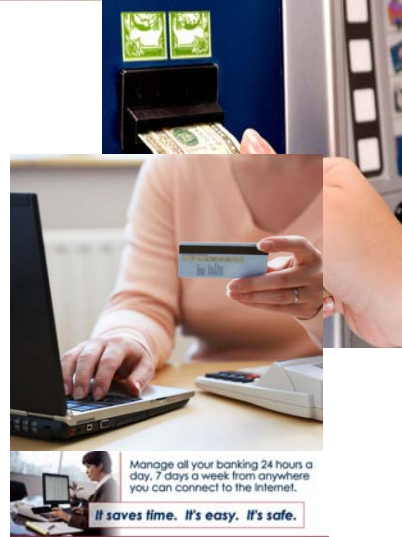
COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud



COBIT, ITIL, PmBok,  
ISO 27000 delivering  
value in a large global bank



- Rapidly growing globally focused on growth emerging markets
- Technology central to the solution and growth
- Changing demographics mobility
- Framework for measuring value and assuring value to the market



COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

## DSS02 Manage Service Requests and Incidents



<b>DSS02 Manage Service Requests and Incidents</b>		Area: Management Domain: Deliver, Service and Support
<b>Process Description</b> Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.		
<b>Process Purpose Statement</b> Achieve increased productivity and minimise disruptions through quick resolution of user queries and incidents.		
<b>The process supports the achievement of a set of primary IT-related goals:</b>		
<b>IT-related Goal</b>	<b>Related Metrics</b>	
04 Managed IT-related business risk	<ul style="list-style-type: none"> <li>• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment</li> <li>• Number of significant IT-related incidents that were not identified in risk assessment</li> <li>• Percent of enterprise risk assessments including IT-related risk</li> <li>• Frequency of update of risk profile</li> </ul>	
07 Delivery of IT services in line with business requirements	<ul style="list-style-type: none"> <li>• Number of business disruptions due to IT service incidents</li> <li>• Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels</li> <li>• Percent of users satisfied with the quality of IT service delivery</li> </ul>	
<b>Process Goals and Metrics</b>		
<b>Process Goal</b>	<b>Related Metrics</b>	
1. IT-related services are available for use.	<ul style="list-style-type: none"> <li>• Number and percent of incidents causing disruption to business-critical processes</li> <li>• Mean time between incidents according to IT-enabled service</li> </ul>	
2. Incidents are resolved according to agreed-on service levels.	<ul style="list-style-type: none"> <li>• Percent of incidents resolved within an agreed-on/acceptable period of time</li> </ul>	
3. Service requests are dealt with according to agreed-on service levels and to the satisfaction of users.	<ul style="list-style-type: none"> <li>• Level of user satisfaction with service request fulfilment</li> <li>• Mean elapsed time for handling each type of service request</li> </ul>	

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

# RACI Chart



## DSS02 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering Programmes/Projects Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
<b>DSS02.01</b> Define incident and service request classification schemes.						C					I	I						A	C	R	R		R	C	C	C
<b>DSS02.02</b> Record, classify and prioritise requests and incidents.						I					I	I									A		R			I
<b>DSS02.03</b> Verify, approve and fulfill service requests.						R												I		R	R		A			
<b>DSS02.04</b> Investigate, diagnose and allocate incidents.						R					I	I				I	I	I		C	R		A	C		
<b>DSS02.05</b> Resolve and recover from incidents.						I					I	I				C	C	I		R	R		A	R		C
<b>DSS02.06</b> Close service requests and incidents.						I					I	I				I	I	I		I	A		I	R		I
<b>DSS02.07</b> Track status and produce reports.						I					I	I				I	I	I		I	A		R	I		

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

# DSS02 Process Practices



## DSS02 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
	From	Description	Description	To
<b>DSS02.01 Define incident and service request classification schemes.</b> Define incident and service request classification schemes and models.	AP009.03	SLAs	Incident and service request classification schemes and models	Internal
	BAI10.02	Configuration repository	Rules for incident escalation	Internal
	BAI10.03	Updated repository with configuration items	Criteria for problem registration	DSS03.01
	BAI10.04	Configuration status reports		
	DSS01.03	Asset monitoring rules and event conditions		
	DSS03.01	Problem classification scheme		
	DSS04.03	Incident response actions and communications		
<b>Activities</b>				
1. Define incident and service request classification and prioritisation schemes and criteria for problem registration, to ensure consistent approaches for handling, informing users about and conducting trend analysis.				
2. Define incident models for known errors to enable efficient and effective resolution.				
3. Define service request models according to service request type to enable self-help and efficient service for standard requests.				
4. Define incident escalation rules and procedures, especially for major incidents and security incidents.				
5. Define incident and request knowledge sources and their use.				

