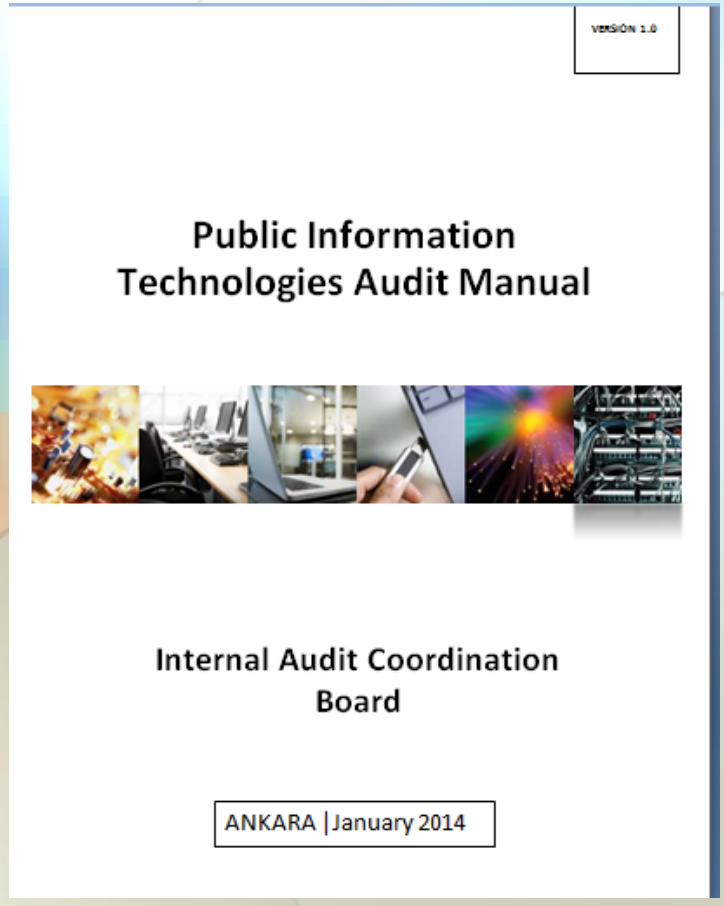


Public Information Technologies Audit Manual

Ahmet Bora ÖZTEKİN CIA,CGAP
Internal Auditor
Ministry of National Defense-TR

Structure and Features of Manual

1) Basic Concepts of IT Audit
2) IT Audit Methodology
3) Audit approach on IT Governance Processes
4) Audit approach on IT Management Processes
5) Implementation Controls
6) IT general controls

Structure and Features of Manual

Part I : Basic Concepts of IT Audit

- This part touches upon fundamental principles regarding IT, its implementation areas, rules of ethics, generally accepted competencies, certifications and international standards and frameworks that can be used.
- Furthermore, this part elaborates on the relation of IT audit with other audit types and the role that IT audit can play in such audits.

Structure and Features of Manual

Part II : IT Audit Methodology

- This part specifies the control types related to IT and their relation with each other. Then, it discusses the methods and tools that can be used from pre-audit study to planning, from risk analysis to audit execution and reporting.

Structure and Features of Manual

Part III : Audit approach on IT Governance Processes

- This part addresses the audit approach on IT Governance Processes, and in this respect, it involves enterprise-level controls and governance controls and relevant audit tests.

Structure and Features of Manual

Part IV : Audit approach on IT Management Processes

- This part addresses the audit approach on IT Management Processes, and in this respect, it involves IT general controls and relevant audit tests on such processes.

Structure and Features of Manual

Part V : Implementation Controls

- This part elaborates on Implementation Controls and focuses on the methods for auditing such controls.

Structure and Features of Manual

Part VI : IT General Controls

- This part includes IT general controls that should be evaluated at the IT infrastructure level or in the security audits to be carried out alone within the scope of IT management processes, and relevant audit tests.

