COBIT® 5
All together now!

Geoff Harmer
PhD, CEng, FBCS, CITP, CGEIT
Maat Consulting
Reading, UK
www.maatconsulting.com
Agenda

- Introduction to COBIT 5
- Dive deeper
  - Framework
    - 5 Principles
    - 7 Enablers
  - Domains and processes
  - Management practices
  - Process capability assessment
  - Current and future ISACA resources for COBIT® 5
- Summary

Based on COBIT 5 (2012)
Introduction to COBIT® 5

“A business framework for the governance and management of enterprise IT”

ISACA
COBIT®: Audit to GEIT in 16 years

Governance of Enterprise IT

IT Governance

Management

Control

Audit

COBIT 1  COBIT 2  COBIT 3  COBIT 4.0/4.1  COBIT 5


Val IT 2.0 2008

Risk IT 2009

Based on COBIT 5 (2012)
Approach to the design of COBIT® 5

- Aims to be the only business framework for the governance and management of enterprise IT
- Integrates ISACA’s frameworks and knowledge resources
  - COBIT® 4.1 (IT governance and management)
  - Val IT™ (Value delivery)
  - Risk IT™ (Risk management)
  - BMIS™ (Business Model for Information Security)
  - ITAF™ (IT Audit Framework)
  - TGF™ (Taking Governance Forward)
  - Board Briefing on IT Governance 2nd Edition
- Integrates other major frameworks and standards
  - Particularly ISO 38500:2008 Corporate Governance of IT
- Plus latest enterprise governance and management techniques

Maat Consulting Ltd  Based on COBIT 5 (2012)
COBIT® documents: 10 April 2012

- **COBIT® 5: A Business Framework for Governance & Management of Enterprise IT**
  - Main guidance document

- **COBIT® 5: Enabling Processes**
  - 5 domains, 37 processes & 208 governance/management practices

- **COBIT® 5: Implementation**
  - Includes a toolkit: PowerPoint® slide sets and PDF docs
  - No equivalent of the COBIT® 4.1 Assessment Excel® tool
“COBIT® 5: A Business Framework …”

- The main guidance document
- Contents:
  - Executive summary
  - Description of framework components
  - 5 principles
  - 7 enablers
  - Overview of implementation guidance
  - Overview of COBIT® Process Capability Model (PCM)
Governance (EDM)
- Evaluates stakeholder needs, conditions and options
- Sets direction by prioritisation and decision making
- Monitors performance, compliance and progress against agreed direction
- Responsibility: Board; Leader: Chairperson

Management (PBRM)
- Plans, builds, runs and monitors activities
- Aligned with governance body’s direction
- With goal of achieving enterprise objectives
- Responsibility: Executive management; Leader: CEO
Management & Governance Practices

COBIT® 4.1
Control Objectives
210

Val IT™
Management Practices
22

Risk IT™
Management Practices
9

COBIT® 5

Governance Practices
15
Management Practices
193

Maat Consulting Ltd
COBIT® 5: 5 Principles

1. Meeting stakeholder needs
2. Covering the enterprise end-to-end
3. Single integrated framework
4. Holistic approach of 7 enterprise enablers
5. Separating governance from management

Based on COBIT 5 (2012)
COBIT® 5: 7 Enterprise Enablers

Organisational Structures

Processes

Culture, Ethics and Behaviour

Principles, Policies and Frameworks

Information

Service Infrastructure & Applications

People, Skills & Competencies

Resources

Based on COBIT 5 (2012)
Summary of COBIT® 5

5 Principles allow

Building of a governance and management framework

Based on 7 enablers that

Optimise information and technology investment and its use to benefit stakeholders
Dive deeper into COBIT® 5

“A business framework for the governance and management of enterprise IT”

ISACA
COBIT® 5: The 5 Principles

1. Meeting stakeholders’ needs
2. Covering the enterprise end-to-end
3. Single integrated framework
4. Holistic approach of 7 enterprise enablers
5. Separating governance from management
What are Stakeholders’ needs?

