Strategic IT audit

Develop an IT Strategic
IT Assurance Plan
Speaker Biography

Hans Henrik Berthing is Partner at Verifica and Senior Advisor & Associated Professor at Aalborg University. He is specialized in IT Assurance and IT Governance, including risk and control reviews. He is a member of the IT Advisory board for the Danish CPA Association (FSR-Danske Revisorer).

Berthing have helped develop a national & international audit and controls guidelines including Good IT Governance (God IT Skik). He has for the last four years been a CISA instructor. He serves as a speaker and instructor at both the local and international levels, on topics relating to Audit, IT Assurance, IT Governance and risk management. During the past 16 years Berthing has been involved in numerous IT General controls reviews and Third Party Audit Reporting (ISAE 3402) for different clients in size and industry.
• Develop an IT strategic assurance plan
• Use Cobit 4.1 as framework for the IT Assurance plan
• Involve CxO and Board of Directors in IT Governance
• Integrate IT Audit with Financial Audit
• Risk based IT audit in practice
• How can technology facilitate IT audit goals for risk identification and measurement
• Audit Programs based on IT Assurance Framework
Objective

• This course will give the participant a detailed IT Assurance plan and Strategic.
• It will ensure that Business Goals, Objectives and Risks are considered as part of the IT Assurance work.
• Requirement from International Standards of Audit will be highlighted and participants will be able to communicate the IT Audit work to the External Auditor.
• The participant will be able to use tools as part of the planning process and communication with executive management and the Risk and Compliance function.
Hans Henrik Berthing

- 44 year, married with Louise and dad for Dagmar and Johannes
- CPA, CRISC, CGEIT, CISA and CIA
- ISO 9000 Lead Auditor
- IT Audit Director and professional responsible
- 7 Years Financial Audit and 16 Years IT Assurance
- Former President & Vice President ISACA, Denmark Chapter
- Instructor, facilitator and speaker
- Articles and editor of ISACA newsletter
- Senior Advisor & Associated professor Aalborg University
Argumentation

• A huge number of various systems interacting
• Operations, maintenance and change management are difficult
• Systems runs critical business processes
• Realisation of business benefits through SSC
• Data flows are not integrated properly
• Data are not adequately available
• Inadequate Business development and standardisation due to IT investment and infrastructure
Strategic IT audit

Develop an IT Strategic IT Assurance Plan
IT Scoping Road Map

1. Establish drivers for the assurance initiative (clarify through interviews with stakeholders).

2. Document the enterprise architecture for IT (clarify through interviews with key IT staff members).

3. Choose an IT control framework [A] (verify that it responds to minimum criteria).

4. Select the IT process [B] (document and validate the link amongst business goal, IT goal and IT process).

5. Select IT component [B] (record the important activities and resources for the processes selected).


7. Select initial control objectives [B] (leverage control framework mappings).

8. Refine control objectives selection with risk analysis [B] (linking significant threats to applicable vulnerabilities to material impact).

A. Framework Criteria
- A common language for IT activities and key management practices
- Business focus
- Governance expectations
- IT tasks and activities organised into discrete processes
- Consistent with generally accepted IT good practices and corporate governance standards

B. Deciding What Is In
- Select
- Weigh
- Cut off
- Customise

#ISACAEU
IT Audit Plan

Understand the Business

• Identify the Organizations strategies and Business Objectives
• Recognize the risk profile for the Organization
• Assess how the organization structures its business operations
• Comprehend the IT Service support model
Business processes

Strategic processes
- BtB letter process
- BtB parcel process
- International letters and parcels processes
- Private customer process

Core processes
- Business sales process
- Collection process
- Transport process
- Letter sorting process A and B
- Parcel sorting process
- International sorting process
- International supply process

Operational processes
- Private sales process
- Transport process
- Distribution process

Support processes
- HR process
- IT process
- Service process
- Comm. process
- Marketing process
- Logistical optimisation process
Systemlandscape
IT risk for Business

• System failure or breakdowns
• Error in Dataflow or Data
• Access to systems and data
• Complex applications
• Legacy IT infrastructure and applications
IT processes

Management and HR
- Administration, program office & Controlling
- IT Strategy and Action plans
- Methods, models & IT work processes
- Architecture process, system & infrastructure

Infrastructure

IT support processes

Business

IT Main Processes

Development
- Process development
- Development
- Improvement

Operations
- Optimize & forebyggelse
- Incident management
- IT Delivery

Business
## IT Assurance Road Map

### Planning
- Establish the IT assurance universe.
- Select an IT control framework.
- Perform risk-based IT assurance planning.
- Perform high-level assessments.
- Scope and define the high-level objectives for the initiative.

