www.ITSec.org.za

Your IT Audit and Information Security Partner

CISA Exam Preparation June 2015

Session 10 : 12 May 2015

Starting around 4:45pm …..

Agenda

- Introductions
- Facilitator
- Participants

- Recap on prep expected and provisional schedule

- Overview of Chapter 5

- Challenges, Questions and answers

- Next Week

- Questions And contacts

Note : Resources : Additional slide on Frequently Avoided Questions!

Introductions

- Facilitator
- Justin Williams B.Com, B.Compt (Hons), CA(SA), MBA, CISSP, CGEIT, CRISC, CISA
- 1st in the World, CISA Dec 2014
- Director at ITSec
- Previously Head of Risk, Security, Governance and Compliance for Transnet Group

- Participants
- Name
- How was the Chapter
- What was your most challenging activity of the week?

- ***Raniel Misra : Auditor General of South Africa***

Recap:Prep for Wk 1 of Ch5 (12/4/2015)

- What you need to do
- Read as much of Chapter 5 as you can **(69 pages)**
- Make notes of things you don’t quite understand
- Do the sample questions (at least 20)
- Flag those you get wrong, even if you know why you got them wrong
- Arrive on time (4:45pm Tuesday 12/5/2015)
- At ITSec offices, Forest Office 6, 15 Summit Drive, Sherwood, Durban
- Broadcast live on Google Hangout on Air (check j-j.co.za for link)

- Re-assess
- See how things are going
- See how all doing with the time commitment
- Decide if continue with two weeks per chapter or cover some chapters in one week

Provisional Schedule

10-Mar-15	Introduction (Complete)
17-Mar-15	Chapter 1 The Process of Auditing Information Systems
24-Mar-15	Chapter 1
31-Mar-15	Chapter 2 Governance and Management of IT
07-Apr-15	Chapter 2
14-Apr-15	Chapter 3 Information Systems Acquisition, Development and Implementation
21-Apr-15	Chapter 3
28-Apr-15	Chapter 4 Information Systems Operations, Maintenance and Support
02-May-15	Additional Study revision session : Review of questions from 1st 4 Chapters
05-May-15	Chapter 4 (Raniel Misra)
12-May-15	Chapter 5 Protection of Information Assets (Raniel Misra)
19-May-15	Chapter 5 (Justin)
26-May-15	Exam Techniques + Revision
02-Jun-15	Sample Exam
06-Jun-15	Additional Study revision session : Review of questions from 1st 4 Chapters
09-Jun-15	Final Exam Techniques
13-Jun-15	Exam Date

As Requested

Chapter 5:

Protection of Information Assets

Dom	*Description*	*%*	*Start*	*End*	*Pages*	*Marks/Page*
1	The Process of Auditing Information Systems	14%	29	62	33	0,42
2	Governance and Management of IT	14%	78	124	46	0,30
3	Information Systems Acquisition, Development and Implementation	19%	141	219	78	0,24
4	Information Systems Operations, Maintenance and Support	23%	234	290	56	0,41
5	Protection of Information Assets	30%	306	375	69	0,43

Extra material : OSI Model

How Packets Travel in Network (3D Animation)
www.youtube.com/watch?v=xIuBmOufbls

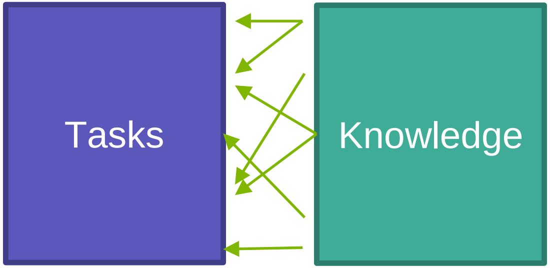
Living in an OSI World – OSI Explained
www.youtube.com/watch?v=-aBgyi5YUbU

Chapter 5 Overview
Protection of Information Assets

- 5 Task Statements

5.1 Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices.
5.2 Evaluate the design, implementation and monitoring of system and logical security controls to verify the confidentiality, integrity and availability of information.
5.3 Evaluate the design, implementation, and monitoring of the data classification processes and procedures for alignment with the organization’s policies, standards, procedures, and applicable external requirements.
5.4 Evaluate the design, implementation and monitoring of physical access and environmental controls to determine whether information assets are adequately safeguarded.
5.5 Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets (e.g., backup media, offsite storage, hard copy/print data, and softcopy media) to determine whether information assets are adequately safeguarded.

