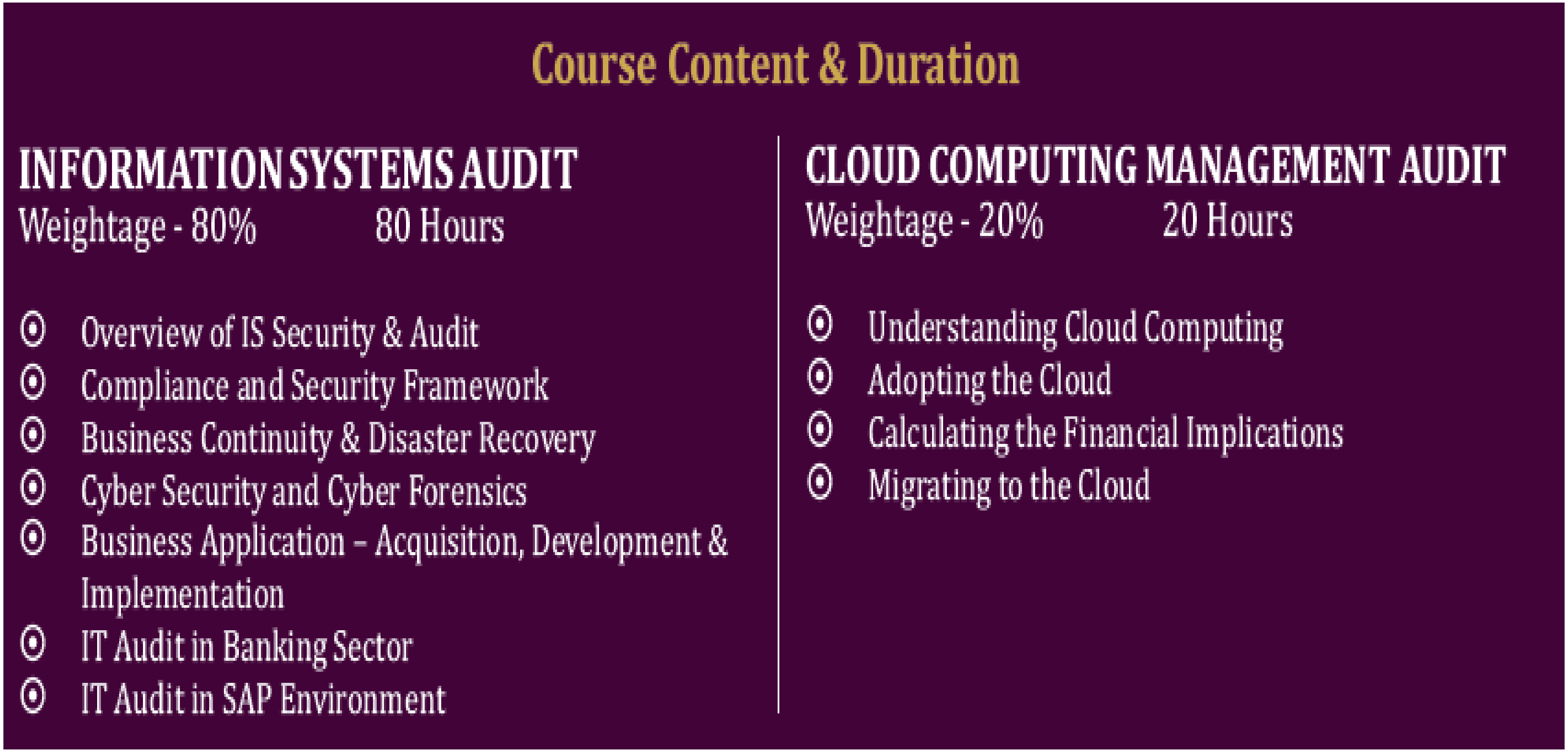
Introduction to DISSA & Information System Security & Audit

(Chapter -1 : DISSA Course)