### Scoping
- Business goals
  - IT goals
  - Key IT processes and key IT resources
  - Key control objectives
  - Customised key control objectives

### Executing
- Refine the understanding of the IT assurance subject.
- Refine scope of key control objectives for the IT assurance subject.
- Test the effectiveness of the control design of the key control objectives.
- Alternatively/additionally test the outcome of the key control objectives.
- Document the impact of control weaknesses.
- Develop and communicate overall conclusion and recommendations.

### Assurance Conclusion

---

#ISACAEU
### Overview of three year plan

<table>
<thead>
<tr>
<th>Plan &amp; Organise:</th>
<th>Maturity</th>
<th>Materiality</th>
<th>20x1</th>
<th>20x2</th>
<th>20x3</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO1 Define a Strategic IT plan</td>
<td>2-3</td>
<td>M</td>
<td>R</td>
<td>R</td>
<td>F</td>
</tr>
<tr>
<td>PO2 Define the information architecture</td>
<td>2-3</td>
<td>M</td>
<td>R</td>
<td>R</td>
<td>F</td>
</tr>
<tr>
<td>PO3 Determine technological direction</td>
<td>2</td>
<td>M</td>
<td>F</td>
<td>R</td>
<td>F</td>
</tr>
<tr>
<td>PO4 Define the IT processes, organisation and relationships</td>
<td>3</td>
<td>M</td>
<td>R</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>PO5 Manage the IT investment</td>
<td>3</td>
<td>L</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>PO6 Communicate management aims and direction</td>
<td>2</td>
<td>M</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>PO7 Manage human resources</td>
<td>3-4</td>
<td>M</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>PO8 Manage quality</td>
<td>2-3</td>
<td>M</td>
<td>F</td>
<td>R</td>
<td>F</td>
</tr>
<tr>
<td>PO9 Assess and manage IT risks</td>
<td>2-3</td>
<td>H</td>
<td>R</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>PO10 Manage projects</td>
<td>3</td>
<td>H</td>
<td>R</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>
IT Assurance process

- Refine the understanding of the IT Assurance subject
- Refine scope of key control objectives for the IT assurance subject
- Test the effectiveness of the control design of the key control objectives
- Test the effectiveness of the controls
- Document impact of control weaknesses
IT Audit Plan

Define the IT Assurance Universe
• Analyze the business fundamentals
• Isolate significant applications that sustain the business operations
• Distinguish critical infrastructure for the significant applications
• Appreciate the role of the supporting technologies
• Categorize major projects and initiatives
Audit Universe

- Planning and controlling
- Logistic and production
- Procurement
- Revenue assurance
- Financial Statement Closing
- IT Governance
- Segment accounting
- Affiliates
- Sales contract
- Human Resource

Business
IT Audit Plan

Perform Risk Assessment

• Evaluate business and IT processes to identify Risk
• Assess risks and rank audit subjects using IT risk factors
• Assess risks and rank audit subjects using Business risk factors
# Risk assessment of IT Processes