- ***Group discussion***



Chapter 5 Overview
Protection of Information Assets

- 21 Knowledge Statements : Knowledge of …

5.1 the techniques for the design, implementation, and monitoring of security controls, including security awareness programs

5.2 processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)

5.3 logical access controls for the identification, authentication and restriction of users to authorized functions and data

5.4 the security controls related to hardware, system software (e.g., applications, operating systems), and database management systems.

5.5 risks and controls associated with virtualization of systems

5.6 the configuration, implementation, operation and maintenance of network security controls

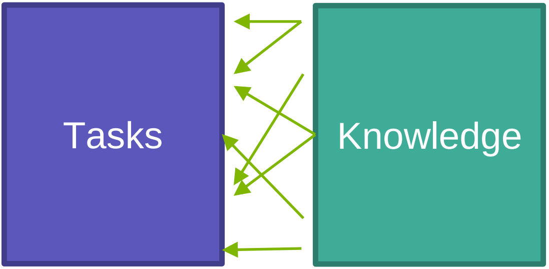
5.7 network and Internet security devices, protocols, and techniques

5.8 information system attack methods and techniques

5.9 detection tools and control techniques (e.g., malware, virus detection, spyware)

5.10 security testing techniques (e.g., intrusion testing, social engineering testing, vulnerability scanning)

5.11 risks and controls associated with data leakage

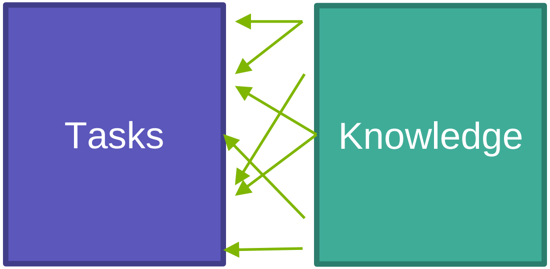


Chapter 5 Overview
Protection of Information Assets

- 21 Knowledge Statements cont. : Knowledge of …

5.12 encryption related techniques
5.13 public key infrastructure (PKI) components and digital signature techniques
5.14 risks and controls associated with peer-to-peer computing, instant messaging, and web-based technologies (e.g., social networking, message boards, blogs)
5.15 controls and risks associated with the use of mobile & wireless devices
5.16 voice communications security (e.g., PBX, VoIP)
5.17 the evidence preservation techniques and processes followed in forensics investigations (e.g., IT, process, chain of custody, fraud evidence collection)
5.18 data classification standards and supporting procedures
5.19 physical access controls for the identification, authentication and restriction of users to authorized facilities
5.20 environmental protection devices and supporting practices
5.21 the processes and procedures used to store, retrieve, transport and dispose of confidential information assets

Group discussion



Chapter 5 Overview
Protection of Information Assets

- 5.2 Importance Of Information Security Management
  - Key Elements Of Information Security Management: Information Security Management System
  - Information Security Management Roles and Responsibilities
  - Inventory and Classification of Information Assets
  - System Access Permissions
  - Mandatory and Discretionary Access Controls
  - Privacy Management Issues and the Role of IS Auditors
  - Critical Success Factors to Information Security Management
  - Information Security and External Parties: Identification of Risks Related to External Parties, Addressing Security When Dealing With Customers, Addressing Security in Third-party Agreements
  - Human Resources Security and Third Parties : Screening, Terms and Conditions of Employment, During Employment, Termination or Change of Employment, Removal of Access Rights.
  - Computer Crime Issues and Exposures: Peer-to-peer Computing, Instant Messaging, Data Leakage and Web-based Technologies (e.g., Social Networking, Message Boards, Blogs)
  - Security Incident Handling and Response