Arijit Chakraborty

19.12.2021

DISSA : course overview



Course Content & Duration

INFORMATION SYSTEMS AUDIT

Weightage - 80%   80 Hours

- Overview of IS Security & Audit
- Compliance and Security Framework
- Business Continuity & Disaster Recovery
- Cyber Security and Cyber Forensics
- Business Application – Acquisition, Development & Implementation
- IT Audit in Banking Sector
- IT Audit in SAP Environment

CLOUD COMPUTING MANAGEMENT AUDIT

Weightage - 20%   20 Hours

- Understanding Cloud Computing
- Adopting the Cloud
- Calculating the Financial Implications
- Migrating to the Cloud

Module 1

- **Part I: Overview of IS Security & Audit**
- Need for IS Audit
- Key drivers for IS & Security controls
- IT Governance, Security Policies and Control
- IT Organisation & Delivery Models
- DevOps
- Risk Assessment, Risk based audit planning
- Applicable Audit Standards
- Pillars of Information Security
- Confidentiality, Integrity, Availability
- ISO / IEC 38500 : IT Governance
- Control & Audit Perspective on each of the above topics

Module 2 =

- **Part II: Compliance & Security Framework**
- PCI DSS
- NIST Privacy Framework
- ISO 27001 Domains
- COBIT Framework, Maturity Model(CMMI)
- GDPR – EU , Key provisions & challenges
- Personal Data Protection bill (Draft) & Developments : (2020 -2021)
- Information Technology Act, 2008
- IT Act Amendment,
- IT Intermediary Rules & Ethics Guidelines 2021
- ISO / IEC 27018, 27701, 29100 = PII , PIMS
- *Cryptocurrency Bill , CBDC (if released)*

Module 3

- **Part III: Business Continuity & Disaster Recovery**
- Business Continuity Management
- ISO / IEC 22301
- Developing a Business Continuity Plan
- Testing Methodology and Checklist-Data communication
- Backups-Vital Records/ Documentation
- IS Audit checklists & reviews

Module 4

- **Part IV: Cyber Security & Cyber Forensics**
- Understanding Network Communication
- Network types – bus, ring etc
- IT Hardware – Cables , router, switch , server
- Network Component and Security
- TCP/IP
- Demilitarized Zones (DMZ)
- Common Cyber Attacks
- Vulnerability and Threat Analysis
- Cryptography and Steganography
- Digital Evidence
- Ethical Hacking- concept, process, tools & techniques
- CEH – roles & opportunities

Module 5

- **Part V: Business Application-Acquisition, Development & Implementation**
- Components of Business Application
- Hardware/ Application Acquisition, Business Application Development
- Business Application Implementation/ Post-Implementation
- Application Control – Input, Process, Output
- IS Audit Teport – complete granular analysis & practical cases
- Data Analytics, CAAT
- Understanding Emerging Technologies:
- Block chain & DLT, Cryptocurrency & BTC – operation & process
- RPA,
- AI – DL, ML
- IoT,
- ISS Audit aspects , control checklists & Reporting

Module 6

- **Part VI: IT Audit In Banking Sector**
- Core Banking System- concept, types, operation
- Payment Application – SWIFT, RTGS, IMPS, NEFT, NSS
- Debit/Credit Card, BankNet
- Digital Banking Channel – Phone Banking, Mobile Banking, Net Banking, ATM, Anywhere Banking, Mobile Wallet
- RBI regulation for system security
- IS Audit in CBS Environment – step by step analysis (Finacle code)
- **Part VII: IT Audit In SAP Environment**
- SAP Basics, Modules, Integration, Technology
- Roles & Authorisation
- SAP Change Management
- SAP Tables, SAP GRC,
- Outline of SAP S/4 HANA (On premise & Cloud)

