




How to Keep Your Auditor Happy!


Cathy Brown, Executive IT Auditor, BT


 



 

How to Keep Your Auditor Happy

- A look at auditing for the non auditor!
- What makes auditors tick?
- How to be prepared when the audit notice arrives on your desk
- DON'T PANIC!






How to Keep Your Auditor Happy

A bit about me:


Cathy Brown



Worked in BT since 1992, in various roles including Head of Capacity Management and Head of Configuration and Asset Management.

Now working in IARCD as an Executive IT Auditor

ITIL V3 Expert, COBIT Accreditation, Member of the BSI Review Panel for ISO20K



© 2012 iSMF
www.ismf.org.uk

How to Keep Your Auditor Happy

General Perception of an Auditor – fairly negative.

ITSMF UK BCS

BT

© 2012 iSMF
www.ismf.org.uk



ITSMF UK BCS

BT

© 2012 iSMF
www.ismf.org.uk

How to Keep Your Auditor Happy

General Perception of an Auditor – fairly negative.

Clipboards and clicky pens!

Often perceived as a hindrance rather than a positive influence – a call to arms!

ITSMF UK BCS

BT

itsmf UK BCS

Your Battle Plan

- Know Your Enemy
- Be Prepared


© 2011 UK Information Security 2011 BT

itsmf UK BCS

Know Your Enemy

"If you know your enemy and know yourself, you will not be imperilled in a hundred battles"

Sun Tzu – The Art of War



© 2011 UK Information Security 2011 BT

itsmf UK BCS


Know Your Enemy – Who?

There are many different types of auditor:

- Internal Audit
- External Audit
- Certification Bodies
- Quality Audits

This presentation is broadly from the point of view of an internal audit function.

© 2011 UK Information Security 2011 BT

ITSMF UK 


Know your enemy – What?


What is being audited?

Is it regulatory or compliance based, like SOX?
 Are you registering for a certification like ISO20K?
 Best practice audit?
 Quality Audit – ISO9001, LRQA

Process or function?


How do you find out if you are unclear?


BT 

ITSMF UK 

Know your Enemy – How?


- How does auditing work?
 - Notification – the bit you will see first! But that's a way into the standard audit process
 - That notification tells you the objective of the audit but a lot of work will have gone before that

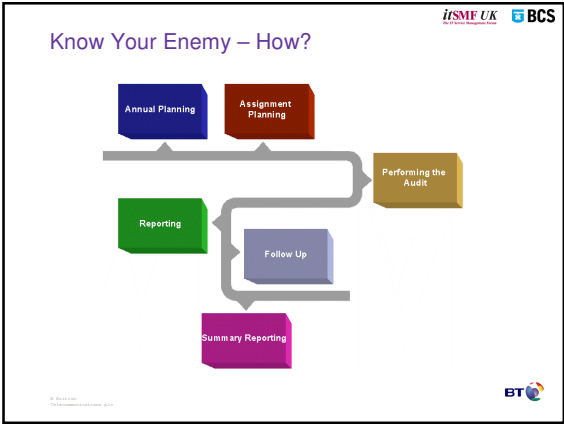
BT 

ITSMF UK 

Risk Based Auditing vs. Other Types

- RBIA – this is dependent on senior management clearly understanding and assessing their risks and the corporate risk appetite.
- Use the risks to drive the audit plan (i.e. Business Dependence on IT Systems)
- Process and Systems Audits
- Combination of the two

BT 



Audit Personalities

- ISTJ – “The Examiner”
 - ISTJs prefer occupations that require thoroughness, accuracy, perseverance, and follow-through. They would rather work in situations in which they can see concrete, tangible results. ISTJs interest in details, justice, practical procedures, and smooth flow of personnel and material is particularly appropriate to audit. They have an acute sense of right and wrong and work hard at preserving established norms and traditions. Because of their deep sense of duty they are dedicated to everything they do and are very dependable.
- ENFP – “The Advocate”
 - ENFPs are introspective, values-oriented, inspiring, social and extremely expressive. They actively send their thoughts and ideas out into the world as a way to bring attention to what they feel to be important, which often has to do with ethics and current events. ENFPs are natural advocates, attracting people to themselves and their cause with excellent people skills, warmth, energy and positivity. ENFPs are described as creative, resourceful, assertive, spontaneous, life-loving, charismatic, passionate and experimental.