Chapter 5 Overview
Protection of Information Assets

- 5.3 Logical Access
  - Logical Access Exposures
  - Familiarization With the IT Environment
  - Paths of Logical Access: General Points of Entry
  - Logical Access Control Software
  - Identification and Logon IDs and Passwords: Token Devices, One-time Passwords, Biometrics, Single Sign-on
  - Authorization Issues : Access Control Lists, Logical Access Security Administration, Remote Access Security, Remote Access Using Mobile Devices, Access Issues With Mobile Technology, Audit Logging in Monitoring System Access, Naming Conventions for Logical Access Controls
  - Storing, Retrieving, Transporting and Disposing of Confidential Information: Preserving Information During Shipment or Storage, Media-specific Storage Precautions.

- 5.4 Network Infrastructure Support
  - LAN Security : LAN Risks and Issues, Virtualization, Dial-up Access Controls
  - Client-server Security : Client-server Risks and Issues
  - Wireless Security Threats and Risk Mitigation ..
  - Internet Threats and Security: Network Security Threats, Passive Attacks, Active Attacks, Causal Factors for Internet Attacks, Internet Security Controls, Firewall Security Systems, Firewall General Features, Firewall Types, Examples of Firewall Implementations, Firewall Issues, Firewall Platforms, Intrusion Detection Systems, Intrusion Prevention Systems, Honeypots and Honeynets.

Chapter 5 Overview
Protection of Information Assets

- 5.4 Network Infrastructure Support …
  - Encryption: Key Elements of Encryption Systems, Symmetric Key Cryptographic Systems, Public (Asymmetric) Key Cryptographic Systems, Elliptical Curve Cryptography, Quantum Cryptography, Advanced Encryption Standard, Digital Signatures, Digital Envelope, Public Key Infrastructure, Applications of Cryptographic Systems, Encryption Risks and Password Protection.
  - Malware: Virus and Worm Controls, Management Procedural Controls, Technical Controls, Anti-malware Software Implementation Strategies
  - Voice-over IP : VoIP Security Issues
  - Private Branch Exchange: PBX Risks, PBX Audit, PBX System Features, PBX System Attacks, Hardware Wiretapping, Hardware Conferencing, Remote Access, Maintenance, Special Manufacturer's Features, Manufacturer's Development and Test Features, Software Loading and Update Tampering, Crash-restart Attacks, Passwords.

Chapter 5 Overview

Protection of Information Assets

- 5.5 Auditing Information Security Management Framework
  - Auditing Information Security Management Framework: Reviewing Written Policies, Procedures and Standards, Logical Access Security Policies, Formal Security Awareness and Training, Data Ownership, Data Owners, Data Custodians, Security Administrator, New IT Users, Data Users, Documented Authorizations, Terminated Employee Access, Security Baselines, Access Standards
  - Auditing Logical Access: Familiarization With the IT Environment, Assessing and Documenting the Access Paths, Interviewing Systems Personnel, Reviewing Reports From Access Control Software, Reviewing Application Systems Operations Manual
  - Techniques for Testing Security: Terminal Cards and Keys, Terminal Identification, Logon IDs and Passwords, Controls Over Production Resources, Logging and Reporting of Computer Access Violations, Follow-up Access Violations, Bypassing Security and Compensating Controls, Review Access Controls and Password Administration
  - Investigation Techniques: Investigation of Computer Crime, Computer Forensics, Protection of Evidence and Chain of Custody.