<table>
<thead>
<tr>
<th>No</th>
<th>What can go wrong/inherent risk</th>
<th>IR</th>
<th>Key control that remedy risk (example)</th>
<th>Control type</th>
<th>Control type</th>
<th>Frequency</th>
<th>CR</th>
<th>Comb IR x CR</th>
<th>IT control objectives</th>
<th>Audit assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Who does what and on the basis of what input?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td><strong>Systems Development &amp; Maintenance Mega Process</strong>&lt;br&gt; - Applies to implementation of new systems, major changes to existing systems, and patches and upgrades to systems software.</td>
<td>H M L</td>
<td>Who does what and on the basis of what input?</td>
<td>DE PR</td>
<td>IM MP</td>
<td>D, W, M, Q, V, AH</td>
<td>H M L</td>
<td>H M L</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td><strong>Implementation &amp; Change Process</strong>&lt;br&gt; - Applies to implementation of new systems, major changes to existing systems, and patches and upgrades to systems software.</td>
<td>M</td>
<td>Systems Development Life Cycle procedures have not been formally documented and communicated.</td>
<td>PR</td>
<td>M</td>
<td>AH</td>
<td>M</td>
<td>M</td>
<td>X</td>
<td>05:359 07:1780</td>
</tr>
<tr>
<td></td>
<td><strong>Project Management procedures have not been formally documented and communicated.</strong></td>
<td>M</td>
<td>Project Management procedures are published and communicated to provide policies, procedures, and standards governing the management of new or modified systems installations. These procedures address, but are not limited to the following <em>(PO 10)</em>&lt;br&gt; - Project initiation <em>(PO 10.1)</em>&lt;br&gt; - Management review and approval requirements <em>(PO 10.2-3)</em>&lt;br&gt; - Scope development and control <em>(PO 10.2)</em>&lt;br&gt; - Team building and management <em>(PO 10.3)</em>&lt;br&gt; - Budget management <em>(PO 10.6-7)</em>&lt;br&gt; - Timeline development and control <em>(PO 10.7)</em></td>
<td>PR</td>
<td>M</td>
<td>AH</td>
<td>M</td>
<td>M</td>
<td>X</td>
<td>05:359 06:444 07:1788, 1780</td>
</tr>
</tbody>
</table>
IT Audit Plan

Form IT Audit Plan

• Choose Audit subjects and group to audit actions
• Establish audit cycle and frequency
• Attach appropriate actions based on management requests or opportunities for advisory
• Confirm the plan with management
## IT audit plan 201x

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Priority</th>
<th>May</th>
<th>June</th>
<th>July</th>
<th>August</th>
<th>September</th>
<th>Q4</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACR</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pre implementation review</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluation of network strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance with ITIL</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portfolio management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review of interfaces</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Baseline for Unix/Oracle</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Development</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QA Reference Group and Business</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blueprint Review</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Advisory for projects</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Outplacement of legacy systems</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Follow up SAP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review SAP basis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>IT procurement</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data center security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review of user administration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Method for Risk Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DRP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Backup and recovery</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedures and guidelines IT security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation for SAP</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review of IT strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAP Portal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
## Management Awareness

<table>
<thead>
<tr>
<th>Importance</th>
<th>Performance</th>
<th>Who Does It?</th>
<th>Who Is Accountable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT</td>
<td>Other</td>
<td>Outside</td>
<td>Do Not Know</td>
</tr>
</tbody>
</table>

### Importance = How important for the organisation on a scale from 1 (not at all) to 5 (very)

### Performance = How well it is done from 1 (very well) to 5 (do not know or badly)

### Formality = Is there a contract, an SLA or a clearly documented procedure (Y, N or ?)

### Audited? = Y, N or ?

### Accountable = Name or ‘do not know’

## COBIT Processes

- **PO1** Define a strategic IT plan.
- **PO10** Manage projects.
- **AI6** Manage changes.
- **DS2** Manage third-party services.
- **DS5** Ensure systems security.
- **ME1** Monitor and evaluate IT performance.
Tactical IT Assurance Strategy
Cobit 4.1

Framework for the IT Assurance Plan
Linking the IT Assurance

Business

IT Processes

Control Objectives

Activity Goals

Audit Guidelines

Control Practices

Key Performance Indicators

Key Goal Indicators

Maturity Models

requirements
information
controlled by
made effective and efficient with
translated into
implemented with

Follow us @ISACANews
#ISACAEU

© 2012 ISACA. All Rights Reserved.
IT Assurance Advice
IT Governance

4 domains -> 34 processes -> 210 control objectives
Maturity Model - Concept

Method of evaluating the organisation,
Rated from a maturity level of non-existent (0) to optimised (5).

Designed as profiles of IT processes
Possible current and target levels.
Facilitated assessments
Motivate improvement.