What does that mean? It means auditors are people, with different styles and approaches

© 2011 IASB
International Standards on Auditing

BT

Audit Personalities

- Common Traits
 - Pedantic – particularly about grammar...
 - An interest in justice & fairness
 - Honesty and integrity are key values
 - An interest in facts and knowledge

© 2011 IASB
International Standards on Auditing


BT

itsmf UK **BCS**

Be Prepared

"If your enemy is secure at all points, be prepared for him"

Sun Tzu – The Art of War



BT

itsmf UK **BCS**

Be Prepared

What type of thing is an auditor going to look for?

Control points
Process walkthrough
Testing

Understand your own process! A process flow diagram is very useful for this.

Evidence is paramount, an auditor won't take your word for it, they'll want proof.


BT

itsmf UK **BCS**


Cracking the code - What's a control?

- An internal control is a policy, procedure or organisational structure implemented to reduce risk.
- Can be manual or automatic
- They are developed in order to provide reasonable assurance to management that the organisations business objectives will be achieved and that risk events will be prevented, detected and corrected
- Preventative (control physical access), detective (IAD), corrective (contingency planning)

A control objective is the statement of the desired result or purpose to be achieved by implementing control activities – i.e. Ensure Availability of IT Services




BT


ISMF UK 


Cracking the Code - Testing & Evaluation

- General or specialised software
- Flow charting techniques
- Use of audit logs
- Documentation review
- Observation & Interview




- Evaluate change, configuration and release management practices to ensure that changes to the IT environment are adequately controlled.





ISMF UK 

Cracking the Code -Testing

- Substantive Testing – evidence gathered to evaluate the integrity of individual transactions or data
 - Analytical procedures
 - Data verification
- Compliance testing – testing compliance with control procedures
 - Reliability, risk prevention and adherence to organisational policies and procedures
 - Process walkthrough








ISMF UK 

Cracking the Code - Other techniques

- Control Self Assessments – a management technique to assure stakeholders and customers that internal controls are reliable
- CAATS – computer aided audit techniques
- Auditors and key operational staff as best practice consultants/subject matter experts







itsmf UK 

Be Prepared – everything ship shape and squared away!

- Know where your documentation is kept
 - Is it complete, accurate, reviewed?
 - Is it owned appropriately?

- If you are running a project
 - Is it governed correctly?
 - Is there a business case?
 - Are benefits and deliverables clearly defined and tracked?
 - Are risks documented and understood?





itsmf UK 

Be Prepared

- If you're a system owner:
 - Are security standards applied? How do you know?
 - How is access controlled?
 - Can you demonstrate what the system consists of?

- If you're a process owner:
 - Is your process documented?
 - Are you empowered as a process owner?
 - Does the process deliver as expected?
 - Are there checks and controls to confirm that?
 - How do you report on it? How do you know it's working?
 - Have you implemented it? Or is it like this:



itsmf UK 


Controls & Frameworks

- COBIT
 - Control Objectives in IT

- ITIL
 - IT Infrastructure Library

- ISO20K
 - International Standard for IT Service Management

- SOX
 - Sarbanes Oxley



itsmf UK **BCS**

COBIT on Configuration Management

COBIT - Control Objectives for IT

COBIT 4.1, issued by the IT Governance Institute, is an internationally applicable and accepted IT governance and control framework for aligning IT with business objectives, delivering value and managing associated risks. It provides a reference framework for management, users, and IS audit, control and security practitioners. Its guidance enables an enterprise to implement effective governance over the IT that is pervasive and intrinsic throughout the enterprise.

www.isaca.org – COBIT Online

4 Domains:

- Plan and Organise
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

DS9 – Manage the Configuration

BT

itsmf UK **BCS**

COBIT on Configuration Management

9.1 Configuration Repository and Baseline

Establish a supporting tool and a central repository to contain all relevant information on configuration items. Monitor and record all assets and changes to assets. Maintain a baseline of configuration items for every system and service as a checkpoint to which to return after changes.

9.2 Identification and Maintenance of Configuration Items

Establish configuration procedures to support management and logging of all changes to the configuration repository. Integrate these procedures with change management, incident management and problem management procedures.

9.3 Configuration Integrity Review

Periodically review the configuration data to verify and confirm the integrity of the current and historical configuration. Periodically review installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements. Report, act on and correct errors and deviations.

BT

itsmf UK **BCS**

COBIT – DS9

Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimises production issues and resolves issues more quickly.