Chapter 5 Overview
Protection of Information Assets

- 5.6 Auditing Network Infrastructure Security
  - Auditing Remote Access: Auditing Internet Points of Presence, Full Network Assessment Reviews, Development and Authorization of Network Changes, Unauthorized Changes

- 5.7 Environmental Exposures and Controls
  - Environmental Issues and Exposures
  - Controls for Environmental Exposures : Alarm Control Panels, Water Detectors, Handheld Fire Extinguishers, Manual Fire Alarms, Smoke Detectors, Fire Suppression Systems, Strategically Locating the Computer Room, Regular Inspection by Fire Department, Fireproof Walls, Floors and Ceilings of the Computer Room, Electrical Surge Protectors, Uninterruptible Power Supply/Generator, Emergency Power-off Switch, Power Leads From Two Substations, Wiring Placed in Electrical Panels and Conduit, Inhibited Activities Within the IPF, Fire-resistant Office Materials, Documented and Tested Emergency Evacuation Plans
  - Auditing Environmental Controls: Water and Smoke Detectors, Handheld Fire Extinguishers, Fire Suppression Systems, Regular Inspection by Fire Department, Electrical Surge Protectors, Power Leads From Two Substations, Fully Documented and Tested Business Continuity Plan, Wiring Placed in Electrical Panels and Conduit, UPS/Generator, Documented and Tested Emergency Evacuation Plans, Humidity/Temperature Control,

Chapter 5 Overview
Protection of Information Assets

- 5.8 Physical Access Exposures and Controls
  - Physical Access Issues and Exposures : Physical Access Exposures, Possible Perpetrators
  - Physical Access Controls
  - Auditing Physical Access
- 5.9 Mobile Computing
- 5.10 Case Studies

Chapter 5 Challenges

- Specific issues raised by participants on Chapter 5

Questions and Answers

- Which questions did the participants cover in the week?
- Which ones did you get wrong, lets discuss

Prep for Week 2 of Chap 5 (19/5/2015)

- What you need to do
- Read the balance of Chapter 5 **(69 pages)**
- Make notes of things you don’t quite understand
- Do the sample questions (at least 20)
- Flag those you get wrong, even if you know why you got them wrong
- Arrive on time (4:45pm Tuesday 19/5/2015)
- At ITSec offices, Forest Office 6, 15 Summit Drive, Sherwood, Durban
- Broadcast live on Google Hangout on Air (check j-j.co.za for link)

- Re-assess
- See how things are going

Questions and Contacts

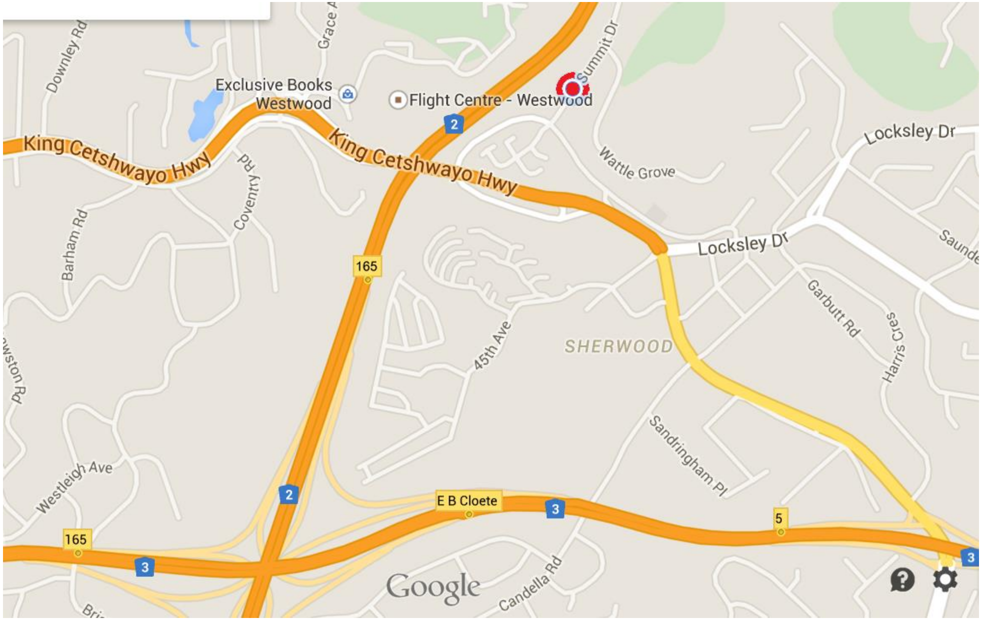
Questions ?