*The advantage of a maturity model approach is that it is relatively easy for management to place itself on the scale and appreciate what is involved if improved performance is needed.*
# Maturity Model - general

<table>
<thead>
<tr>
<th>General</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Non-existent</td>
<td>0 Non-existent</td>
</tr>
<tr>
<td>1 Initial.</td>
<td>1 Initial/Ad Hoc</td>
</tr>
<tr>
<td>2 Repeatable.</td>
<td>2 Repeatable but Intuitive</td>
</tr>
<tr>
<td>3 Defined.</td>
<td>3. Defined Process</td>
</tr>
<tr>
<td>4 Managed.</td>
<td>4 Managed and Measurable</td>
</tr>
<tr>
<td>5 Optimised</td>
<td>5 Optimised</td>
</tr>
</tbody>
</table>
Self assessment of COBIT Processes

- Maturity of the process
- Risk
- Materiality
- Controls
- Goals
- Awareness and Communication
- Policies, Standards and Procedures
- Tools and Automation
- Skills and Expertise
- Responsibility and Accountability
- Goal Setting and Measurement
Maturity Assessment
Involve Management

CxO and Board of Directors
IT Governance
IT challenges

• Low involvement of management
• 8 EU Directive & SOX
• Formal IT strategy
• Preparation of Business Impact Analysis
• Guidelines for IT Security
• Description of system development life cycle
• Preparation of IT operation manuals
• Lack of or inadequate DRP or recovery
• Inadequate security
• Lack of system documentation
• Lack of procedures for access to systems and data
• Overruns of project budgets
• Increasing of IT TCO
IT Governance life cycle

**Governance Objective**
- Direct
- Create
- Protect
- Execute
- Monitor

**IT Governance Focus Area**
- Strategic Alignment
- Value Delivery
- Risk Management
- Resource Management
- Performance Measurement

**Cobit and Val IT Contribution**
- Business and IT goals
- Outcome and performance metrics
- Performance metrics
- Process framework
- Control objectives
- Management practices
- Maturity models
- Control objectives
- Management practices
- IT balanced scorecard
- Cobit Online benchmarks
- Maturity models
- IT Assurance guide

© 2012 ISACA. All Rights Reserved.

Follow us @ISACANews #ISACAEU
Roles and responsibility

Board

- Strategic Direction

CEO

- Delivery of Strategy

CIO

- Implementation of Strategy

Major/Main Responsibilities

- Accountability
- Performance Measurement
- Risk Management
- Resource Management
IT Management

- Follow up
- Plan & Organise:
  - PO1 Define a Strategic IT plan
  - PO2 Define the information architecture
  - PO3 Determine technological direction
  - PO8 Manage quality
- Acquire & Implement
  - AI1 Identify automated solutions
  - AI2 Acquire and maintain application software
  - AI3 Acquire and maintain technology infrastructure
  - AI4 Enable operation and use
  - AI5 Procure IT resources
- Deliver & Support
  - DS1 Define and manage service levels
  - DS2 Manage third-party services
  - DS8 Manage the service desk and incidents
  - DS12 Manage the physical environment
- Monitor and evaluate
  - ME1 Monitor & evaluate performance
  - ME2 Monitor & evaluate internal control
  - ME3 Ensure regulatory compliance
  - ME4 Provide IT governance
IT Governance

• Strategy
• VAL IT
• COSO / ERM
• IT Risk
• COBIT
• Business oriented
Failure in implementing new complex IT-systems

Implementation of SAP increases the risk for material errors in financial report:
- Data conversion errors
- Systems errors
- Inadequate controls
- Inadequate training of users

Early warning challenges in SAP:
- Fixed assets
- Procurement
- SOD
- IT GC

Increase business risks and financial risks
- SAP CRM
- Sales contracts
- Orders and invoicing
- SAP Portal solution
- SAP HR
- Time planning and salary

Audit work related to SAP and the program
- User rights and SOD
- Compliance
- Data conversion and related controls
- Training plans
- System documentation and users manual
- SAP-Basis and ACR
- QA meeting and QA reference group
- Review of Business Blueprint

First year:
- Review of implemented modules
- ITGC
- Compliance

Second & Third year
- Follow up on first years findings
- Review of new modules
- SAP Transport (Change management)
- QA on HR

