



EUCIP
European Certification of
Informatics Professionals

EUCIP Information Systems Auditor

Elective Level Profile Specification

Version 2.4, February 2007

Short Description

A EUCIP Information Systems Auditor provides an independent assurance of security, quality, compliance and value contribution of information systems to a specific organization (reporting to the highest corporate or board responsibility). An IS Auditor is expected to demonstrate sound technical competence, independence of opinion, compliance to the Code of Professional Ethic.

This profile requires a minimum work experience of **60** months in a compatible job role; if this requirement is not fulfilled, the candidate might be certified as an **Associate** Information Systems Auditor.

Tasks Overview

The Information Systems Auditor provides client organizations with an independent assurance of the risk level coming from the current business practices with a specific focus on the use of Information Technology.

Evaluates security, quality, laws and regulatory compliance and value contribution, reporting to the highest corporate or board directors.

Assesses technology risks, i.e. sorts and finds out how technology tackles business-specific risks in the operations to a specific information system.

Evaluates IT Governance and IT Control, i.e. besides the risk assessment conducts the consequent evaluation of efficiency, effectiveness and compliance of all control activities in place to minimize technology-related risk.

Through risk assessment and control evaluation, provides advice to the top management in order to achieve and maintain secure operating level for systems and to support evidence to shareholders and stakeholders that all technology-related risks are tackled and minimized.

Analyzes compliance to laws and regulatory issues connected with the usage of information systems (data privacy, balance sheet and financial reporting, etc).

Evaluates compliance of IT governance issues and application-specific systems to specific legal and regulatory in order to minimize non-compliance issues: fines, civil and criminal prosecutions, insurance risks, removal from regulated environments (finance, e-business, telecommunications, etc).

Conducts independent assessments during the implementation phase of an information system, in order to assure that time constraints and-or the complexity of the issue do not undermine security, compliance, cost-effectiveness of the resulting system.

After a system implementation and go-live phase, manages formal reviews in order to evaluate residual risks and the global cost-effectiveness or the value contribution of the system.

Conducts independent assessments of technology related incidents, i.e. in the case of a risk occurrence that can take form of a security incident, a fraud, a processing error or a legal non-compliance, drives the post-incident review to define the causes and effects of the occurrence, to analyze the effectiveness of the control environment, to highlight potential optimizations as those required to enhance resiliency and conformity.

Essential Behavioural Skills [3]¹

The Information Systems Auditor must demonstrate sound technical competence in order to evaluate risks and controls, independence of opinion, ability to consistently comply with a Code of Professional Ethics.

The role requires outstanding learning attitude to tackle with both business and technology related issues; a brilliant oral and written expression in order to communicate with board-level or higher executives, and a very wide range of interpersonal skills.

Cooperative approach and positive behaviour are required in order to be able to deal with the different teams involved in the Information processing: users, developers, systems managers, business managers. Therefore, understanding for the real needs and thoughts is essential.

Attention, ability to collect information, keen organisational and economical sensitivity are required to quickly understand the needs of the organization and of relevant stakeholders and shareholders.

Open minded vision, analytical and synthetic intelligence, imagination and proactivity are required to analyze and validate the quality and security levels of the systems and of the data.

A persistent logical-minded and goal-driven approach, flexibility, determination, planning and control aptitude, attention to details, teambuilding and leadership are required to achieve actual results.

¹ numbers in brackets represent EUCIP points

Detailed Skills Required ²

Deep competence level [15]

A7.09 IS audit process [2]

- Describe the IS audit process:
 - o Distinguish accepted auditing standards
 - o Audit planning and chartering
 - o Complete the preliminary review
 - o Prepare an audit plan
 - o Identify audit tools and techniques
 - o Produce an audit report and follow-up
 - o Post-audit actions
- Evaluate and select between different audit techniques
- Use of Computer-assisted audit tools and techniques
- Define a plan and related organizational aspects for auditing the various processes:
 - o Planning and analysis of new systems,
 - o IT strategies and standards,
 - o Planning and controlling,
 - o Process management,
 - o Quality management.