- **Internal Stakeholders**
  - Board
  - CxOs
  - Business process owners & managers
  - Risk and security managers
  - HR managers
  - IT managers and IT audit
  - IT users

- **Needs**
  - Value from IT
  - Performance of IT
  - Strategic use of new technology
  - Compliance with regulations
  - IT-related risk control
  - Control IT costs (+ sourcing options)
  - IT skills
  - IT programme/project control

- **External Stakeholders**
  - Shareholders
  - Business partners and suppliers
  - Regulators/government
  - Customers
  - External users
  - External auditors

- **Needs**
  - Security/reliability of partners?
  - Is enterprise compliant?
  - Effective enterprise internal controls?

Based on COBIT 5 (2012)
Stakeholders’ Needs

**Governance Objective: Value Creation**

- Benefits Realisation
- Risk Optimisation
- Resource Optimisation

Based on COBIT 5 (2012)
Meeting Stakeholders’ Needs

- **Stakeholder Drivers**
  - PESTLE

- **Stakeholder Needs**
  - Benefits
  - Risk
  - Resource
  - Realisation
  - Optimisation

- **Enterprise Goals**

- **IT-related Goals**

- **Enabler Goals**
  - (Processes +++)

- **Governance Requirements**

Based on COBIT 5 (2012)

Maat Consulting Ltd
Covering the Enterprise End-to-End

- COBIT® 5 covers governance & management of IT (GEIT)
- Integrates GEIT into Enterprise Governance
- Seamless integration since aligned with latest views
- Not focused ONLY on the IT function
  - Covers all functions and processes with the enterprise
  - IT is like all other assets in an enterprise

Based on COBIT 5 (2012)
Single Integrated Framework

COBIT® 5

COSO
ERM
OECD CG
UK CCCG
King III
MSP

COSO
Kotter
ISO 31000
ISO 9001
BS 25999

ITIL 2011
ISO 38500
TOGAF
CEAF
FEA

PRINCE2
PMBOK
ISO 27000
ISO 20000
CMMI–DEV

Maat Consulting Ltd
Enabling a Holistic Approach - 1

The 7 Enablers

 Processes

 Organisational Structures

 Culture, Ethics And Behaviour

 Principles, Policies and Frameworks

 Information

 Service Infrastructure & Applications

 People, Skills & Competencies

Resources

Based on COBIT 5 (2012)
Enabling a Holistic Approach - 2

- Enablers must be interconnected
  - Inputs from other enablers
  - Outputs to benefit other enablers

![Diagram showing the relationship between Information, People, Skills and Competencies, Organisational Structures, and Processes.]

Based on COBIT 5 (2012)
## Enabler Performance Management

<table>
<thead>
<tr>
<th>Metrics for Achievement of Goals (LAG indicators)</th>
<th>Metrics for Application of Practice (LEAD indicators)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stakeholders’ needs addressed?</td>
<td>Lifecycle managed?</td>
</tr>
<tr>
<td>Enabler Goals achieved?</td>
<td>Good practices applied?</td>
</tr>
</tbody>
</table>

Based on COBIT 5 (2012)
Separating Governance from Management

ISO 38500
Based on ISO 38500 (2008)

COBIT 5
Based on COBIT 5 (2012)

Business Needs

Governance
Evaluate
Direct
Monitor

Management
Plan (APO)
Build (BAI)
Run (DSS)
Monitor (MEA)

Management Feedback
Domains & Processes
COBIT® 5: Processes (37)

Processes for Governance of Enterprise IT

**Evaluate, Direct and Monitor (EDM)**

**Align, Plan and Organise (APO)**
- APO01 – APO13

**Build, Acquire and Implement (BAI)**
- BAI01 – BAI010

**Deliver, Service and Support (DSS)**
- DSS01 – DSS06

**Monitor, Evaluate And Assess (MEA)**
- MEA01 – MEA03

Processes for Management of Enterprise IT

Based on COBIT 5 (2012)
Evaluate, Direct and Monitor (EDM)

EDM01  Ensure Governance Framework Setting and Maintenance
EDM02  Ensure Benefits Delivery
EDM03  Ensure Risk Optimisation
EDM04  Ensure Resource Optimisation
EDM05  Ensure Stakeholder Transparency

Based on COBIT 5 (2012)
Align, Plan and Organise (APO)