Relation Between Parts of Manual and Competence Level

Relation between parts of Manual and competence level

Parts of Manual	Increasing competence level (+) → Definitions and Principles	Compulsory Audit Steps	Optional Audit Steps	Detailed References
Part 1: IT Audit Basic Concepts				
Part 2: IT Audit Methodology				
Part 3: IT Enterprise-level and Governance Processes Audit				
Part 4: IT General Controls (Management Processes) Audit				
Part 5: IT Application Controls Audit				
Part 6: IT General Controls (IT Infrastructure) Audit				

Required minimum competence level	Level 1 (Beginner)	Level 2 (Advancing)	Level 3 (Expert)	Not Applicable

Relation Between Parts of Manual and Competence Level

Level 1 (Beginner):

- Refers to the level of an internal auditor who has performed internal audit in public administrations and participated in **Basic IT Audit Training.**

Relation Between Parts of Manual and Competence Level

Level 2 (Advancing):

- Refers to the level of an internal auditor who has performed internal audit in public administrations and participated in Basic IT Audit Training and **Advanced IT Audit Training** and who has worked on IT Audit in public administrations for at least 1-2 years.

Relation Between Parts of Manual and Competence Level

Level 3 (Expert):

- Refers to the level of the internal auditor who holds **CISA certificate** or has already completed the training required for taking the exam, and has minimum 2-3 years experience on IT audit.

IT Audit Competence Model

Required Competencies

Technical Competencies

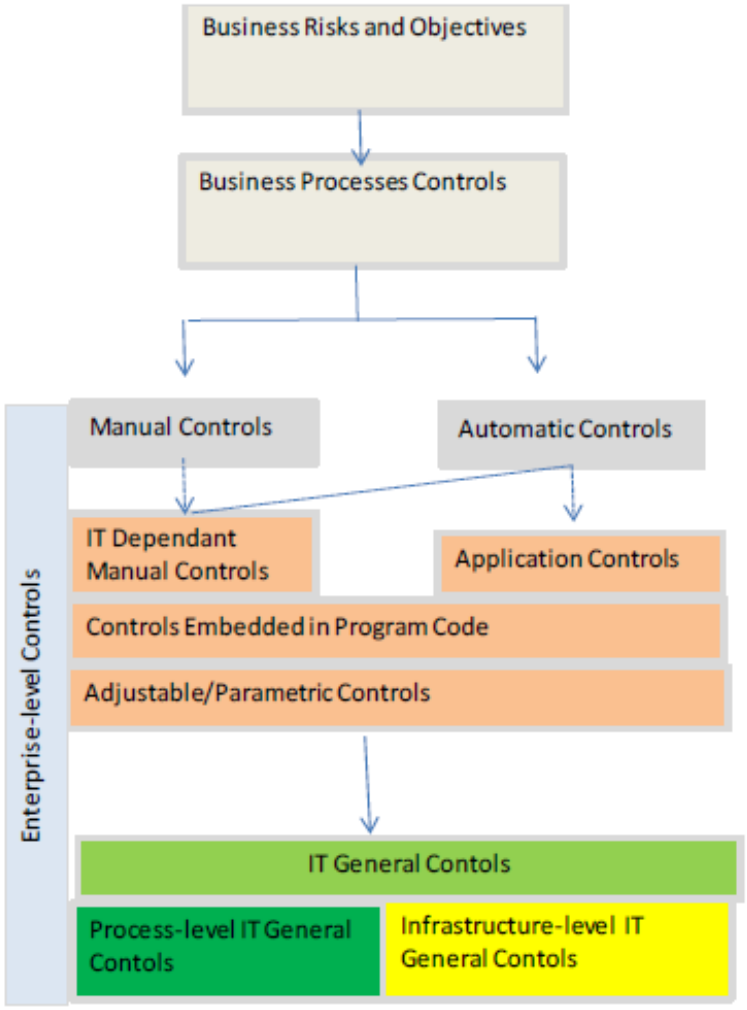
- Information Systems Auditing Process
- Management and Governance of Information Systems
- Acquisition, Development and Installation of Information Systems
- Operation, Maintenance and Support of Information Systems
- Protection of Information Assets