A7.10 Gathering evidence through sampling [1,5]

- Define a sampling strategy
 - o Apply judgmental sampling
 - o Apply statistical sampling
 - o Apply attribute-based sampling
- Use sampling techniques to support audit findings
 - o Foster repeatability of sample population definition
 - o Foster repeatability metrics and measurement
 - o Foster clarity of measures
- Use walkthroughs and expert support for evidence analysis

A2.06 Key IT process control [1,5]

- Conduct IT acquisition and implementation audit:
 - o Audit of software acquisition procedures
 - o Audit of systems implementation
- Conduct change and configuration management audit:
 - o Verify vulnerabilities in software development
 - o Explain software configuration management
 - o Understand impact assessment

² **Remark:** the competence category A7.09 contains part of the AICPA Auditing Standards concerning Information Technology, other categories contains part of the areas described by the Information Systems Audit and Control Association ISACA in the CISA and CISM certification schemes and in the COBIT 4.0 (Control Objectives for Information technology) reference framework.

Those references have been used as a standard reference; further detailed descriptions can thus be found in COBIT framework, and in CISA and CISM exam reference manuals and AICPA Auditing Standards

- Explain revisions to documentation and procedures
- Define software release and distribution policies
- Explain organizational change management.

A6.06 Audit Reporting and Communication [1,5]

- Prepare Audit Reports for effective communication:
 - Focus Reporting for Top Management
 - Focus Reporting for the auditee management
- Prepare substantiation of communication:
 - Define elements of an audit Report
 - Apply Balanced audit report presentation techniques
 - Develop a strategy for working paper retention
 - Choose alternative formats for audit reporting
- Adopt Reporting standards
- Contribute to a fruitful acceptance of audit results:
 - Prepare and negotiate the draft executive summary
 - Prepare and negotiate the detailed report of findings
 - Prepare and negotiate the remediation plan

A7.11 Compliance evaluation [1,5]

- Define a framework for laws and regulations applying to the organization and to its specific business, including:
 - International regulations
 - European directives
 - National legislation
 - Regional/local legislation
 - Specific rules and regulations referring to the industry / business sector
 - General laws and specific contracts regulating the acquisition and usage of IT products (warranties, licenses, maintenance contracts, ...)
 - Possible rules and standards defined at the corporate level
- Synthesize control requirements coming from laws and regulations
- Communicate legal requirements to IT staff and key application users
- Communicate with external compliance authorities

A3.07 Risk Management [1,5]

- Master Risk Management Process and Risk Management standards
- Perform Risk Assessment tasks:
 - Perform Information Resource Valuation
 - Perform Information Asset Classification
 - Scope threats
 - Find vulnerabilities
 - Define risks
 - Evaluate impacts
- Perform Risk Management tasks:
 - Highlight Controls and Countermeasures
 - Design and evaluate methods to transfer risks
 - Define Recovery Time objectives
 - Define Control Baselines

- Perform Risk Monitoring:
 - o Define monitoring metrics
 - o Collect monitoring evidence
 - o Prepare and communicate management monitoring reports
- Prepare Risk documentation
 - o Prepare and communicate executive-level reports
 - o Prepare remediation plans
 - o Define risk documentation repository for compliance

A7.12 IT Security Assurance [1,5]

- Master design and review controls for information and systems security issues:
 - o Confidentiality
 - o Integrity
 - o Availability
 - o Need-to-know, separation and segregation
 - o Auditability
 - o Non-repudiation
 - o Accountability
- Master design and review controls compliant with most relevant IT Security standards and common control practices:
 - o Physical security
 - o Network security
 - o Platform security
 - o Operating system
 - o Middleware
 - o DBMS
- Master design and review applications security controls
 - o Users/Roles/Segregation of duties
 - o Need-to-know
 - o Data Backup
 - o Application flow and interface controls
 - o Batch processing
 - o Data flows

A2.08 IT Governance [1,5]

- Apply standards and practices for IT Governance in the audit context (e.g. COBIT)
- Highlight and review practices and procedures for the IT Governance process
- Master IT strategic alignment and Value delivery practices
- Master IT resource management practices
- Execute performance management analysis
- Master legal compliance and control system evaluation
- Master Service Management techniques for operations management (e.g. ITIL)

A5.01 Project Management essentials [2,5]

- Define the role of the various specialists in a typical project organisation structure (e.g. Rational Unified Process, PRINCE2, etc.).
- Contribute to the IS project plan for a given business scenario.

