COBIT 5 for Risk – An overview
Introduction

• Education
  • 1st Class BSc (Hons) Computing
  • BS7799 Lead Auditor, ITIL Service Manager
  • Prince 2 Certified Practitioner, CGEIT, CRISC

• Professional Career
  • International Brewer, various roles (1991-1996)
  • KPMG, Head of IT Risk (1996-2012)
  • Betfair, Head of Governance, Risk & Assurance (2012-…)

• ISACA involvement – past and present
  • RiskIT TF, COBIT 5 TF, Cloud Computing TF
  • Knowledge Board member, Framework Committee Chair
  • COBIT 5 for Risk TF Chair, COBIT Growth Strategy TF

Steven Babb
steven.babb@betfair.com
Objectives

• **After completing this session, you will:**
  • Be clear on the drivers, benefits and target audience for COBIT 5 for Risk
  • Understand the two perspectives on how COBIT 5 for Risk can be used
  • Understand how to use risk scenarios and COBIT 5 enablers for governing and managing risk activities
  • Understand how COBIT 5 for Risk relates and aligns to other standards

• **Health warning** – The diagrams used here are from an advanced development draft, the published diagrams may be slightly different
The COBIT 5 journey… so far
Release of COBIT 5

- COBIT 5 Framework
- COBIT 5 Implementation Guide
- COBIT 5: Enabling Processes

IT professionals and CIOs need up-to-date tools and expertise to navigate an increasingly complex business environment
June 2012

**Release of COBIT 5 for Information Security**

Leverages the COBIT 5 framework through a security lens

Provides guidance to help IT and security professionals understand, utilise, implement and direct important information security-related activities
January 2013

Release of the COBIT 5 Assessment Programme

- COBIT Process Assessment Model: Using COBIT 5
- COBIT Assessor Guide: Using COBIT 5
- COBIT Self-Assessment Guide: Using COBIT 5

Provides a clear process assessment capability and helps enterprises ensure strong, reliable and consistent processes.
Release of COBIT 5 for Assurance

Leverages the COBIT 5 framework through an assurance lens

Provides guidance for Assurance professionals and other interested parties at all levels on how to use COBIT 5 to support a variety of IT assurance activities.
Imminent release!

Release of COBIT 5 for Risk

Leverages the COBIT 5 framework through a risk management lens

Provides… Stay tuned to the rest of this presentation!
In development...

COBIT 5 Enabling Information

A replacement for COBIT Online

- **Phase 1**, Q4 2013 – Access to COBIT 5 publications
- **Phase 2**, Q1 2014 (tentative) – Access to other, non-COBIT, ISACA content and current, relevant GEIT material
- **Phase 3**, Q3 2014 (tentative) – Ability to customize COBIT to fit the needs of your enterprise with access for multiple users
What are the drivers, benefits and target audience for COBIT 5 for Risk
Drivers

The main drivers for risk management include providing:

- Stakeholders with substantiated and consistent opinions over the current state of risk throughout the enterprise
- Guidance on how to manage the risk to levels within its risk appetite
- Guidance on how to set-up the right risk culture for the enterprise
- Wherever possible, quantitative risk assessments enabling stakeholders to consider the cost of mitigation and the required resources against the loss exposure
To meet these drivers, COBIT 5 for Risk provides:

- Guidance on how to use the COBIT 5 Framework to establish the risk governance and management function(s) for the enterprise
- Guidance and a structured approach on how to use the COBIT 5 Principles to govern and manage IT Risk
- A clear understanding on the alignment of COBIT 5 for Risk with other relevant standards
Which in turn brings a number of risk-related capabilities – or "benefits" – to the enterprise:

- End-to-end guidance on how to manage risk
- A common and sustainable approach for assessment and response
- A more accurate view of significant current and near-future risk throughout the Enterprise – and the impact of this risk on the Enterprise
...continued:

- Understanding how effective IT risk management optimises value by enabling process effectiveness and efficiency
- Opportunities for integration of IT risk management with the overall risk and compliance structures within the enterprise
- Promotion of risk responsibility and its acceptance throughout the enterprise
Target audience

The intended audience for COBIT 5 for Risk is extensive – the target audience includes:

• Risk professionals across the enterprise
  – assistance with managing IT risk and incorporating IT risk into ERM

• Boards and executive management
  – understanding of their responsibilities and roles with regard to IT risk management
  – the implications of risk in IT to Enterprise strategic objectives
  – how to better optimise IT use for successful strategy execution

• IT and business management
  – understanding of how to identify and manage IT risk and how to communicate IT risk to business decision makers
Outcomes

Well governed and managed information and technology delivers business benefits and/or preserves value

- New IT-enabled business opportunities
- Enhanced business opportunities
- Sustainable competitive advantage

Poorly governed and managed information and technology will destroy value or fail to deliver benefits.

- Unrealised or reduced business value
- Missed IT-enabled business opportunities
- Adverse IT-related events destroying value
Key questions

• What is IT risk?
  
  *IT risk is defined as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise*

• How are the COBIT 5 enablers used to provide risk management?
  
  *They are used to provide two perspectives on how to use COBIT 5:*
  
  – *The risk function perspective – what is needed in an enterprise to establish a risk function*
  
  – *The risk management perspective – how the core risk management process of identifying, analysing and responding to risk are delivered*

• How do I set up and maintain an efficient risk function?
  
  *COBIT 5 for Risk provides guidance on what is needed to set up and maintain an effective and efficient risk function. It does so by listing and briefly describing the COBIT 5 enablers required, e.g., processes, organisational structures, culture, ethics and behaviour*
Key questions

- Are there any practical examples of risk scenarios provided?
  Yes. A comprehensive list of example IT-related risk scenarios are provided, as well as some practical advice on how to best use these example scenarios.

- How does COBIT 5 for Risk help me in responding to risk?
  COBIT 5 for Risk makes the link between risk scenarios and an appropriate response. Examples are also given on how risk scenarios can be mitigated through COBIT 5 enablers (controls).

- Does COBIT 5 align with risk management standards?
  Yes. A detailed comparison, in the form of a mapping or qualitative description, is included for a number of related standards.

- Does COBIT 5 for Risk help me in defining detailed risk analysis methods?
  No. Additional guidance on detailed risk analysis methods, taxonomies, tools, etc., is available from multiple sources, including ISACA.
What are the two perspectives on how COBIT 5 for Risk can be used
Value creation

- Enterprises exist to **create stakeholder value**
- Any enterprise, commercial or not, has **value creation as a governance objective**
- Value creation means **realising benefits** at an **optimal resource** cost while **optimising risk**
- Benefit forms, e.g., **financial** for commercial enterprises or **public service** for public bodies
- Risk optimisation is therefore an **essential part** of any governance system
- Risk optimisation cannot be seen in isolation, i.e., actions taken as part of **risk management will influence** benefits realisation and resource optimisation.
Value creation

- Governance objectives need to be translated into **manageable goals**
- This is the **COBIT 5 goals cascade**
- This translates stakeholder needs into **specific, actionable and customised goals**
COBIT 5 makes a clear distinction between governance and management

- **Governance**
  - Ensuring that stakeholder needs are driven through agreed-on enterprise objectives; Setting direction through prioritisation and decision making; Monitoring performance and compliance and progress

- **Management**
  - Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives
Risk perspectives

Risk Function Perspective

The risk function perspective describes how to build and sustain a risk function in the enterprise by using the COBIT 5 enablers.

COBIT 5 Enablers

- Processes
- Organisational Structures
- Culture, Ethics and Behaviour
- Principles, Policies and Frameworks
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

Risk Management Perspective

The risk management perspective looks at core risk governance and risk management processes and risk scenarios. This perspective describes how risk can be mitigated by using COBIT 5 enablers.
COBIT 5 for Risk provides guidance and describe how each enabler contributes to the overall governance and management of the risk function. For example, which:

- **Processes** are required to define and sustain the risk function, govern and manage risk.
- **What Information flows** are required to govern and manage risk – e.g. risk universe, risk profile, etc.
- **The Organisational structures** that are required to govern and manage risk effectively – e.g. Enterprise risk committee, risk function, etc.
- **What People and Skills** should be put in place to establish and operate an effective risk function.
COBIT 5 for Risk identifies all COBIT 5 processes that are required to support the risk function:

- **Key supporting processes** – dark pink
- **Other supporting processes** – light pink

Core risk processes, shown in light blue are also highlighted – these processes support the **Risk Management Perspective**:

- EDM03 – Ensure risk optimisation
- APO12 – Manage risk
COBIT 5 for Risk provides specific guidance related to all enablers for the effective management of risk:

- The core **Risk Management process(es)** used to implement effective and efficient risk management for the enterprise in order to support stakeholder value
- **Risk Scenarios**, i.e. the key information item needed to identify, analyse and respond to risk; Risk scenarios are the concrete, tangible and assessable representation of risk
- How **COBIT 5 enablers** can be used to **respond** to unacceptable risk scenarios
How should I use risk scenarios and COBIT 5 enablers for governing and managing risk activities
Risk scenarios

Definition

“A risk scenario is a description of a possible event that, when occurring, will have an uncertain impact on the achievement of the enterprise’s objectives. The impact can be positive or negative.”
Risk scenarios

Risk scenario’s are a key element of the risk management process APO12; two approaches are defined:

- **Top-down approach** – Use the overall enterprise objectives and consider the most relevant and probable IT risk scenarios impacting these

- **Bottom-up approach** – Use a list of generic scenarios to define a set of more relevant and customised scenarios, applied to the individual enterprise
Risk scenarios

• Both approaches are complementary and should be used simultaneously
• Risk scenarios must be relevant and linked to real business risk
• Specific risk items for each enterprise and critical business requirements need to be considered in the enterprise risk scenarios
• COBIT 5 for Risk provides a comprehensive set of generic risk scenarios – these should be used as a reference to reduce the chance of overlooking major/common risk scenarios
When a risk scenario materialises, a **loss event** occurs. The loss event has been triggered by a **threat event** (Threat type + Event).

- The frequency of the threat event is influenced by a **vulnerability**.
- The vulnerability is usually a state; it can be increased/decreased by vulnerability events, e.g., controls strength or by the threat strength.
COBIT 5 for Risk provides:

- **111 risk scenario examples**
- **across 20 scenario categories**

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Risk Scenario Category</th>
<th>IT Benefit/Value Enablement</th>
<th>IT Programme and Project Delivery</th>
<th>IT Operations and Service Delivery</th>
<th>Negative Example Scenarios</th>
<th>Positive Example Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>Business ownership of IT</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>Business does not assume accountability over those IT areas it should, e.g., functional requirements, development priorities, assessing opportunities through new technologies.</td>
<td>Business assumes appropriate accountability over IT and co-determines the strategy of IT, especially application portfolio.</td>
</tr>
<tr>
<td>1002</td>
<td></td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>There is extensive dependency and use of end-user computing and ad hoc solutions for important information needs, leading to security deficiencies, inaccurate data or increasing costs/inefficient use of resources.</td>
<td></td>
</tr>
<tr>
<td>1003</td>
<td></td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>Cost and ineffectiveness is related to IT related purchases outside of the procurement process.</td>
<td>A business case is always made up to ensure optimal cost and effective purchasing of software.</td>
</tr>
<tr>
<td>1004</td>
<td></td>
<td></td>
<td></td>
<td>P</td>
<td>Inadequate requirements lead to ineffective service level agreements (SLAs).</td>
<td></td>
</tr>
</tbody>
</table>
Risk response

- To bring risk in line with the risk appetite for the enterprise
- A response needs to be defined such that as much future residual risk as possible (current risk with the risk response defined and implemented) falls within accepted limits
- When risk analysis has shown that risk is not aligned with the defined risk appetite and tolerance levels, a response is required
- This response can be any of the four possible responses:
  - Avoid, Mitigate, Share/Transfer, Accept
- Risk response evaluation is not a one-time effort – it is part of the risk management process cycle
COBIT 5 for Risk provides a number of examples on how the COBIT 5 enablers can be used to respond to risk scenarios.

In the risk response process, risk mitigation is identified as one of the options to respond to any excessive risk. IT risk mitigation is equivalent to implementing a number of IT controls.