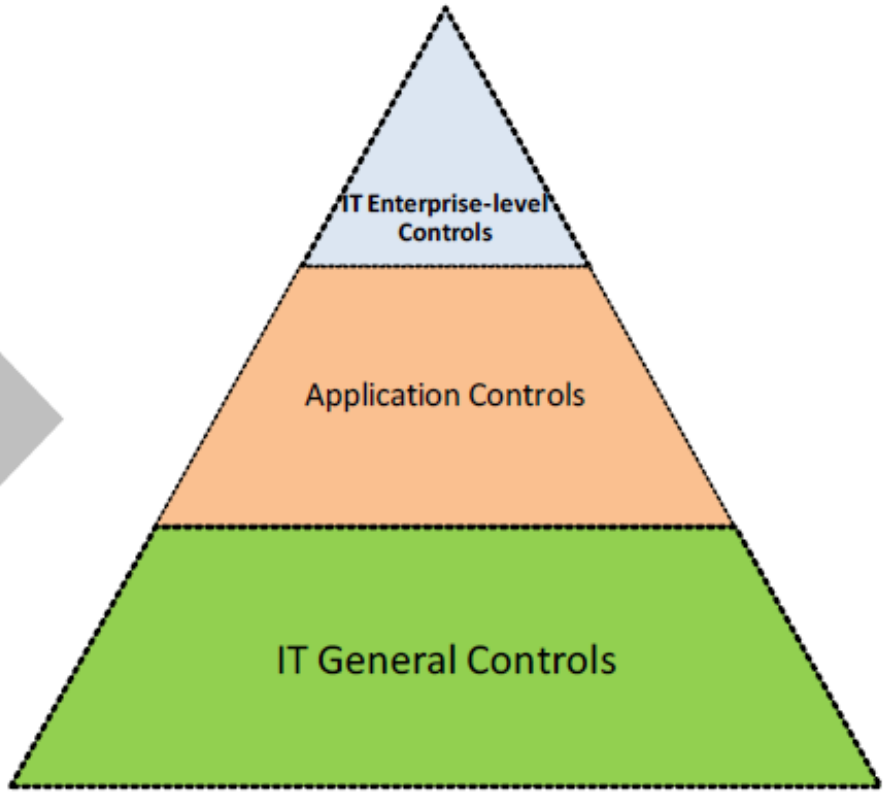
Soft Skills

- Influence (persuasion) and communication
  - Effectively uses and develops persuasion power
  - Works efficiently in cooperation
  - Creates team synergy under common objectives

  ……..
- Method of change
  - Open to change and innovation
- Dispute Resolution
  - Manages and resolves the disputes effectively through negotiations