- Contribute to risk analysis of a project proposal, concentrating on business risk.
- Use standard approaches to evaluate a project plan from the business viewpoint.
- Assist in defining the phases within a project and the role of the business analyst in those phases.
- Assist in the creation of constraints and the definition of milestones, checkpoints and reviews for a project.
- Define Corporate Standards for the documentation of business analysis deliverables in a project.
- Contribute to quality assurance processes within a project, from a business perspective.

Incisive competence level [14]

A 7. 04 Managing Business risk and IT security [1,5]

- Specify the business need for recovery and back-up of data and for protection against viruses.
- Evaluate the need for encryption of data (at rest/in transit) in the light of network “threats” to data integrity.
- Evaluate the risks to the business caused by security threats to IS/IT.
- Contribute to a Security policy for (part of) a business organisation.
- Understand the key factors of IT security and know the main international standard regarding IT Governance (e.g. CobiT) and IT security (es. BS 7799)
- Develop a feasibility study to adopt an ISMS (Information Security Management System)
- Plan and install the installation of ISMS
- Realise the ICT Risk management assessment in the Company
- Propose the ICT organisation in the Company (IT security Directional Committee, identification of Information security Officer, etc), defining roles and skill of ICT professionals dedicated to ICT security
- Define and assure the Guidelines of ICT Security policy in the Company, assuring the segregation of duties between operations and development, and classification of level of security for the different information type
- Define and assure the Guidelines of Business Continuity solutions (Business Impact Analysis)
- Define and assure the technical architecture of ICT Disaster Recovery, considering the alternative options (on line updating, delayed updating, san and virtual architecture, etc)
- Define and assure the Guidelines for ICT Risk Management
- Define a Company Policy for ICT users (authentication and authorisation), defining the techniques for the password utilisation (written password, smart card, token, biometrics, etc), in coherence with risk assessment

- Define and assure the Guidelines for physical security (perimetral security, access control, electric power for Computer room, Ups, etc)
- Define and assure the Guidelines for Applications and Infrastructure Change Management (design stage, test stage, production stage)
- Define and assure the Guidelines for Incident handling
- Define and produce the ICT security reporting
- Organise the Controls regarding ICT security
- Plan and realise the selection of ICT security tools (antivirus, firewall, ips systems, etc)
- Promote and organise the Vulnerability Assessment
- Promote the user training on ICT security
- Work to realise project (documentation, organisation and technical solutions) requested by laws (es. Privacy, SOX, etc)
- Promote and develop projects on ICT security (es. Cryptography, etc)

A7.05 Managing Data protection [1,5]

- Classify the security level of data
- Define Data security requirements in IT projects
- Organise and choose the automatic tools for the back up of system software, application software and data banks
- Organise back up storing outside the company, selecting the most effective and efficient solution (e.g. Traditional shipment, Back up via Network etc)
- Protect data sent on network, using cryptography or tunnelling solutions
- Organise system and application test, creating test files without using the official data of the Company (and protect critical data test)
- Understand the key factors of IT security and know the main international standard on IT Governance (e.g. CobiT) and IT security (e.g. BS 7799)
- Define rules for employees and external supplier to assure the confidentiality of information in data bases used in the current operations (guidelines, controls, responsibilities, etc)

A4.01 New technology opportunities and the matching of these to business needs [2]

- Analyse business processes and compare them against alternative solutions proposed by standard software packages (“best practice” approach).
- Evaluate various options for the “virtual organisation” within a business scenario.
- Establish a business case for moving from a “segregated” sales and marketing strategy to the “unique customer” approach in a given organisation.
- Produce a report on the effects of globalisation for an organisation.
- Evaluate the Internet as a tool for creating new opportunities for an organisation.