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

Based on COBIT 5 (2012)
Build, Acquire and Implement (BAI)

BAI01 Manage Programmes and Projects
BAI02 Manage Requirements Definition
BAI03 Manage Solution, 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 (DSS)

DSS01  Manage Operations
DSS02  Manage Service Requests and Incidents
DSS03  Manage Problems
DSS04  Manage Continuity
DSS05  Manage Security Services
DSS06  Manage Business Process Controls

Based on COBIT 5 (2012)
### Monitor, Evaluate and Assess (MEA)

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEA01</td>
<td>Monitor, Evaluate and Assess Performance and Conformance</td>
</tr>
<tr>
<td>MEA02</td>
<td>Monitor, Evaluate and Assess the System of Internal Controls</td>
</tr>
<tr>
<td>MEA03</td>
<td>Monitor, Evaluate and Assess Compliance with External Requirements</td>
</tr>
</tbody>
</table>

Based on COBIT 5 (2012)
Processes new to COBIT® 5

Adopted from other frameworks and standards

EDM01 – EDM05  The 5 Governance processes
APO03  Manage Enterprise Architecture
APO04  Manage Innovation
APO05  Manage Portfolio
APO06  Manage Budget and Costs
APO08  Manage Relationships
APO10  Manage Suppliers
APO13  Manage Security
BAI05  Manage Organisational Change Enablement
BAI08  Manage Knowledge
BAI09  Manage Assets
DSS05  Manage Security Service
DSS06  Manage Business Process Controls

Based on COBIT 5 (2012)
What’s in each COBIT® 5 process?

- Process Name, Area (Gov. or Mgt.) and Domain
- Process Description (a paragraph)
- Process Purpose Statement (a paragraph)
- Process Goals and Metrics
- RACI chart
  - For each governance/management practice
  - 26 roles used
- Practices, Inputs, Outputs and Activities
- Related guidance
  - Other frameworks and standards

Based on COBIT 5 (2012)
Governance Practices

E.g. Ensure Benefits Delivery (EDM02)

- **EDM02.01** Evaluate value optimisation
- **EDM02.02** Direct value optimisation
- **EDM02.03** Monitor value optimisation

- Each Governance process has 3 Governance practices
  - Evaluate, Direct and Monitor
- Each Governance practice has between 3 & 8 activities
- Each Governance practice has inputs and outputs

Based on COBIT 5 (2012)
Management Practices

E.g. Manage Service Requests and Incidents (DSS02)

- **DSS02.01** Define incident & service request classification schemes
- **DSS02.02** Record, classify and prioritise requests and incidents
- **DSS02.03** Verify, approve and fulfil service requests
- **DSS02.04** Investigate, diagnose and allocate incidents
- **DSS02.05** Resolve and recover from incidents
- **DSS02.06** Close service requests and incidents
- **DSS02.07** Track status and produce reports

- Each Management practice has between 2 & 13 activities
- Each Management practice has inputs and outputs

Based on COBIT 5 (2012)
COBIT® 5 Process Capability Model

- Replacement for Maturity Models:
  - COBIT®, Val IT™, Risk IT™
- Based on COBIT® 4.1 Process Assessment Model (PAM)
- Which itself is based on ISO/IEC 15504-2:
  - Process Assessment: Performing an assessment

**NB: Processes are only 1 of 7 Enablers**
*Process assessment alone won’t assess IT Governance maturity*
How COBIT® 5 PCM works – 1

Process Capability Levels

0 – Incomplete Process (1 attribute)
Process not implemented or fails to achieve its purpose

1 – Performed Process (1 attribute)
Implemented process achieves its purpose

2 – Managed Process (2 attributes)
Performed process is managed (planned, monitored, adjusted).
Its Work Products are established, controlled, maintained.