IT Audit Methodology

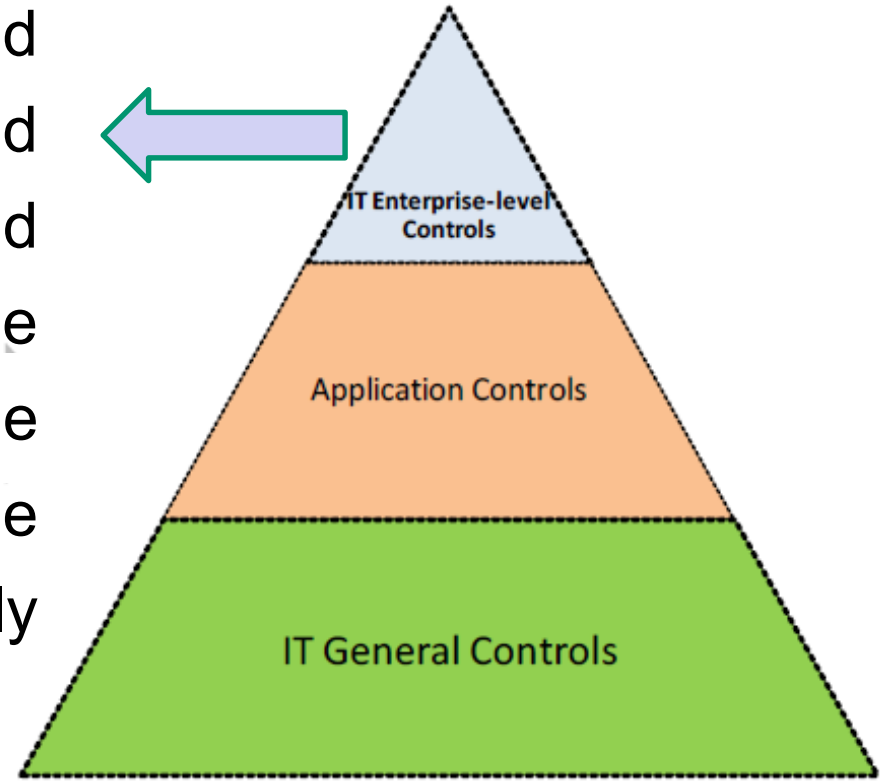




IT Control Pyramid

IT Audit Methodology

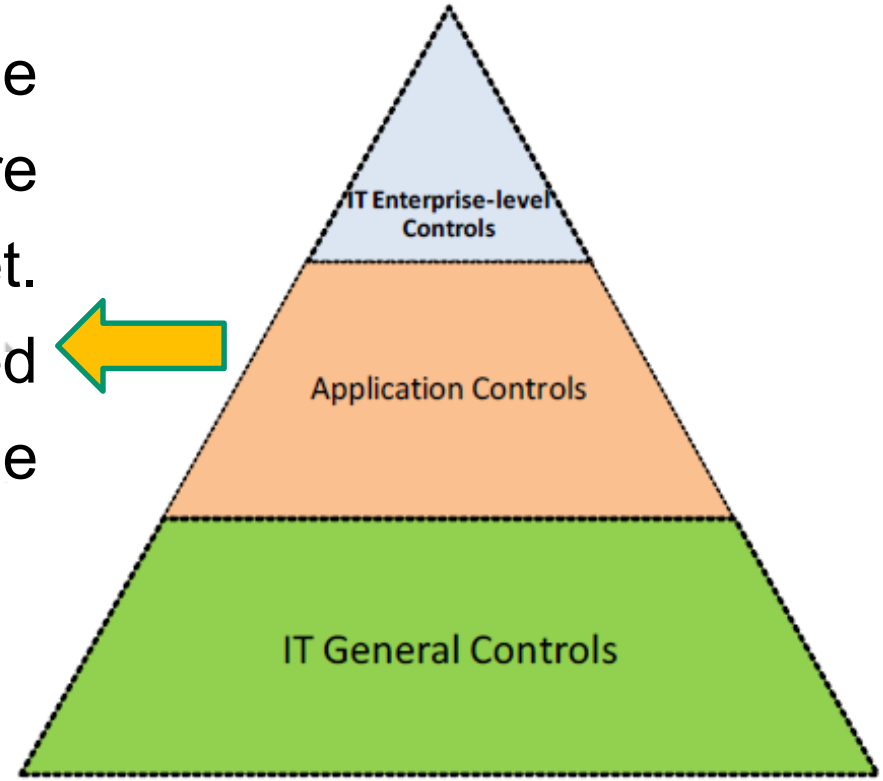
- **Enterprise-level controls** are internal controls, in the broad sense, that are designed throughout the organization and its personnel to provide reasonable assurance that the directives and instructions of the entity's management are fully applied.



IT Control Pyramid

IT Audit Methodology

- **Application controls** include control procedures that ensure that critical IT functionality is met. They are automatically performed by information systems of the entity.