Justin Williams
jwilliams@itsec.org.za or Justin.j.Williams@gmail.com
+27 82 772 9881 or +27 83 279 0998
@itsecza @jjza

Copies of slides :
www.j-j.co.za
www.itsec.org.za

Location of ITSec

Forest Office 6
15 Summit Drive
Sherwood
Durban



Extra material

Study Materials

ISACA has prepared a variety of study resources in various languages to fully prepare for your CISA Exam. These include primary references, publications, articles, the ISACA Journal and other links.

Online Learning

ISACA eLearning Campus offers a variety of online learning courses for certification exam preparation and continuing professional education.

Review Courses

ISACA chapters in numerous countries offer CISA Review courses. View the Review Course list to determine if there is a course in your area, or contact your local chapter for additional courses. There will be courses in Durban, CapeTown & Jhb if demand exists.

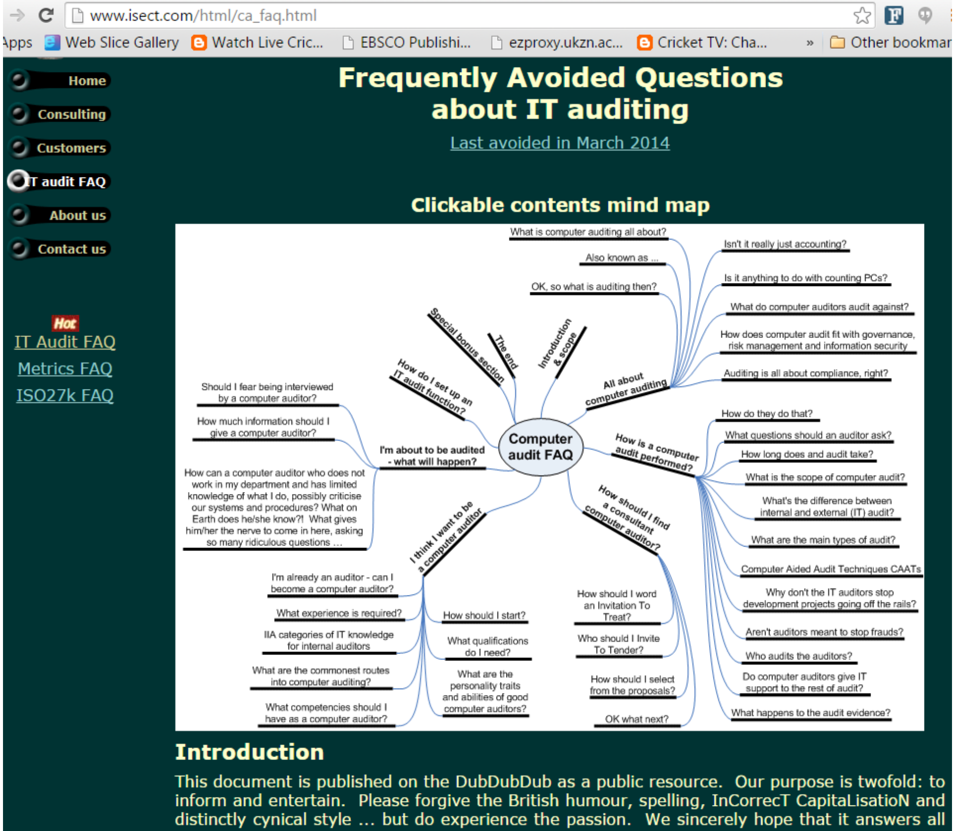
Exam Preparation Community

ISACA created the CISA exam preparation community as a place for current CISA exam registrants to collaborate and study with other registrants within the ISACA environment.