Cloud Computing , 20 hrs

- **Part VIII: Understanding Cloud Computing System**
- Characteristics of Cloud Computing, Types of Cloud Computing
- Cloud Service Models, Major CSP
- Benefit and Risks in Cloud Computing
- **Part IX: Adopting the Cloud**
- Key Drivers of Cloud Computing Solutions, Instantaneous provisioning of computing resources
- Tapping into an infinite storage capacity
- Cost- effective pay-as-you-use billing models, Evaluating barriers to Cloud Computing
- Handling sensitive Data-Aspects of Cloud Security
- Assessing Governance Solutions
- **Part X: Calculating the Financial Implications**
- Comparing in-house facilities to the Cloud, Estimating Economic Factors Downstream
- Preserving Business Continuity, Selecting appropriate Service
- Service Level Agreements, Safeguarding access to Assets in the Cloud
- Security availability and Disaster Recovery Strategies
- **Part XI: Migrating to the Cloud**
- Technical Considerations, Re-architecting Application for the Cloud
- Integrating the Cloud with existing Applications
- Avoiding Vendor lock-in-Planning the migration and selecting a Vendor

DISSA Course Pedagogy & Coverage:

- Familiarisation with Technical terms of ISS Audit (handout will be emailed to BoASR for circulation)
- In-class Module specific discussions (Live online)
- Session approach & coverage aligned with Institute’s hi-quality Background Materials
- Additional real-life case studies
- Applicable Standards (COBIT, ISO/ IEC)
- Discussions of relevant ISS audit checklists

DISSA = Enabler

- Digital India Mission
- Higher Outlay in Union Budget
- Higher corporate capex for IT interventions
- E-commerce : stupendous rise
- RBI : 16.4 Cr digital payments , INR 6 Lakh Cr value
- RTGS, NEFT, IMPS – UPI payment gateways
- CERT-In : Increasing oversight

Emergence & importance= DISSA

- Enterprise Resource Planning (ERP) enabled organisation- data integrity
- Robotic Process Automation (RPA), Artificial Intelligence (AI) , Big Data & DA , Cloud Computing (adopting & migration)
- Cyber-threats
- India = Data Privacy Bill (GDPR)
- Post-COVID ‘’VED‘’ world - On-line meetings, transactions
- Use of CAATs
- DRP /BCP

Crypto wave & IS Security Audit

- Initial RBI Ban
- Hon’ble SC opinion - 2018-19
- Pandemic : rise of BTC, Aggressive ads on ‘’ high returns’’
- Crypto-exchanges soliciting investments = luring young ‘’gullible’’ investors seeking high returns overnight
- Question : Crypto – asset or currency
- GoI : *Cryptocurrency and Regulation of Official Digital Currency Bill, 2021* (seeking control, accountability etc)
- Regulators mandating proper KYC , Investor education , caveats
- RBI – Partial ban on crypto = not productive

IS Auditor & ERP systems

- **IS Audit of Business processes** : O2C, R2R, P2P
- SAP
- Oracle
- Peoplesoft
- Navision
- JDE
- CBS : importance in BFS sector
- **ERP Implementation & data migration**
- **ERP version upgradation**
- **IS Audit of websites /portals (Ecommerce)**
- **Focus** : Transaction Codes, Exception reporting, program, config /settings , TOC (Input, output etc), data integrity, access

Growing investments in Fintech
MSME : Focus of digitisation

- Digital India Mission
- Digitisation of :

❖marketing

❖Manufacturing

- Govt initiatives in MSME in tier-2, rural & tribal areas
- Higher Outlay in Budget

The Digital age - snippets

- **Tata steel** – global 1st for Steel industry- used **Blockchain platform** pioneered by HSBC to complete trade finance transaction with UAE Based company – end-to end digitisation of LC transaction & all e-presentation of trade documents
- **Data breach :**
- Tik Tok sued in UK & EU for billions over use of kids' PRIVATE data to benefit unknown 3rd parties (April 2021)- violation of EU & UK Data Protection Laws

Hacking case : April 2021

- India's 2nd largest brokerage firm Upstox 's information hacked
- 25 lakhs investors' data/ KYC info stolen & put up on dark web
- Data breach happened in 3rd party data warehouse facility
- Upstox : news release : **strengthening its IS Security system by ISS Audit** & ensured investors' stocks & funds are safe
- **Airtel CEO** : Alert to subscribers about malware / harmful apps
- **Air India** – passengers data (2011-2021) compromised from SITA server : name, email, contact, gender, credit card details, **carried out extensive IS & Cyber Audit**