IT Control Pyramid

IT Audit Methodology

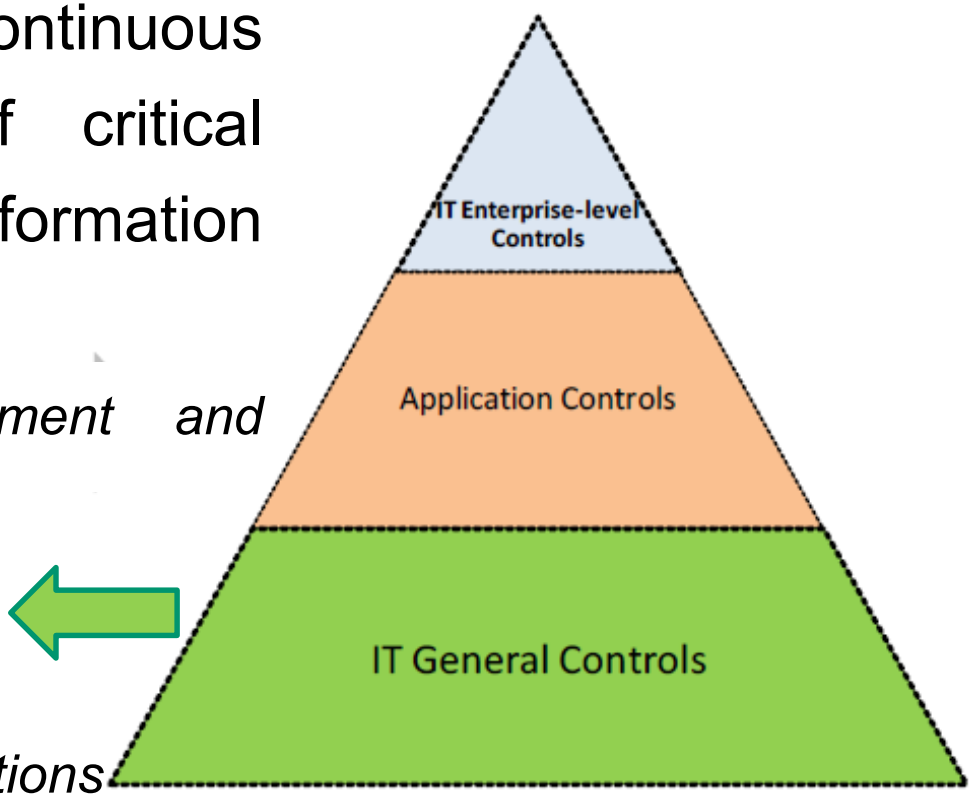
- **IT general controls** that form procedures to support the continuous and proper functioning of critical functionality expected from information technologies.