Control over the IT Process of
Manage the Configuration

that satisfies the business requirement for IT of
optimising the IT infrastructure, resources and capabilities, and accounting for IT assets

by focusing on
establishing and maintaining an accurate and complete repository of asset configuration attributes and baselines, and comparing them against actual asset configuration


is achieved by

- Establishing a central repository of all configuration items
- Identifying configuration items and maintaining them
- Reviewing integrity of configuration data

and is measured by

- Number of business compliance issues caused by improper configuration of assets
- Number of deviations identified between the configuration repository and actual asset configurations
- Percent of licences purchased and not accounted for in the repository


BT


ITSMF UK 

COBIT – DS9 Manage the Configuration

Control Objective DS9.1


Establish a supporting tool and a central repository to contain all relevant information on configuration items. Monitor and record all assets and changes to assets. Maintain a baseline of configuration items for every system and service as a checkpoint to which to return after changes.




ITSMF UK 

COBIT - Value Drivers


- Hardware and software planned effectively to maintain business services
- The configuration is deployed consistently across the enterprise
- Planning is enhanced so that changes are in accordance with the overall architecture
- Cost savings through supplier consolidation
- Fast incident resolution




ITSMF UK 

COBIT - Risk Drivers


- Failure of changes to comply with the overall technology architecture
- Assets not protected properly
- Unauthorised changes to hardware and software not discovered, which could result in security breaches or service impacting failures
- Documented information failing to reflect the current architecture
- Inability to fall back




ITSMF UK 

COBIT – Test the Control Design


- Enquire whether and confirm that senior management sets scope and measures for configuration management functions, and assesses performance.
- Enquire whether and confirm that a tool is in place to enable the effective logging of configuration management information in a repository.
- Determine that access to the tool is restricted to appropriate personnel.
- Review a sample of configuration items to ensure that a unique identifier is assigned.
- Enquire whether and confirm that configuration baselines for components are defined and documented.
- Review that baselines enable identification of system configuration at discrete points in time.
- Enquire whether and confirm that there is a documented process to revert to the baseline configuration.
- Test a sample of systems and applications by verifying that they can be reverted to baseline configurations.
- Enquire whether and confirm that mechanisms exist to monitor changes against the defined repository and baseline.
- Verify that management is receiving regular reports and that these reports result in continuous improvement plans.




ITSMF UK 

ITIL V2 & V3 on Configuration Management

- An auditor can't audit against ITIL specifically, however they can use it as representative of good or best practice
- In ITIL V3 Service Asset & Configuration Management sits in Service Transition.
- Some interesting changes:
 - Service Asset
 - Knowledge Management
 - CMS




ITSMF UK 

ITIL V2 & V3 on Configuration Management

- The **objective of SACM** is to “define and control the components of services and infrastructure and maintain accurate configuration information on the historical, planned and current state of the services and infrastructure”
- You can self audit using online assessments

An internal auditor would be likely to reference ITIL in a recommendation as the 'criteria' that a process was being measured against



itsmf UK **BCS**

ITIL on Configuration Management

Is there a CMS?
 What is its scope?
 How is data controlled?
 How are processes integrated?
 Is there a policy? A process? A plan?
 Does the process cover the whole lifecycle?
 Are the ITIL sub processes in place?
 Is there a link to financial asset management?
 How is the process measured and reported on?

BT

itsmf UK **BCS**

ISO20K on Configuration Management

Objective: To define and control the components of the service and infrastructure and maintain accurate configuration information.

Key elements:
 Integration of change and config processes
 Interface to financial asset accounting process
 A policy covering scope and definitions down to attribute level and including relationships
 Mechanisms for identifying, controlling and tracking versions of identifiable components of the service and infrastructure.
 Configuration control procedures shall ensure that the integrity of systems, services and service components are maintained.
 Integration of release management and config through baselining
 Master copies of digital configuration items shall be controlled in secure libraries and referenced to the configuration records
 All configuration items shall be uniquely identifiable and recorded in a controlled system. Data should be actively managed and verified to ensure its reliability and accuracy.
 Configuration audit procedures shall include recording deficiencies, initiating corrective actions and reporting on the outcome.



BT

itsmf UK **BCS**

ISO20K on Configuration Management

- Part 2 contains more detailed information
- ISO20K undergoing a process of rewrite – an international activity
- Harmonisation with ITIL V3 to keep them in step

BT

ITSMF UK  


SOX & Turnbull on Asset & Configuration Management



The Turnbull guidance was originally published in 1999. In July 2004 the FRC set up a group chaired by Douglas Flint (Group Finance Director, HSBC Holdings plc) to review the guidance and update it where necessary, in the light of experience in implementing the guidance and developments in the UK and internationally since 1999.