Free online CISA Course

Cybrary has just launched a CISA online course, its free http://www.cybrary.it/

Extra material : FAQ IT Audit


www.isect.com/html/ca_faq.html

IT Audit FAQ

Metrics FAQ

ISO27k FAQ

Frequently Avoided Questions about IT auditing

Last avoided in March 2014

Clickable contents mind map

Computer audit FAQ

Introduction & scope

All about computer auditing
- What is computer auditing all about?
- Also known as ...
- OK, so what is auditing then?
- Isn't it really just accounting?
- Is it anything to do with counting PCs?
- What do computer auditors audit against?
- How does computer audit fit with governance, risk management and information security
- Auditing is all about compliance, right?

How is a computer audit performed?
- How do they do that?
- What questions should an auditor ask?
- How long does and audit take?
- What is the scope of computer audit?
- What's the difference between internal and external (IT) audit?
- What are the main types of audit?
- Computer Aided Audit Techniques CAATs
- Why don't the IT auditors stop development projects going off the rails?
- Aren't auditors meant to stop frauds?
- Who audits the auditors?
- Do computer auditors give IT support to the rest of audit?
- What happens to the audit evidence?

How should I find a consultant computer auditor?
- How should I word an Invitation To Treat?
- Who should I Invite To Tender?
- How should I select from the proposals?
- OK what next?

I think I want to be a computer auditor
- I'm already an auditor - can I become a computer auditor?
- What experience is required?
- IIA categories of IT knowledge for internal auditors
- What are the commonest routes into computer auditing?
- What competencies should I have as a computer auditor?
- How should I start?
- What qualifications do I need?
- What are the personality traits and abilities of good computer auditors?

I'm about to be audited - what will happen?
- Should I fear being interviewed by a computer auditor?
- How much information should I give a computer auditor?
- How can a computer auditor who does not work in my department and has limited knowledge of what I do, possibly criticise our systems and procedures? What on Earth does he/she know?! What gives him/her the nerve to come in here, asking so many ridiculous questions ...

How do I set up an IT audit function?

Special bonus section

The end

Introduction

This document is published on the DubDubDub as a public resource. Our purpose is twofold: to inform and entertain. Please forgive the British humour, spelling, InCorrecT CapitaLisatioN and distinctly cynical style ... but do experience the passion. We sincerely hope that it answers all

A comprehensive, honest, fresh and rather amusing overview of IT Audit

Worth a read

http://www.isect.com/html/ca_faq.html

CISA Practice Tests (free)

One of the free resources that we make available at AuditScripts.com is a database of free ISACA CISA exam questions. Many auditors use the CISA as a way to validate their information systems audit skills. Many consider the CISA certification an entry point or requirement for anyone in the IS audit field. Because so many people in the AuditScripts community value this certification we created a database of 900 exam questions to help students prepare for the exam. We hope that these questions will help students properly prepare for the exam.

CISA Exam Prep Questions – Chapter #1 (100 Questions Available)
CISA Exam Prep Questions – Chapter #2 (150 Questions Available)
CISA Exam Prep Questions – Chapter #3 (250 Questions Available)
CISA Exam Prep Questions – Chapter #4 (150 Questions Available)
CISA Exam Prep Questions – Chapter #5 (250 Questions Available)

CISA Exam Prep Questions – Complete Exam (900 Questions Available)

http://www.auditscripts.com/free-resources/cisa-practice-tests/

Caution : These are not official ISACA practice questions, use them for additional practice when you have exhausted all of the official ISACA questions you have access to