© 2012 ISACA. All Rights Reserved.
Complex IT-infrastructure

System failure impact service goal. IT infrastructure are business critical for BUS. Unavailability might impact on financial loss.
- Unable to deliver products
- Delay in Financial Statements
- Non timely management decision reports
Increase business risks and financial risks
- Network interruption
- Virus attack
- Emails
- Hardware/OS failure
- Poor baseline in infrastructure
- SOD
- Lack of application controls

Audit work related to IT infrastructure
- General IT controls based on COBIT
- IT Governance
- Procedures and processes
- Follow up on identified failure

IT assurance strategy:
- Risk Assessment
- Cover Domains in COBIT
- Advisory assignments
Integrate IT Audit with Financial Audit
Assignments

- External Audit Support (ISA 315 og 330)
- Quality Assurance
- Clients seminars, Speaks and education
- Advisory
- External Clients
## IT Assurance and Assurance

<table>
<thead>
<tr>
<th>Stages in the Road Map</th>
<th>Assurance Stages (IAASB)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Planning</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Scoping</strong></td>
<td></td>
</tr>
<tr>
<td>Refine the understanding of the IT assurance subject.</td>
<td>✓</td>
</tr>
<tr>
<td>Refine the scope of key control objectives.</td>
<td>✓</td>
</tr>
<tr>
<td>Test the effectiveness of the control design.</td>
<td></td>
</tr>
<tr>
<td>Test outcomes of key control objectives.</td>
<td>✓</td>
</tr>
<tr>
<td>Document the impact of control weaknesses.</td>
<td>✓</td>
</tr>
<tr>
<td>Develop and communicate the overall conclusion and recommendations.</td>
<td>✓</td>
</tr>
</tbody>
</table>
Internal Controls - COSO
Cobit and Financial Audit

Significant Accounts in the Financial Statements
- Balance Sheet
- Income Statement
- Cash Flow
- Notes
- Other Disclosures

Business Processes/Classes of Transactions
- Process A
- Process B
- Process C

Financial Applications
- Application A
- Application B
- Application C

IT Infrastructure Services
- Database
- Operating System
- Network/Physical

IT General Controls
- § Program development
- § Program changes
- § Program operations
- § Access control
- § Control environment

Application Control Objectives/Assertions
- § Accuracy
- § Completeness
- § Authorization
- § Segregation of duties

© 2012 ISACA. All Rights Reserved. Follow us @ISACANews #ISACAEU
Strategic IT audit

How can technology facilitate
IT Assurance

- COBIT
  - Planning and organize
  - Acquisition and implementing
  - Delivery and support
  - Monitoring and evaluate
- IT Assurance guide
- Process audit standards
Tools

MDS (Methods for Documentation and standards)
• Risk and control matrix
• Audit programs
• Audit report
• Audit papers

Audit work
• SAP GRC for SOD conflicts
• Script for IT infrastructures
• ACL and SAP Direct link for Data analysis
• Microsoft Office
External and professional Standards and guidelines

• ISACA standards and guidelines
• ISACA Audit programs (Oracle, Unix, SAP, CRM)
• ISACA IT assurance guide
• Cobit and VAL IT
• IIA standards and ISA
• COSO
Internal guidelines and standard

- IT security policy including procedures and guidelines based on ISF
- Procedures in systems development (CMMI level 2)
- Procedures in delivery and support based on ITIL
- ISO20000 and ISO9001
- Compliance Manual
Strategic IT audit

Audit Programs based on IT Assurance Framework
The objective of IT Assurance Guide is to provide guidance on how to use COBIT to support a variety of IT assurance activities.
IT Assurance Guide

Detailed guidance for **assurance and IT professionals** to use COBIT

Assurance steps and advice are provided for:
- **Generic controls** that apply to all processes (identified within the COBIT framework)
- **Application controls** (identified within the COBIT framework)
- Specific **process controls** (identified within the COBIT framework)

Assurance steps and guidelines are provided to:
- Test the control design of the control objective
- Test the outcome of the control objective (operational effectiveness)
- Document control weaknesses and their impact
IT Assurance Guide
### Control Objective

**DS1.1 Service Level Management Framework**
Define a framework that provides a formalised service level management process between the customer and service provider. The framework should maintain continuous alignment with business requirements and priorities and facilitate common understanding between the customer and provider(s). The framework should include processes for creating service requirements, service definitions, SLAs, OLAs and funding sources. These attributes should be organised in a service catalogue. The framework should define the organisational structure for service level management, covering the roles, tasks and responsibilities of internal and external service providers and customers.