3 – Established Process (2 attributes)
Managed process uses a defined process that can achieve outcomes

4 – Predictable Process (2 attributes)
Established process operates within defined limits to meet outcomes

5 – Optimising Process (2 attributes)
Predictable process: continually improved to meet current/projected bus. goals

Based on COBIT 5 (2012)
How COBIT® 5 PCM works – 2

1. Lower level must be achieved else can’t go to next level
2. Significant distinction between Cap. L1 & Cap. L2 - L5
   - Cap. Level 1 requires:
     - Process performance attributes to be largely achieved
     - i.e. process works and outcomes achieved
   - Whereas, Cap. Level 2 – L5 add different attributes to it
   - So, Capacity Level 1 is a Significant Achievement!
# Current & future COBIT® 5 resources

<table>
<thead>
<tr>
<th>Guide type</th>
<th>Title</th>
<th>Publication Date</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framework</td>
<td>COBIT 5: A Business Framework…</td>
<td>10 April 2012</td>
<td>94</td>
</tr>
<tr>
<td>Enabler</td>
<td>COBIT 5: Enabling Processes</td>
<td>10 April 2012</td>
<td>230</td>
</tr>
<tr>
<td>Enabler</td>
<td>COBIT 5: Enabling Information</td>
<td>In development</td>
<td></td>
</tr>
<tr>
<td>Professional</td>
<td>COBIT 5 Implementation</td>
<td>10 April 2012</td>
<td>78</td>
</tr>
<tr>
<td>Professional</td>
<td>COBIT 5 for Information Security</td>
<td>July 2012</td>
<td></td>
</tr>
<tr>
<td>Professional</td>
<td>COBIT 5 for Assurance</td>
<td>In development</td>
<td></td>
</tr>
<tr>
<td>Professional</td>
<td>COBIT 5 for Risk</td>
<td>In development</td>
<td></td>
</tr>
<tr>
<td>Professional</td>
<td>COBIT Assessment Programme ?</td>
<td>C4.1 PAM upgrade?</td>
<td></td>
</tr>
<tr>
<td>Professional</td>
<td>COBIT 5 Online</td>
<td>In planning</td>
<td></td>
</tr>
</tbody>
</table>
Summary
5 key facts about COBIT® 5

1. Leads to more value from information and technology
   - Improved risk management
   - Improved business-IT communication
   - Improved delivery of business objectives
   - Improved business competitiveness and lower costs

2. Is a business framework for GEIT
   - Meets needs of business execs. and IT leaders

3. Provides effective decision making
   - Systematic approach that clarifies goals

4. Addresses needs of stakeholders
   - An end-end framework integrating 80+ other approaches

5. Based on collective wisdom of 95 global experts.
COBIT® integrates…

- ITIL® (ITSM)
- ISO 20000 (ITSM)
- PRINCE2®, PMBOK® (ProjMan)
- ISO 27000 (InfoSec)
- TOGAF® (Enterprise Architecture)
- Basel III (Banking compliance)
- PCI DSS (Data card security standard)
- COSO (Internal and financial controls)
- Sarbanes- Oxley (Financial practice & corporate governance)

Based on COBIT 5 (2012)
COBIT 5: Training Roadmap

- **Foundation**: 6/2012
- **IT Process Level**: 9/2012
  - **Implementation**: 12/2012
  - **Assessor**: 12/2012

All have certificates
Is there a COBIT® 5 competitor?

- Maybe, but not at the level of COBIT®’s user-base
- Nearest that includes governance and management is:
  - IT Capability Maturity Framework (IT-CMF®) V1.0: 2010
  - From Innovation Value Institute (IVI) – consortium of “blue-chips”
  - 4 macro-capabilities = domains
    - Managing IT like a business (13 critical capabilities= processes)
    - Managing the IT Budget (4)
    - Managing the IT Capability (13)
    - Managing IT for Business Value (3)
  - Based on a maturity assessment approach to improvement
  - Qualifications: 5 tiers up to MSc in IT Management available

http://ivi.nuim.ie/itcmf.shtml

Uses 80+ frameworks and standards!
References


ISO 38500 (2008), *Corporate governance of information technology*, Geneva, ISO

IT-CMF (2010), *IT Capability Maturity Framework*, Maynooth, Irish Republic, Innovation Value Institute

Risk IT (2009), *Risk IT Framework*, Rolling Meadows, Illinois, USA, ISACA

Val IT 2.0 (2008), *Val IT V2.0 Framework*, Rolling Meadows, Illinois, USA, ISACA
Any Further Questions?
Education and Consultancy for IT Best Practices

www.maatconsulting.com