COBIT 5 – an Overview with an InfoSec Focus
Michael T Hoesing
CISSP, CISA, CCP, ACDA, CIA, CFSA, CMA, CPA
mhoesing@unomaha.edu
(broke faculty, do not sue me)
Agenda

• Objectives of this version
• Parts n Pieces (it is not all in one place anymore, [was it ever?])
• Compare COBIT 5 to CobiT 4.1 processes
• Drill Down – DS5 Manage Security is now DSS 02 & 05 and APO13 (and is influenced by others)
• COBIT 5 for Information Security
• References, Q n A
Objectives of COBIT 5
COBIT 5 Objectives

• More emphasis on Management and Governance, the 5 principles:
  1) Stakeholder emphasis - benefits, risk, & resource optimization
  2) The whole enterprise end to end (not just IT)
  3) A Single Framework then plug-in the details, (ISO 38500 31000 27000 20000 15504, PCI/DSS, FFIEC, HIPPA, ITIL, TOGAF, PRINCE2, PMBOK....) Appendix E
  4) Holistic (7 enablers)
     ❖ Policies, Principles, Framework
     ❖ Processes
     ❖ Organization Structure
     ❖ Culture, Ethics, Behavior
     ❖ Information
     ❖ Services, Infrastructure, Applications
     ❖ People, Skills, Competencies
  5) Separating Governance from Management
COBIT 5 Objectives (continued)

• Since ValIT is superseded, these documents stress alignment (cascade) of IT goals with the Business goals (appendix B & C & D)
• Distinguishes Management (Plan, Build, Run Monitor) from Governance (Evaluate, Direct, Monitor)
• 37 enabling processes (was 34)
• Implementation (change process) guidance
• 5 level MM follows Carnegie, +level 0 nothing
• CIA + effective & efficient & compliant are now buried in verbiage (Appendix F)
COBIT 5  Evaluating the 7 Enablers

• Appendix G:
  - (Who) Stakeholders
  - (Why) Goals
  - (When) Lifecycle
  - (What) Good Practices
  - (Where) Relationship to Other Enablers

• Add Maturity assessment for a process

• Information (frame work pages 81 – 84)
  a.) physical (storage)  b.) empiric (access)
  c.) syntactic (structure)  d.) sematic (type/value of the information)
  e.) pragmatic (retention, dependencies)  f.) social (context, [i.e. contract vs. good practice])
Part and Pieces of COBIT 5
Parts and Pieces

• Enabling Processes – 234 pages, explains the 37 process categories that used to be the 34 process categories in 4.1 ($135 non-members)
• Framework – 94 pages, explaining the goals background and structure of the new multi component COBIT 5 , ($50 non-members)
• COBIT 5 for Information Security – 220 pages (slides coming up) ($175 non-members)
• Implementation – 78 pages now to deploy COBIT5 ($150 non-members)
Parts and Pieces (continued)

• Enabling Information (not published yet, see slide 6 for an outline)
• Toolkit – mostly power points and PDF’s to “market” COBIT 5 within your organization (14 Laminate pdf has the graphics, slide 12)
• Process Assessment Model – refers to CobiT 4.1
• In Process –
  - COBIT 5 for Risk
  - COBIT 5 for Assurance
  - COBIT Translations (business cases)
  - COBIT 5 Online
Comparing and Contrasting COBIT 4.1 and 5
CobiT 4.1
34 Processes
# Process Groups

<table>
<thead>
<tr>
<th>COBIT 5</th>
<th>CobiT 4.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluate, Direct, Monitor (Governance, RiskIT)</td>
<td>n/a</td>
</tr>
<tr>
<td>Align, Plan , Organize (ValIT)</td>
<td>Plan and Organize</td>
</tr>
<tr>
<td>Build, Acquire, Implement</td>
<td>Acquire and Implement</td>
</tr>
<tr>
<td>Deliver, Service, Support</td>
<td>Deliver &amp; Support</td>
</tr>
<tr>
<td>Monitor, Evaluate, Assess (Management)</td>
<td>Monitor &amp; Evaluate</td>
</tr>
</tbody>
</table>
37 Enabling Processes – “New” (7)

• The new Group, Evaluate, Direct, Monitor (EDM)
  ➢ EDM1, Set a Governance Framework, was in 4.1 as ME 4
  ➢ EDM2, 3, 4, and 5 are new
    Value Optimization
    Risk Optimization
    Resource Optimization
    Stakeholder Transparency

• BAI 2 new Define Requirements, carved out as a specific process, previously part of AI 1

• BAI 8 new Knowledge Management, carved out as a specific process, previously part of PO 7 and referenced in many processes

• (depending on what you read into it)
37 Enabling Processes – “Removed” (2)

- AI 5 Procure IT Resources, part of EDM 4 Resource Optimization
- DS 6 Identify and Allocate Costs, part of EDM 4 Resource Optimization