- Following the review the FRC published updated guidance in October 2005. It applies to listed companies for financial years beginning on or after 1 January 2006. The revised guidance can be downloaded from this website, and printed copies can be obtained free of charge from CCH Information (tel: 0870 777 2906 or online at www.cch.co.uk).

Section 404 of the US Sarbanes-Oxley Act 2002


- The US Securities and Exchange Commission (SEC) has identified the Turnbull guidance as a suitable framework for complying with US requirements to report on internal controls over financial reporting, as set out in Section 404 of the Sarbanes-Oxley Act 2002 and related SEC rules.
- The FRC published on December 2004 a guide for UK and Irish companies registered with the SEC on the use of the Turnbull guidance for these purposes





ITSMF UK  

SOX on Asset & Configuration Management


- Control Objective**—Controls provide reasonable assurance that all IT components, as they relate to security, processing and availability, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.
- Rationale**—Configuration management ensures that security, availability and processing integrity controls are set up in the system and maintained through its life cycle. Insufficient configuration controls can lead to security and availability exposures that may permit unauthorized access to systems and data and impact financial reporting.
- Inventory process and a fixed assets process also apply – very dependent on how your organisation is managing SOX



ITSMF UK  

How do these things fit together?

- Harmonisation of standards
- Mapping activities
 - COBIT/ITIL/BS17799 (ISO27001)
 - COBIT/CMMI/TOGAF/Prince2
 - SOX loosely based on COBIT (ITGI/COSO)



itsmf UK BCS

Dealing with the Aftermath

- Reports & recommendations
- Manage as a project if you can – clear milestones are useful. Audit will follow up in many circumstances.
- Not up to audit to tell you what to do – you are the experts! Audit will identify a control weakness, you establish the best way to fix it. We are checking that you are checking...
- Senior Management focus, at least for a while!

BT

itsmf UK BCS

Shell Shock

- Audit Fatigue
 - Across a large corporate audit activity will be taking place in a number of areas


What can you do?

With a basic knowledge of control points and objectives you can ensure your process reflects good practice. Most of the frameworks and guidelines are complimentary. Look at your process holistically, rather than in the light of just one of these frameworks or standards

BT


itsmf UK BCS

When Auditors go bad...



- Enron/Arthur Anderson – Accounting Scandals
 - Audit – impartiality and independent challenge is key
 - The goal is to progress the company objectives, however if impartiality is lost then audit is no longer functional
 - Applies at individual level and at corporate level
- Integrity is paramount – a bad spot for audit recently was the scandal surrounding the head of the National Audit Office...
- Who watches the watchmen?


BT


iSMF UK 

The Audit Equivalent of the Geneva Convention?


- The Audit Charter
 - Ethics and standards
 - ISACA & the IIA
 - What we can and can't do
 - Peer Review
 - External Auditors
 - CISA and other qualifications

- Corporate Governance
 - BAC
 - Line to Chairman

BT 

iSMF UK 

Collaborators





- Whistle blowing
 - World Com - Cynthia Cooper

 - Collusion between employees is a big risk as it's so hard to identify

 - Most companies run some type of anonymous whistleblower line into the security department

 - It's not 'telling tales' – it's being a decent corporate citizen


BT 

iSMF UK 

What Happens if you Ignore Your Auditors?


- Break down of respect for the audit function, or ineffective use of internal or external auditors can lead to:
 - Breaking of regulations (involving fines or prison)
 - Endemic and entrenched fraud
 - Poor operational management

 - Look at the bigger picture – other areas are being audited too, such as HR, Finance – this is all good for you as an employee. Even in a small company.

BT 


Make Peace not War!

itsmf UK *BCS*




- The auditor is your friend!!!
- Or has the same goals at least
 - Progressing the strategic goals of the company.
 - Keeping the company on the right side of the law.
 - Ensure risk is understood and managed
- Audit can help you
 - Be honest and straightforward
 - Remember, ownership will sit at senior management level, which tends to focus their attention

© 2011 IASB




Make Peace not War!

itsmf UK *BCS*



- Maintain a dialogue, or request audit input at early stages of projects
- Remember, a successful audit function will be dynamic and able to adapt to changing business needs and risks
- And much as we might like you to think it, we can't actually read minds...

© 2011 IASB



itsmf UK *BCS*



BT

Bringing it all together

© 2011 IASB