✓ *Controls on the improvement and maintenance of application controls*

✓ *System software controls*

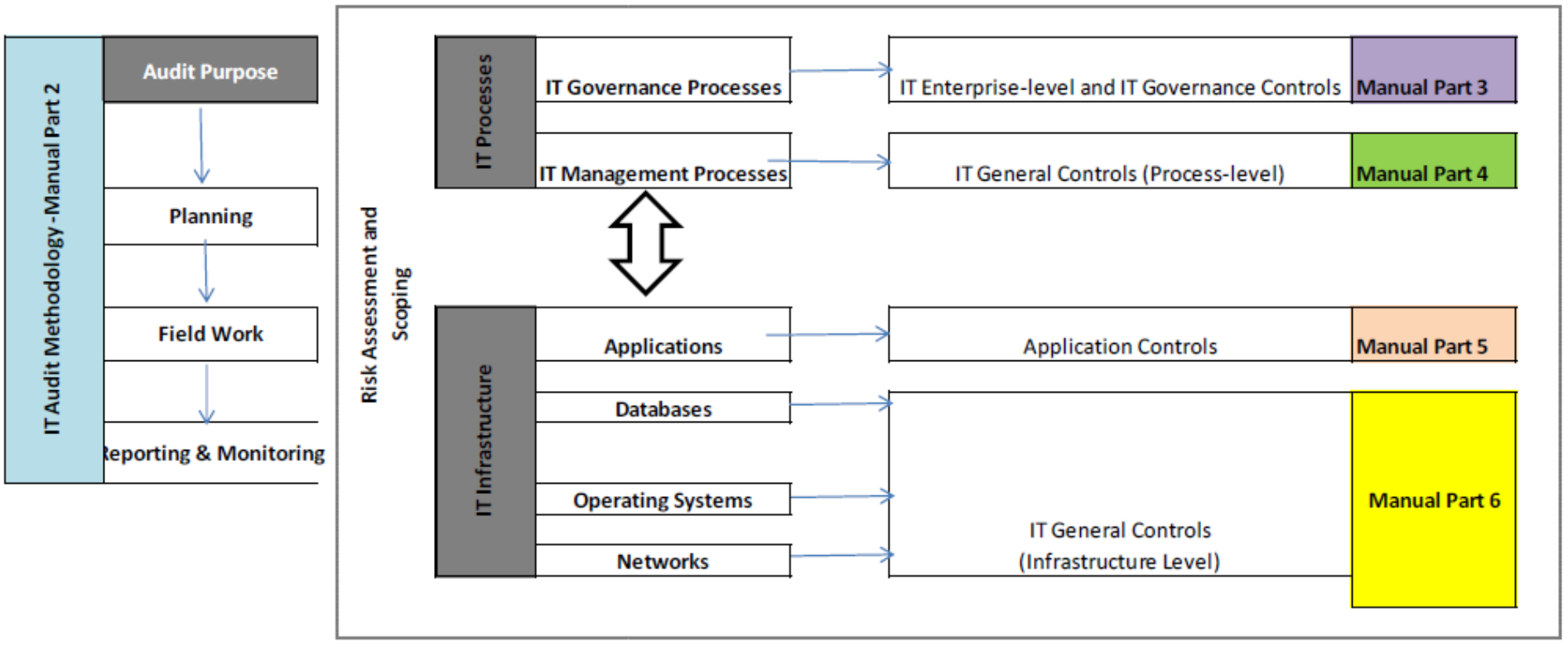
✓ *Access security controls*

✓ *Controls on data centre operations*



IT Control Pyramid

IT Audit Methodology



IT Audit Methodology

- **Planning**

  - **Understanding the audit objectives**
  - **Understanding IT Environment**
  - **Risk assessment**

    Enterprise-level Risk Assessment

    Application-level Risk Assessment

  - **Scoping**

    Financial Audit, System Audit, Performance Audit, Compliance Audit

  - **Preparing Work Plan**

Enterprise-level Risk Assessment Form

Risk Components	#	Risk Assessment Subject/Risk Factors	Answer
1) Strategic impact	1	Effect on the institutional reputation of a possible breakdown in the organisation's IT functions in terms of public opinion	
		Low: Institutional operations and reporting needs are mostly fulfilled manually.	
		Medium: Institutional operations and reporting needs are partly fulfilled via IT automation.	
		High: Institutional operations and reporting needs are entirely based on IT automation.	
	12	Annual transaction volume performed on IT applications and infrastructure.	
	13	Number of end-users of IT applications and infrastructure	
	14	Whether the IT applications and infrastructure have centralised or decentralised (e.g. provincial) organisation	
	15	Whether remote access is enabled to IT applications and infrastructure	
	16	Technological transformation (e.g. main servers) on IT applications and infrastructure during audit period	
	17	Integration level between IT applications and infrastructures supporting main activities	
	18	Level of dependency on the third parties (application and infrastructure components) in IT service and infrastructure management	
	19	Ratio of interruptions in IT services during audit period	
	20	Level of documentation regarding IT processes	
	21	State of monitoring capacity and performance regarding IT applications and infrastructures	
	22	Ratio of IT budget within the institution's budget	
	23	Whether the financial impact of the errors stemming from IT are evaluated within the institution	
	24	Meaning of the IT resources for the organisation in terms of information security	
		Confidentiality	
		Integrity	
		Accessibility	
5) Organizational structure	25	Level of information, knowledge and experience of IT function in terms of meeting the strategic needs of the institution	
	26	Dependency level of critical IT activities on certain IT personnel	
	27	Average level of seniority of the IT personnel within the institution	
	28	Level of dependency on the third parties (in terms of activities) in IT service and infrastructure management	
	29	Level of IT personnel's benefiting from internal and external training opportunities	
	30	Whether the performance of IT personnel is monitored against certain indicators	
	31	Whether the roles and responsibilities of IT personnel are documented	

1	Effect on the institutional reputation of a possible breakdown in the organisation's IT functions in terms of public opinion

Enterprise-level Risk Assessment Form

Enterprise-level Risk Assessment Form Sample

	Subject of Risk Assessment / Risk Factors	Possible Answers and Their Weights*						Question Coefficient**		
1 Strategic Impact		Answer	Weight	Answer	Weight	Answer	Weight	Question Coeff.	Answer (Exp)	Score(Exp)
1	Effect on the institutional reputation of a possible breakdown in the organisation's IT functions in terms of public opinion	Low	20%	Medium	60%	High	100%	4	High	4
2										4
3										4

