Frameworks and ISO Standards

Robert Meyer
Senior Systems Engineer, Cincinnati Insurance Companies
robert_meyer@cinfin.com

Session Description

As global commerce and the IT that powers communication and business continue to grow, the frameworks and standards that protect the organization’s stakeholders have become increasingly critical. This session will give you an overview of these frameworks and standards while providing you with the opportunity to explore COBIT 5, CMMI, and ITIL, in addition to ISO management, audit, and process assessment standards. (Experience Level: Advanced)

Speaker Background

Robert Meyer has been a member of itSMF USA for the past eight years, and has served as president of the Ohio Valley LIG since 2015. A highly decorated ITSM professional, Robert is an expert at assessing the relationships between frameworks, including ITIL, COBIT 5, CMMI, and the US federal regulations. Robert also holds ISACA’s Certified Information Systems Auditor credential.
Frameworks and ISO Standards

Robert A. Meyer

Topics

- Value
- Terms
- Relationships
- Framework Publications
- Framework Revisions
- ISO – by the numbers
- ISO Standards
  - Principles
  - Quality Management Principles
  - Audit Standards
  - Process Maturity Standards
- Discussion
Value

• Better value creation through effective and innovative use of enterprise IT.
• Increased business user satisfaction with IT engagement and services
• Increased compliance with relevant laws, regulations and policies
• Improved relationship between business needs and IT objectives
• Increased financial return from the governance over enterprise IT by obtaining the greatest value from investments in technology
• Connection to, and, where relevant, alignment with, other major frameworks and standards in the marketplace

Methodology
Framework

Standard
## Frameworks Publications

<table>
<thead>
<tr>
<th>Publications in Searched Categories</th>
<th>Scholarly Journals</th>
<th>Trade Journals</th>
<th>Dissertations</th>
<th>Books</th>
<th>Government Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>COBIT</td>
<td>133</td>
<td>23</td>
<td>93</td>
<td>157</td>
<td>5</td>
</tr>
<tr>
<td>CMMI</td>
<td>247</td>
<td>93</td>
<td>236</td>
<td>222</td>
<td>83</td>
</tr>
<tr>
<td>ITIL</td>
<td>59</td>
<td>6</td>
<td>71</td>
<td>252</td>
<td>6</td>
</tr>
</tbody>
</table>

## Framework Revision Dates

<table>
<thead>
<tr>
<th>Organizations</th>
<th>Title</th>
<th>Introduced</th>
<th>Prior Updates</th>
<th>Major Revision</th>
<th>Latest Release</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>AXELOS</td>
<td>ITIL</td>
<td>1988</td>
<td>2007</td>
<td>V3</td>
<td>ITILV3r</td>
<td>2011</td>
</tr>
</tbody>
</table>
COBIT 5
A Single Integrated Framework

COBIT 5
Enterprise Enablers
COBIT 5 Governance and Management Key Areas

COBIT 5 Process Reference Model
Summary of the COBIT 5 Process Capability Model

COBIT 5 Implementation Life Cycle

- Programme management (outer ring)
- Change enablement (middle ring)
- Continual improvement life cycle (inner ring)
The Deming Cycle
(Plan, Do, Check, Act)
7-step CSI Define > Measure > Control > Manage>

CMMI – SVCS CAPABILITY MATURITY MODEL INTEGRATION for Services Version 1.3
ISO strategic direction 2016-2020

• Road Maps – published every 5 years

ISO and developing countries

• Three-quarters of ISO members are from developing countries
• Administered at the ISO Central Secretariat (ISO/CS)
• Key Outcome is to support the development or strengthening of the national quality infrastructure
• Benefit – Contribute access to
  • World markets
  • Technical progress
  • Sustainable development
ISO Management Standards

• Quality management standard: ISO 9001:2015 (QMS, ISO 9001)
• Environmental management standard: ISO 14001:2004 (EMS, ISO 14001)
• Food safety management system (FSMS, ISO 22000)
• Energy management system (EnMS, ISO 50001)
• Information Technology Service Management: ISO/IEC 20000-1:2011
• Risk Management Standard: ISO 31000:2009
• Corporate Governance Management Standard: ISO/IEC 38500:2008

ISO 9000 - Quality management

Standards in the ISO 9000 family include:
• ISO 9001:2015 - sets out the requirements of a quality management system
• ISO 9000:2015 - covers the basic concepts and language
• ISO 9004:2009 - focuses on how to make a quality management system more efficient and effective
• ISO 19011:2011 - sets out guidance on internal and external audits of quality management systems.
ISO/IEC 20000 - Information technology -- Service management