### Value Drivers

- Clarified IT service responsibilities and IT objectives aligned with business objectives
- Improved communication and understanding between business customers and IT service providers
- Consistency promoted in service levels, service definitions, and service delivery and support

### Risk Drivers

- Gaps between expectations and capabilities, leading to disputes
- Customers and providers not understanding their responsibilities
- Inappropriate priority given to different services provided
- Inefficient and costly operational service

### Test the Control Design

- Inspect SLA policies and procedures for the alignment of SLA objectives and performance measures with business objectives and IT strategy.
- Enquire whether and confirm that policies exist for the alignment of SLA objectives and performance measures with business objectives and IT strategy.
- Inspect the service catalogue and verify that it incorporates service requirements, service definitions, SLAs, OLAs and funding sources.
- Enquire of staff members accountable for SLA escalation and resolution to determine whether the procedures or methods established reasonable service levels in responding to issues.
- Inspect a sample of relevant changes and verify that changes were implemented in accordance with the change management process.
- Inspect the design of the service improvement programme for standards to measure performance.
## Audit instruction

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Audit step</th>
<th>Audit result</th>
<th>Auditor</th>
<th>Reviewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><strong>Service Level Management Framework</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Enquire whether and confirm that a process exists for developing, reviewing and adjusting the service catalogue or portfolio of services.</td>
<td>Formal service level management process, and supporting processes (continuity management, change management, configuration management, incident and problem management etc.).</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>2.2</td>
<td>Confirm the existence of a management process to ensure that the service catalogue or portfolio is available, complete and up to date.</td>
<td>See 2.1. Renegotiation should be done yearly. We have noted that not all reviewed SLA have been renegotiated the last two years.</td>
<td>NN Obs</td>
<td>NN</td>
</tr>
<tr>
<td>2.3</td>
<td>Inspect the service catalogue or portfolio process to verify that it is reviewed on a regular basis.</td>
<td>Se 2.2</td>
<td>NN Obs</td>
<td>NN</td>
</tr>
<tr>
<td></td>
<td>Conclusion</td>
<td>Based on work performed we evaluated the area as Defined (3). Some elements are Managed and Measurable (4).</td>
<td>NN</td>
<td>NN</td>
</tr>
</tbody>
</table>
Reporting and conclusion

3 Defined when
Responsibilities are well defined, but with discretionary authority. The SLA development process is in place with checkpoints for reassessing service levels and customer satisfaction. Services and service levels are defined, documented and agreed-upon using a standard process. Service level shortfalls are identified, but procedures on how to resolve shortfalls are informal. There is a clear linkage between expected service level achievement and the funding provided. Service levels are agreed to, but they may not address business needs.

4 Managed and Measurable when
Service levels are increasingly defined in the system requirements definition phase and incorporated into the design of the application and operational environments. Customer satisfaction is routinely measured and assessed. Performance measures reflect customer needs, rather than IT goals. The measures for assessing service levels are becoming standardised and reflect industry norms. The criteria for defining service levels are based on business criticality and include availability, reliability, performance, growth capacity, user support, continuity planning and security considerations. Root cause analysis is routinely performed when service levels are not met. The reporting process for monitoring service levels is becoming increasingly automated. Operational and financial risks associated with not meeting agreed-upon service levels are defined and clearly understood. A formal system of measurement is instituted and maintained.
Questions
Collaborate – Contribute – Connect

• [http://www.isaca.org/Knowledge-Center](http://www.isaca.org/Knowledge-Center)

• The Knowledge Center is a collection of resources and online communities that connect ISACA members – globally, across industries and by professional focus - under one umbrella. Add or reply to a discussion, post a document or link, connect with other ISACA members, or create a wiki by participating in a community today!