- Evaluate extranets as a tool for achieving efficiencies in customer/supplier interaction.
- Produce an impact analysis for an organisation related to the increased use of e-business mechanisms.
- Evaluate a project which used IT as the enabler for significant business change.
- Produce a report documenting the major features of Customer Relationship Management tools.
- Compare the features offered by two major Supply Chain Management packages.
- Evaluate the case for using Enterprise Resource Planning tools for a given business scenario.
- Compare the strengths and weaknesses (from a business viewpoint) of developments in IT technical architectures (e.g. web based vs. “2 tier” client server).
- Evaluate the case for using Document Management systems.

A4.02 Package selection and implementation lifecycle [1]

- Define a framework for effective package selection.
- Identify, investigate and assess potential package suppliers.
- Evaluate a software package against defined requirements.
- Present recommendations concerning the “fit” of the software package to agreed functional and non-functional requirements.
- Evaluate the advantages and disadvantages of the package approach.
- Evaluate the human, technical and financial implications of a decision to outsource development/buy a package solution.
- Apply a checklist of factors to a decision on in-house development vs. package procurement.
- Work within a framework for package selection.
- Understand the impact on package selection of Prototyping approaches.
- Acquire an understanding of the software package market in a particular business context.
- Produce a High Level Functional Model for a system.
- Contribute to identifying potential package suppliers.
- Contribute to the production of Invitations to Tender (ITTs) and questionnaires.
- Investigate suppliers.
- Assist in the creation of Supply Contracts and Support Agreements.
- Perform cost comparisons – purchase and support.
- Document the functional match of a package solution.
- Contribute to gap analysis for a package selection.
- Use a weighted scorecard approach to evaluation.
- Present the recommendation for a specific package solution.
- Assist in the implementation of packages.
- Liaise with procurement staff for package purchase.
- Define the modified business processes required in a package solution.
- Appreciate the issues with tailoring the package software.
- Contribute to long term supplier management.

- Appreciate the advantages/disadvantages of packages.

A1.01 Business activity and business process modelling [1,5]

- Understand the Rationale for Business Activity Modelling.
- Perform Internal Environment Analysis (e.g. MOST).
- Perform External Environment Analysis (e.g. PESTLE).
- Use SWOT Analysis.
- Perform Business Viewpoint Analysis.
- Define Business Activities for an organisation.
- Define CSFs and KPIs for a business change.
- Formalise Business Rules within an organisational unit.
- Define Information Support needed for the defined activities.
- Perform conflict resolution between perspectives.
- Create Rich Pictures to describe a business scenario.
- Utilise the Soft Systems Approach to developing an Information System.
- Evaluate alternative ways of modelling business processes; e.g. Data Flow Diagrams, PHD, Process Dependency, Event Models.
- Conform to the syntax of business process modelling.
- Document Information flows (sources, destinations).

B1.08 Software Engineering principles [1]

- Understand roles of the software engineering process (project manager, software developer, maintenance staff, quality assurance and the user).
- Understand software development life cycle models and their applications.
- Understand and apply software development estimation techniques.
- Understand and apply principles of software Project Management.
- Understand Risk Management.
- Understand Quality Assurance.
- Understand Configuration Identification, Control and Auditing.
- Understand Configuration Status Accounting.
- Understand and apply Software Estimating Techniques and Metrics.

A5.02 Estimating for System Development [1]

- Use a variety of estimating approaches and apply them to a practical project.
- Understand the importance of estimating and measurement.
- Distinguish between top-down and bottom-up estimating.
- Contribute to “estimating by analogy”.
- Contribute to Delphi estimating.
- Contribute to estimating by the analysis percentage effort method.
- Appreciate the principles of Function Point Analysis (FPA).
- Contribute to FPA estimates by using formal counting rules.
- Assist in defining effort estimates and elapsed duration estimates.
- Appreciate the use of Line Count Cost Models.
- Contribute to building Work Breakdown structures and hence estimating for software development projects.
- Appreciate the impact of timeboxing and RAD on estimating.

- Evaluate the factors affecting productivity in IS development.
- Contribute to collecting and analysing project statistics/metrics.
- Contribute to the use of metrics to improve project estimation.