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud



## DSS02 Process Practices



### DSS02 Process Practices, Inputs/Outputs and Activities (cont.)

Management Practice	Inputs		Outputs	
	From	Description	Description	To
<b>DSS02.02 Record, classify and prioritise requests and incidents.</b> Identify, record and classify service requests and incidents, and assign a priority according to business criticality and service agreements.	APO09.03	SLAs	Incident and service request log	Internal
	BAI04.05	Emergency escalation procedure	Classified and prioritised incidents and service requests	APO08.03 APO09.04 APO13.03
	DSS01.03	<ul style="list-style-type: none"> <li>Incident tickets</li> <li>Asset monitoring rules and event conditions</li> </ul>		
	DSS05.07	Security incident tickets		
<b>Activities</b>				
1. Log all service requests and incidents, recording all relevant information so that they can be handled effectively and a full historical record can be maintained.				
2. To enable trend analysis, classify service requests and incidents by identifying type and category.				
3. Prioritise service requests and incidents based on SLA service definition of business impact and urgency.				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
<b>DSS02.03 Verify, approve and fulfil service requests.</b> Select the appropriate request procedures and verify that the service requests fulfil defined request criteria. Obtain approval, if required, and fulfil the requests.	APO12.06	Risk-related root causes	Approved service requests	BAI06.01
			Fulfilled service requests	Internal
<b>Activities</b>				
1. Verify entitlement for service requests using, where possible, a predefined process flow and standard changes.				
2. Obtain financial and functional approval or sign-off, if required, or predefined approvals for agreed-on standard changes.				
3. Fulfill the requests by performing the selected request procedure, using, where possible, self-help automated menus and predefined request models for frequently requested items.				
COBIT 5: MANAGING RISK AND INCREASING VALUE   <a href="mailto:Robert.Stroud@ca.com">Robert.Stroud@ca.com</a>   @RobertEStroud				

## DSS02 Related Guidance



### DSS02 Related Guidance

Related Standard	Detailed Reference
ISO/IEC 20000	<ul style="list-style-type: none"> <li>6.1 Service level management</li> <li>8.2 Incident management</li> </ul>
ISO 27002	13. Information Security Incident Management
ITIL V3 2011	<ul style="list-style-type: none"> <li>20. Incident Management</li> <li>21. Request Fulfilment</li> </ul>



**FUSION** 13  
GRADUATE TO BETTER SERVICE MANAGEMENT

Recommendations

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

## COBIT 5 Future and Supporting Products

**FUSION** 13  
GRADUATE TO BETTER SERVICE MANAGEMENT

- **Professional Guides:**
  - COBIT 5 for Information Security
  - COBIT 5 for Assurance
  - COBIT 5 for Risk
- **Enabler Guides:**
  - COBIT 5: Enabling Information
- **COBIT Online Replacement**
- **COBIT Assessment Programme:**
  - Process Assessment Model (PAM): Using COBIT 5
  - Assessor Guide: Using COBIT 5
  - Self-assessment Guide: Using COBIT 5
- **COBIT 5 – Vendor Management**
- **COBIT 5 – Configuration Management**



COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

## Summary

**FUSION** 13  
GRADUATE TO BETTER SERVICE MANAGEMENT

- "Just enough" should be the approach to governance in terms of "what" is governed and to what depth.
- Governance processes are the purview of senior management
- Your Management processes are how resources are used effectively every day

COBIT 5: MANAGING RISK AND INCREASING VALUE | [Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com) | @RobertEStroud

- **Monday Morning**
  - Visit [www.isaca.org](http://www.isaca.org), register and download COBIT 5
  - Look through the overview presentations
- **Next 90 Days**
  - Read the Implementation Guide
  - Understand the low hanging opportunities
- **Next Year**
  - Develop your plan for action
  - Execute

embrace with knowledge





**FUSION 13**

**Robert E Stroud CGEIT CRISC**  
[Robert.Stroud@ca.com](mailto:Robert.Stroud@ca.com)  
Twitter @robertestroud

<http://community.ca.com/blogs/ITIL>  
<http://community.ca.com/blogs/ppm>

WWW.SMFUSION13.COM | OCTOBER 20-23, 2013 | NASHVILLE, TN