- (depending on what you read into it)
37 Enabling Processes – “Collapsed” & “Expanded” (2)

• Collapsed (5 -2)
  ➢ IA 1, 2 & 3 Identify Solutions, Acquire Applications, Acquire Infrastructure, now are in BAI 3
  ➢ DS 11 & 12 Physical Environment & manage Data are now mostly are in DSS 2

• Expanded (3 – 4)
  ➢ PO 5 Manage IT Investment, now APO 5 & 6
  ➢ AI 6 Manage Changes, now APO 5 & 6
  ➢ DS 2 Manage Third Parties, now APO 9 & 10

• 34 + 7 -2 - ( 5- 2) + (3 -4) = 37

• (depending on what you read into it)
Drill Down - What Used to be DS5
## Detailed Mapping – 4.1 to 5 Appendix A in COBIT 5

<table>
<thead>
<tr>
<th>CobiT 4.1</th>
<th>Description</th>
<th>COBIT 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS5.1</td>
<td>Management of IT Security</td>
<td>APO13.01; APO13.03</td>
</tr>
<tr>
<td>DS5.2</td>
<td>IT Security Plan</td>
<td>APO13.02</td>
</tr>
<tr>
<td>DS5.3</td>
<td>Identity Management</td>
<td>DSS05.04</td>
</tr>
<tr>
<td>DS5.4</td>
<td>User Account Management</td>
<td>DSS05.04</td>
</tr>
<tr>
<td>DS5.5</td>
<td>Security Testing, Surveillance and Monitoring</td>
<td>DSS05.07</td>
</tr>
<tr>
<td>DS5.6</td>
<td>Security Incident Definition</td>
<td>DSS02.01</td>
</tr>
<tr>
<td>DS5.7</td>
<td>Protection of Security Technology</td>
<td>DSS05.05</td>
</tr>
<tr>
<td>DS5.8</td>
<td>Cryptographic Key Management</td>
<td>DSS05.03</td>
</tr>
<tr>
<td>DS5.9</td>
<td>Malicious Software Prevention, Detection and Correction</td>
<td>DSS05.01</td>
</tr>
<tr>
<td>DS5.10</td>
<td>Network Security</td>
<td>DSS05.02</td>
</tr>
<tr>
<td>DS5.11</td>
<td>Exchange of Sensitive Data</td>
<td>DSS05.02</td>
</tr>
</tbody>
</table>

### COBIT 5
- APO 13 Align, Plan Organize - Manage Security
- DSS 02 Deliver, Service & Support – Manage Security Services
- DSS 05 Deliver, Service & Support – Manage Service Requests & Incidents
DS 5.3 and 5.4 - Are Now DSS 05.04
Identity Management & User Account Management

DS 5.3 Identity Management
1. Users uniquely identifiable
2. Authentication mechanisms.
3. Confirm user access rights
4. Approved by system owner
5. Implemented by the security-responsible person (see APO 07)
6. Use a central repository
7. Deploy cost-effective technical and procedural measures

DS 5.4 User Account Management
1. User account management procedures
2. Approval procedure
3. Rights and obligations relative to access contractually arranged
4. Perform regular management review
5. Segregate and manage privileged user accounts.
6. Perform regular management review of all accounts and related privileges.
7. Users are uniquely identifiable.
   Uniquely identify all information processing activities by user.
8. Maintain an audit trail of access to information classified as highly sensitive.
COBIT 5 For Information Security
COBIT 5 for Information Security

• Section I – COBIT Overview
• Section 2 - Enabling Processes
  ➢ Chapter 1 – Management 101
  ➢ Chapter 2 A – Policy components and life cycle
  ➢ Chapter 3 B – Process Model
  ➢ Chapter 4 C – Organisaztion Model
  ➢ Chapter 5 D – Ethics, Culture, Behavior (COSO)
  ➢ Chapter 6 E – Information (CISO documents and reports) and Stakeholders (ext auditors)
  ➢ Chapter 7 F – Services, Infrastructure, & Applications
  ➢ Chapter 8 G – People Skills Competencies
• Section 3 – Adapting COBIT 5 to the org
COBIT 5 for IS – Appendix F = Services, Infrastructure & Applications

- Provide a security architecture
- Provide security awareness
- Provide secure development
- Provide security assessments
- Provide adequately secured and configured systems
- Provide user access and access rights in line with business requirements
- Provide adequate protection against malware, external attacks and intrusion attempts
- Provide adequate incident response
- Provide security testing
- Provide monitoring and alert services
## F.3 Secure Development

### Description of the Service Capability
Figure 45 describes the service capability for secure development services.

<table>
<thead>
<tr>
<th>Service Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop secure coding practices.</td>
<td>The design and delivery of coding practices, examples and content demonstrating secure coding and development (development of code that can withstand attacks) for a given set of languages and environments</td>
</tr>
<tr>
<td>Develop secure infrastructure libraries.</td>
<td>The design and delivery of language- and environment-specific information security modules that provide essential or critical information security functions</td>
</tr>
</tbody>
</table>