In COBIT 5 terms, IT controls can be any enabler, e.g.,
- putting in place an organisational structure, putting in place certain governance or management practices or activities, etc.

For each of the 20 risk scenario categories, potential mitigating actions relating to all seven COBIT 5 enablers are provided, with a reference, title and description for each enabler that can help to mitigate the risk.
### D.3. Scenario 3: IT Investment Decision Making

**Risk Scenario Category**
- IT investment decision making

**Principles, Policies and Frameworks Enabler**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Contribution to Response to Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programme/Project management policy</td>
<td>The policy should define who needs to be involved in investment decisions and the chain of approval.</td>
</tr>
</tbody>
</table>

**Process Enabler**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Management Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO05.06</td>
<td>Manage benefits achievement.</td>
<td>Monitor the benefits of providing and maintaining appropriate IT services and capabilities, based on the agreed-on and current business case.</td>
</tr>
<tr>
<td>APO06.02</td>
<td>Prioritise resource allocation.</td>
<td>Implement a decision-making process to prioritise the allocation of resources and rules for discretionary investments by individual business units. Include the potential use of external service providers and consider the buy, develop and rent options.</td>
</tr>
<tr>
<td>APO06.03</td>
<td>Create and maintain budgets.</td>
<td>Prepare a budget reflecting the investment priorities supporting strategic objectives based on the portfolio of IT-enabled programmes and IT services.</td>
</tr>
<tr>
<td>APO07.01</td>
<td>Maintain adequate and appropriate staffing.</td>
<td>Evaluate staffing requirements on a regular basis or on major changes to the enterprise or operational or IT environments to ensure that the enterprise has sufficient human resources to support enterprise goals and objectives. Staffing includes both internal and external resources.</td>
</tr>
<tr>
<td>BAI01.03</td>
<td>Manage stakeholder engagement.</td>
<td>Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information that reaches all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.</td>
</tr>
<tr>
<td>BAI03.04</td>
<td>Procure solution components.</td>
<td>Procure solution components based on the acquisition plan in accordance with requirements and detailed designs, architecture principles and standards, and the enterprise’s overall procurement and contract procedures, QA requirements, and approval standards. Ensure that all legal and contractual requirements are identified and addressed by the supplier.</td>
</tr>
</tbody>
</table>
How COBIT 5 for Risk relates and aligns to other standards
• COBIT 5 for Risk – much like COBIT 5 itself – is an umbrella approach for the provisioning of risk
• COBIT 5 for Risk is positioned in context with the following risk-related standards:
  – COSO Enterprise Risk Management
• ISO 31000:2009 – Risk Management
  – COBIT 5 for Risk addresses all ISO 31000 principles, through:
    • The COBIT 5 for Risk principles and enablers themselves
    • Its conceptual design or through the enabler models
  – In addition, the framework and process model aspects are covered in greater detail by the COBIT 5 for Risk process model
  – All elements are included in COBIT 5 for Risk and are often expanded on or elaborated in greater detail, specifically for IT risk management
ISO 27005:2011 – Information security risk management

- COBIT 5 for Risk addresses all of the components described within ISO 27005. Some of the elements are structured or named differently.
- COBIT 5 for Risk takes a broader view on IT risk management compared with ISO 27005 which is focused on the management of security related risk.
- There is a strong emphasis in COBIT 5 for Risk on processes and practices in order to ensure the alignment with business objectives, the acceptance throughout the organisation and the completeness of the scope, amongst other factors.
Alignment

• COSO Enterprise Risk Management
  – COBIT 5 for Risk addresses all of the components defined in COSO ERM, sometimes extending the coverage of COSO ERM to the specifics of IT use in the enterprise
  – Although COBIT 5 for Risk focuses less on control, it provides linkages to management practices in the COBIT 5 framework
  – The essentials with regards to both control and general risk management as defined in COSO ERM are present in COBIT 5 for Risk, either through:
    • The principles themselves and the framework’s conceptual design
    • The process model and additional guidance provided in the framework
Thank you for your interest in COBIT 5 and the forthcoming COBIT 5 for Risk
Publication will be very soon – WATCH THIS SPACE!!
To learn more – [www.isaca.org/COBIT5](http://www.isaca.org/COBIT5)