MCA Notification

- Ministry of Corporate Affairs (MCA) issued a notification regarding enforcement of Gazette Notification No. GSR 205 (E) dated 24th March 2021 – Amendment to Rule 3(1) of Companies (Accounts) Rules 2014 which seeks to bring a host of reforms and improvements in the way businesses operate in India
- Transparency of FS
- Audit trail

Audit trail

- A provision to Rule 3 (1) of the Companies (Accounts) Rules, 2014 reads, "*Provided that for the financial year commencing on or after the 1st day of April, 2021, every company which uses accounting software for maintaining its books of account, shall only use a software* ***that has a feature :***
- *for* ***recording audit trail of each and every transaction****,*
- *creating an* ***edit log of each change*** *made in the books of accounts*
- ***along with the date*** *when such changes were made and*
- *ensuring that the* ***audit trail cannot be disabled***."

Maintenance & compliance

- Point (g) of Companies (Audit and Auditors) Amendment Rules, 2021, which reads as –
- whether the company has used such **accounting software** for maintaining its books of account which has **feature of recording Audit Trail (edit log**) facility and the same has been **operated throughout the year** for **all transactions recorded** in the software and
- the **Audit Trail feature has not been tampered** with and
- **the audit trail feature has been preserved by the company** as per the statutory requirements for **record retention**

Possible intent

- To detect (wherever allegation is levelled) **manipulation of electronic accounting records by management of corporates to play a fraud** on the interests of stakeholders and in the process, defeat the object and purpose of law.
- **Audit trail** : trail of all activities surrounding a particular transaction.
- Requirement of audit trail is critical aforesaid notification
- **Auditors** now will be in a better position to comment on the **authenticity of the books of accounts** and will have more chances **to reduce risk by way of checking the trails and logs available** in the system.

BFSI – RBI stance- May 2021

- **RBI sharpens IS, risk tools to gauge banks, NBFCs**
- review & strengthen **Risk Based Supervision (RBS)**

❑ Commercial banks,

❑ UCB,

❑ NBFC & all India financial institutions.

- RBI **inviting bids - IT technical experts/ IS Audit consultants**
- For UCBs and NBFCs, EOI for 'Consultant for Review of Supervisory Models' floated

- **RBI : risk-based internal audit (RBIA) & IS Audit system**
- Entities **to implement RBIA framework by March 31, 2022,** constitute **committee of senior executives**, to be entrusted with the responsibility of formulating a **suitable action plan**

IS Audit – emerging GLOBAL Professional opportunities

1. **Government audits** – PSU , Departments
2. **Banks – CBS , IS Audit need (PNB Case), NABARD**
3. **Co-operative Banks and Co-operative societies** : mandatory IT Audits
4. Consulting opportunities in RPA, AI, CC ,
5. ISA qualified for **Internal Audits**
6. **RBI, SEBI and IRDAI** - mandated annual system audits
7. Companies **using SAP , Oracle, JDE , Peoplesoft, CBS**

8. **Data privacy laws like GDPR and draft version of data protection bill(India)** created a demand for ISA qualified professionals.

9. **Cyber forensic & IS Security audit – CBI, EOW, ED, SFIO , SEBI, CAG , CERT, DSCI**