B1.05 Systems design and implementation [1]

- Identify the tasks involved in implementing and designing an IT system.
- Evaluate the business benefits of database technologies, data warehousing and data mining tools.
- Understand the contents of a system specification.
- Understand function specifications.
- Appreciate the need for (and constraints on) Physical Design of Databases (e.g. tables and indexes).
- Perform Forms Design for a business system.
- Contribute to design of screens and dialogues.
- Contribute to recovery and contingency plans.
- Ensure that audit of an Information System is possible.
- Define system controls for an Information System.
- Define the data integrity needs for an IT System.
- Understand Technical System Options and assist the business in evaluation.
- Employ relevant methods of changeover to new systems.
- Contribute to System Review (post implementation).
- Detail the need for design of security, confidentiality and privacy in a system.
- Produce an implementation plan and assist with business implementation and system review.

B3.05 Principles of Testing [1,5]

- Explain the principles of Testing.
- Maintain the importance of Testing in the Lifecycle.
- Understand Dynamic Test Techniques.
- Apply Test Management Standards.
- Use Static Testing Techniques.
- Understand core testing terminology (e.g. Expected Results, Expected Information).
- Appreciate the economics of Testing.
- Perform High Level Test Planning.
- Organise User Acceptance Testing (UAT).
- Ensure Functional and Non-Functional UAT is completed.
- Contribute to Dynamic Testing (Black Box).
- Contribute to Test Management (e.g. organisation, estimating, resourcing).

C7.03 Change and configuration management [1]

- Describe a structured approach to Configuration Management.
- Coordinate and control the steps of system development.
- Administer versions of artefacts.
- Control access to artefacts.
- Administer dependencies between (versions of) artefacts.
- Define and administer reproducible products (baselines).
- Administer development states of artefacts.

- Ensure that a consistent version of the system exists at any time.
- Describe a structured approach to Change Management.
- Collect change requests.
- Evaluate change requests and commit on schedules.
- Drive the execution of changes.
- Test the results of changes done on the various artefacts.

A6.01 Managing business change [1]

- Develop a communication plan to facilitate organizational changes
- Foster innovation by an appropriate evaluation system for IT staff
- Promote training to facilitate the change
- Identify organizational and technological drivers of resistance to change
- Understand human behaviour and its impact on business change.
- Create a plan to overcome resistance to change from the business, including “selling” the benefits of new technology.
- Make effective use of Audio-Visual tools in making the case for change within an organisation.
- Explain to non-IT staff the role of IT in achieving corporate aims, and its place within the organisation.
- Ensure that the case for change is presented effectively, using modern delivery techniques.
- Evaluate the Impact of an IT solution on the Business, its Customers/Suppliers, Staff, Internal processes etc.
- Select between Programmes and Projects for Business Change.
- Organise the delivery of user training for both new business processes and the use of any underpinning ICT services.
- Control the interfaces between Business Change projects and enabling IT projects.
- Identify cultural, organisational and business constraints affecting options for change.
- Establish an understanding of business aims and develop alternative processes to achieve them.
- Assess the risks, costs and potential benefits of alternative business process designs.

External references to SFIA[®] version 3 by the SFIA Foundation

Skill 6: Business process improvement

“The identification of new and alternative approaches to performing business activities. The analysis of business processes, including recognition of the potential for automation of the processes, assessment of the costs and potential benefits of the new approaches considered and, where appropriate, management of change and assistance with implementation”.

Level 5

Skill 8: Business risk management

“The planning and implementation of organisation-wide processes and procedures for the management of operational risk”.

Level 5

Skill 9: Information security

“The management of, and provision of expert advice on, the selection, design, justification, implementation and operation of information security controls and management strategies to maintain the confidentiality, integrity, availability, accountability and relevant compliance of information systems”.

Levels 4 and 5

Skill 10: Information assurance

“The protection of systems and information in storage, processing, or transit from unauthorised access or modification. Denial of service to unauthorised users; or the provision of service to authorised users. Includes those measures necessary to detect, document and counter threats to the integrity of stored information, such as the application of firewalls and intrusion detection systems (IDS)”.