### Attributes
Figure 46 describes attributes for secure development services.

<table>
<thead>
<tr>
<th>Service Capability</th>
<th>Supporting Technology</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop secure coding practices.</td>
<td>• Compilers, linkers &lt;br&gt; • Secure coding resources (books, courses, examples) &lt;br&gt; • Static and binary analysis tools &lt;br&gt; • Code scanners</td>
<td>• Decreased likelihood of vulnerabilities in code &lt;br&gt; • Assistance in conforming with compliance standards</td>
</tr>
<tr>
<td>Develop secure infrastructure libraries.</td>
<td>• Development languages &lt;br&gt; • Secure coding resources (books, courses) &lt;br&gt; • Code scanners &lt;br&gt; • Static and binary analysis tools &lt;br&gt; • Compilers, linkers</td>
<td>• Protection of intellectual property &lt;br&gt; • Decreased likelihood of vulnerabilities in software development</td>
</tr>
</tbody>
</table>

### Goals
Figure 47 describes goals for secure development services.

<table>
<thead>
<tr>
<th>Service Capability</th>
<th>Quality Goal</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop secure coding practices.</td>
<td>Accurate identification of all information risk and resulting business risk/effects to a given asset or entity</td>
<td>Number of new types of risk discovered via incidents not covered in report</td>
</tr>
<tr>
<td>Develop secure infrastructure libraries.</td>
<td>Improvements in information security configuration of systems in alignment with information security requirements</td>
<td>Number of information security issues discovered after an information security assessment of the hardened system</td>
</tr>
</tbody>
</table>
**F.5 Adequately Secured and Configured Systems, Aligned With Security Requirements and Security Architecture**

**Description of the Service Capability**

Figure 51 describes the service capability for adequately secured systems services.

<table>
<thead>
<tr>
<th>Service Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide adequately secured hardened and configured systems, in line with information security requirements and information security architecture.</td>
<td>Provide the information security-related configuration, settings and system hardening to ensure that the information security posture of a given system is based on a set of requirements or architectural designs.</td>
</tr>
<tr>
<td>Provide device information security protection.</td>
<td>Provide device-specific information security measures and activities.</td>
</tr>
<tr>
<td>Provide physical information protection.</td>
<td>Provide adequate, specific information security measures for data and information that exist in non-digital forms, including documents, media, facilities, physical perimeter and transit.</td>
</tr>
</tbody>
</table>
Attributes

Figure 52 describes attributes for adequately secured systems services.

<table>
<thead>
<tr>
<th>Service Capability</th>
<th>Supporting Technology</th>
<th>Benefit</th>
</tr>
</thead>
</table>
| Provide adequately secured hardened and configured systems, in line with information security requirements and information security architecture. | • File Transfer Protocol (FTP)  
• CMOS update methods  
• Signature verification solutions  
• File integrity monitoring  
• Kernel modules  
• Information security requirements and information security architecture  
• System management  
• Patch management  
• Virtualisation management  
• Cloud management | • Reduced unauthorised access to data  
• Reduced external and internal threats  
• Simplified compliance                                                                 |
| Provide device information security protection.                                    | • Device-specific platform OS  
• Platform management console/systems | • Confidentiality in case of theft  
• Prevention of unauthorised access to specific devices  
• More explicit information security for specific devices |
| Provide physical information protection.                                           | • Closed-circuit television (CCTV)  
• Locks  
• Alarms  
• Access control  
• Vaulting  
• Intelligence reports  
• Firstresponder interface  
• Facilities management solutions  
• Fire protection systems  
• Time locks  
• Physical access solutions | Protection of physical assets from external and internal threats |

Goals

Figure 53 describes goals for adequately secured systems services.

<table>
<thead>
<tr>
<th>Service Capability</th>
<th>Quality Goal</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide adequately secured hardened and configured systems, in line with information security requirements and information security architecture.</td>
<td>Improvements in information security configuration of systems in alignment with information security requirements</td>
<td>Number of information security issues discovered after an information security assessment of the hardened system</td>
</tr>
<tr>
<td>Provide device information security protection.</td>
<td>Improvements in information security configuration of device in alignment with information security requirements</td>
<td>Number of information security issues discovered after an information security assessment of the secured device</td>
</tr>
</tbody>
</table>
| Provide physical information protection.                                          | Physical controls in line with information security requirements            | • Number of incidents not discovered by review/assessment  
• Number incidents detected not addressed by existing controls |
References – not whole lot at this time, COBIT 5 released late April 2012, “for Information Security” 6/25/2012

1.) THE source
http://www.isaca.org/COBIT/Pages/default.aspx

2.) most others are announcement articles with lots of glowing quotes from ISACA, no real analysis yet (7/18/2012)
Questions ??

You are not seriously thinking about getting up?

Where would you like the scar?