10. Control implementation , capacity building for clients

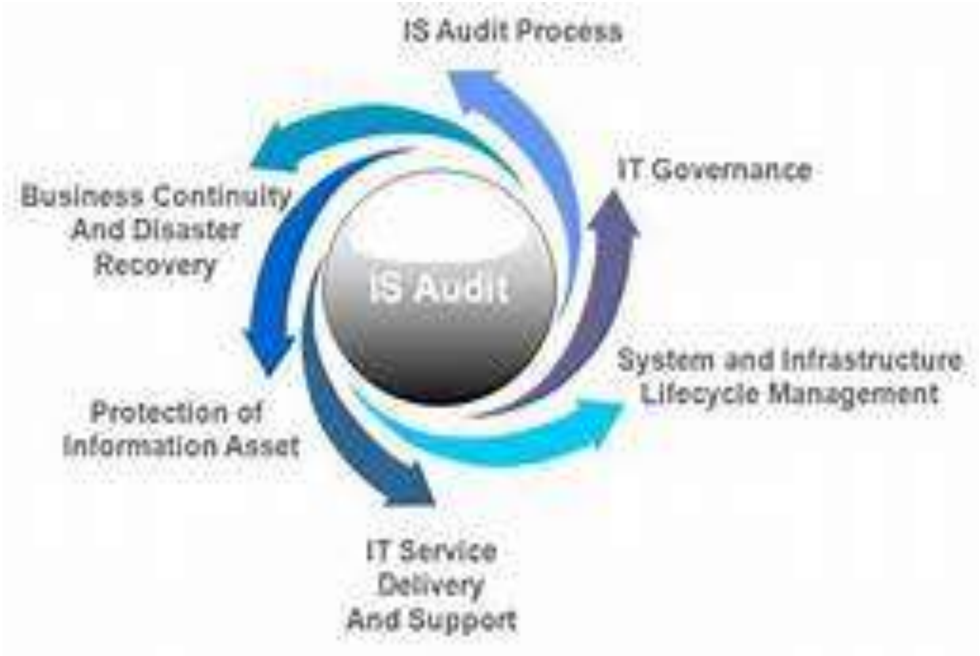
11. Industry wide inclusive applications - security governance

12. Supporting in e-governance & Digital India (DBT, vax etc)

DISSA : Effective tool <u>both for Industry & Practising Members</u>

- ✓ <u>new professional window for Members</u>
- ✓ **BFSI, Corporate & regulators – variety of client base**
- ✓ **ISA + Cyber Forensic Audit**

IS Audit


IS Audit Process
IT Governance
System and Infrastructure Lifecycle Management
IT Service Delivery And Support
Protection of Information Asset
Business Continuity And Disaster Recovery
IS Audit

- An **information technology audit**, or **information systems audit**, is an examination of the management controls within an IT infrastructure and business applications.

Scope of IS Audit

- The evaluation of evidence obtained determines if the information systems are :

1. safeguarding assets,
2. maintaining data integrity, and
3. operating effectively to achieve the organization's goals or objectives.

- These reviews may be performed in conjunction with a FS audit, internal audit etc
- IT audits are also known as **automated data processing audits** (**ADP audits**) and **computer audits**.

IS Audit coverage areas

- **1. Systems and Applications**:
- An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.
- System and process assurance audits form a subtype, focussing on business process-centric business IT systems.
- Such audits have the objective to assist financial auditors

IS Audit coverage

- **2. Information Processing Facilities**:
- An audit to verify that the **processing facility is controlled to ensure timely, accurate, and efficient processing** of applications under normal and potentially disruptive conditions
- **3. Systems Development**:
- An audit to verify that the **systems under development meet the objectives of the organization**, and to ensure that the systems are developed in accordance with generally accepted standards

- **4. Management of IT and Enterprise Architecture**:
- An audit to verify that **IT management has developed an organizational structure and procedures** to ensure a controlled and efficient environment
- ***Control Objectives for Information and related Technology (COBIT) -*** set of best practices (ISACA)
- **5. Client/Server, Telecom, Intranets, Extranets**:
- An audit to verify that **telecommunications controls are in place on the client (computer receiving services), server, and on the network** connecting the clients and servers.
- Perimeter security , firewalls etc

Role of ISS Auditors

- ***Performance measurement*** *- how well is the IT function supporting business requirement?*
- ***IT control profiling*** *- What IT processes are important? What are the critical success factors for control?*
- ***Awareness*** *- what are the risks of not achieving the objectives?*
- ***Benchmarking*** *- what do others do? How can results be measured and compared?*