Levels 4 and 5

Skill 13: Continuity management

“The provision of service continuity planning and support. This includes the identification of information systems that support critical business processes, the assessment of risks to those systems’ availability, integrity and confidentiality and the coordination of planning, designing, testing and maintenance procedures and contingency plans to address exposures and maintain agreed levels of continuity. This function should be performed as part of, or in close cooperation with, the function that plans business continuity for the whole organisation”.

Levels 4 and 5

Skill 25: Systems testing

“The planning, design, management, execution and reporting of tests, using appropriate testing tools and techniques and conforming to agreed standards, to ensure that new and amended systems, together with any interfaces, perform as specified”.

Levels 4 and 5

Skill 34: Business analysis

“The methodical investigation, analysis, review and documentation of all or part of a business in terms of business functions and processes, the information used and the

data on which the information is based. The definition of requirements for improving any aspect of the processes and systems and quantification of potential business benefits. The creation of viable specifications and acceptance criteria in preparation for the construction of information and communication systems”.

Levels 4 and 5

Skill 37: Business process testing

“The planning, design, management, execution and reporting of business process tests and usability evaluations. The application of evaluation skills to the assessment of the ergonomics, usability and fitness for purpose of defined processes. This includes the synthesis of test tasks to be performed (from statement of user needs and user interface specification), the design of an evaluation programme, the selection of user samples, the analysis of performance and inputting results to the development team”.

Levels 4 and 5

Skill 38: Change implementation planning and management

“Defining and managing the process of deploying and integrating IT capabilities into the business in a way that is sensitive to, and fully compatible with, business operations”.

Level 5

Skill 41: Stakeholder relationship management

“The coordination of relationships with and between key stakeholders, during the design, management and implementation of business change”.

Levels 4 and 5

Skill 43: Change management

“The management of all changes to the components of a live infrastructure, from requests for change (RFC) through to implementation and review, to support the continued availability, effectiveness and safety of the infrastructure”.

Levels 4 and 5

Skill 61: Quality management

“The management of, or provision of advice on, the application of appropriate quality and/or environmental management and process improvement techniques to any aspect of a function or process. The achievement of, and maintenance of compliance to, national and international standards, as appropriate”.

Levels 5

Skill 62: Quality assurance

“The process of ensuring that the agreed quality standards within an organisation are adhered to and that best practice is promulgated throughout the organisation”.

Levels 4 and 5

Skill 64: Compliance audit

“The independent, third-party assessment of the conformity of any activity, process, deliverable, product or service with the criteria of specified standards, such as BS EN ISO 9000/14000, local standards, best practice or other documented requirements. May relate to, for example, asset management, network security tools, firewalls and Internet security, real-time systems and application design”.

Levels 4 and 5

Skill 65: Safety assessment

“The assessment of safety-related software systems to determine compliance with standards and required levels of safety integrity. This involves making professional judgements on software engineering approaches, including the suitability of design, testing, and validation and verification methods, as well as the identification and evaluation of risks and the means by which they can be reduced. The establishment, maintenance and management of an assessment framework and practices may also be included”.

Level 5

External references to AITTS by the German Government – *Arbeitsprozessorientierten Weiterbildung in der IT-Branche*

Profil 2.3: IT Quality Management Coordinator (ITQualitätssicherungskoodinator/in)

“Quality Management Coodinator beraten bei der Erstellung von Qualitätsmanagementkonzepten und entsprechender Handbücher, setzen Qualitätsvorgaben für die Entwicklung, Installation und Nutzung komplexer IT-Systeme und Produkte um und kontrollieren die Einhaltung der Qualitätsvorgaben”.

External references to Nomenclature 2005 by CIGREF (club informatique des grandes entreprises françaises)

(?) Métier 1.1: Consultant en systèmes d’information

“Il anticipe et fait mûrir les nouveaux projets par une sensibilisation à l’apport des technologies nouvelles et une analyse prospective des processus métiers. Il assiste la maîtrise d’ouvrage pour la définition des besoins et des solutions à mettre en œuvre, dans un souci de meilleure intégration dans le système d’information d’entreprise.”