• ISO/IEC 20000-1:2011
  • Information technology -- Service management -- Part 1: Service management system requirements
• ISO/IEC 20000-2:2012
  • Information technology -- Service management -- Part 2: Guidance on the application of service management systems
• ISO/IEC 20000-3:2012
  • Information technology -- Service management -- Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1
• ISO/IEC TR 20000-4:2010
  • Information technology -- Service management -- Part 4: Process reference model

ISO/IEC 20000 - Information technology -- Service management

• ISO/IEC TR 20000-5:2013
  • Information technology -- Service management -- Part 5: Exemplar implementation plan for ISO/IEC 20000-1
• ISO/IEC TR 20000-9:2015
  • Information technology -- Service management -- Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services
• ISO/IEC TR 20000-10:2015
  • Information technology -- Service management -- Part 10: Concepts and terminology
• ISO/IEC TR 20000-11:2015
GRC Definitions

**GRC:**

- **Governance** — Exercise of authority; control; government; arrangement.
- **Risk (management)** — Hazard; danger; peril; exposure to loss, injury, or destruction. (The act or art of managing; the manner of treating, directing, carrying on, or using, for a purpose; conduct; administration; guidance; control)
- **Compliance** — The act of complying; a yielding; as to a desire, demand, or proposal; concession; submission

[Webster’s Online Dictionary](https://www.dictionary.com)

Types of Governance

- Different types of governance exist:
  - Corporate governance
  - Project governance
  - Information technology governance
  - Environmental governance
  - Economic and financial governance
Corporate Governance of IT

• ISO/IEC 38500: 2008

• **Corporate governance of information technology**

• 1.1 **Scope**
  • This standard provides guiding principles for directors of organizations (including owners, board members, directors, partners, senior executives, or similar) on the effective, efficient, and acceptable use of Information Technology (IT) within their organizations.
  • This standard applies to the governance of management processes (and decisions) relating to the information and communication services used by an organization. These processes could be controlled by IT specialists within the organization or external service providers, or by business units within the organization.

ISO/IEC 38500: 2015

Corporate governance of information technology

2.1 **Principles**

2.1.1 Principle 1: Responsibility
2.1.2 Principle 2: Strategy
2.1.3 Principle 3: Acquisition
2.1.4 Principle 4: Performance
2.1.5 Principle 5: Conformance
2.1.6 Principle 6: Human Behaviour
ISO/IEC 38500: 2015

Corporate governance of information technology

2.2 Model

Directors should govern IT through three main tasks:

a) Evaluate the current and future use of IT.

b) Direct preparation and implementation of plans and policies to ensure that use of IT meets business objectives.

c) Monitor conformance to policies, and performance against the plans.

Principle defined

- A basic belief, theory or rule that has a major influence on the way in which something is done.
- "Quality management principles" are a set of fundamental beliefs, norms, rules and values that are accepted as true and can be used as a basis for quality management.

- Statement
- Rationale
- Key Benefits
- Actions you can take
Quality management principles

- QMP 1 – Customer focus
- QMP 2 – Leadership
- QMP 3 – Engagement of people
- QMP 4 – Process approach
- QMP 5 – Improvement
- QMP 6 – Evidence-based decision making
- QMP 7 – Relationship management

ISO Audit Standards

- Conformity Assessment
  - ISO / IEC 17021:2011
  - ISO 19011:2011
ISO Process Maturity Standard

• ISO/IEC 15504-3:2004 —
  • Information technology -- Process assessment -- Part 3: Guidance on performing an assessment

• ISO/IEC 15504-4:2004 —
  • Information technology -- Process assessment -- Part 4: Guidance on use for process improvement and process capability determination

Multiple management standards

• Leveraging integration
Conclusion

• Relationships

References

• ISO Homepage - http://www.iso.org/iso/home.html
• ISO Figures - http://www.iso.org/iso/home/about/iso-in-figures.htm
• Strategic Plans
• http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1577
• COBIT 5 A Business Framework for the Governance and Management of Enterprise IT
• SEI Institute Carnegie-Mellon - CMMI for Services, Version 1.3
• Service Strategy 2011 – Best Management Practice
Thank you for attending this session.

Please don’t forget to complete an evaluation for this session!

Evaluation forms can be completed electronically on the FUSION 16 Conference App.