Possible Answers and Their Weights*						Question Coefficient**		
Answer	Weight	Answer	Weight	Answer	Weight	Question Coeff.	Answer (Exp)	Score(Exp)
Low	20%	Medium	60%	High	100%	4	High	4
Low	20%	Medium	60%	High	100%	4	High	4
Low	20%	Medium	60%	High	100%	4	Medium	2,4
Low	20%	Medium	60%	High	100%	3	High	3

100 /4 =25 point

Enterprise-level Risk Assessment

Enterprise-level Risk Assessment	Low Risk ERS: 1-9	Medium Risk ERS: 10-18	High Risk ERS: 19-25
IT Enterprise-level Controls	Included.	Included.	Included.
IT Governance Controls	Not included.	Recommended to be included.	Included.
IT General Controls (Management-level Controls) – Group 1	Compulsory audit tests included.	• Compulsory audit tests included. • Optional audit tests recommended to be included.	All the compulsory and optional audit tests included.
IT General Controls (Management-level Controls) – Group 2	Not included except for the processes selected depending on the activities of the auditee or whether there is any system change during the audit term (e.g.: DS2, AI2).	• Compulsory audit tests included. • Optional audit tests included for the processes selected depending on the activities of the auditee or whether there is any system change during the audit term (e.g.: DS2, AI2).	All the compulsory and optional audit tests included.

Application-level Risk Assessment Form

Application-level Risk Assessment	Low Risk ARS: 1-9	Medium Risk ARS: 10-18	High Risk ARS: 19-25
Business Applications	Among the compulsory audit tests listed in Group 1 of IT General Controls (Management-level Controls), those which can be conducted on the relevant business application are included.	Among all audit tests listed in Group 1 of IT General Controls (Management-level Controls) and the compulsory tests listed in Group 2, those which can be conducted on relevant business application are included.	Among all audit tests listed in Group 1 of IT General Controls (Management-level Controls) and the compulsory tests listed in Group 2, those which can be conducted on relevant business application are included. In addition, among the optional audit tests listed in Group 2, those which can be conducted on relevant business application are also recommended to be included.
Operating/Server Systems	Audit tests on IT General Controls at the Infrastructure level may be included, depending on the operating logic of the selected business application and its interaction with the server system, the number of end user accounts at the server system level, and the quality of the programs that can be run directly on the server system.	Audit tests on IT General Controls at the Infrastructure level are recommended to be included, depending on the operating logic of the selected business application and its interaction with the server system, the number of end user accounts at the server system level, and the quality of the programs that can be run directly on the server system.	Audit tests on IT General Controls at the Infrastructure level are included, depending on the operating logic of the selected business application and its interaction with the server system, the number of end user accounts at the server system level, and the quality of the programs that can be run directly on the server system.
Database Systems	Audit tests on IT General Controls at the Infrastructure level may be included, depending on the operating logic of the selected business application and its interaction with the database system, the number of end user accounts at the database system level, methods of access to database systems and the quality of the programs that can be run directly on the database system.	Audit tests on IT General Controls at the Infrastructure level are recommended to be included, depending on the operating logic of the selected business application and its interaction with the database system, the number of end user accounts at the database system level, methods of access to database systems and the quality of the programs that can be run directly on the database system.	Audit tests on IT General Controls at the Infrastructure level are included, depending on the operating logic of the selected business application and its interaction with the database system, the number of end user accounts at the database system level, methods of access to database systems and the quality of the programs that can be run directly on the database system.

Application-level Risk Assessment Form

#	Risk assessment questions for applications	Answer
1	Importance of application in terms of forming financial accounts, updating financial statements and financial reporting	
11	Technological transformation (e.g. main servers) on the applications during audit period	
12	Frequency of changes made on the application during audit period	
13	Level of dependency on the third parties in management of the application	
14	Ratio of interruptions on the application during audit period	
15	Whether up-to-date technologies are followed in terms of the application's programming language and infrastructure (database etc.)	
16	Value referred to the application by the organisation in terms of information security	
	Confidentiality	
	Integrity	
	Accessibility	

Importance of application in terms of forming financial accounts, updating financial statements and financial reporting

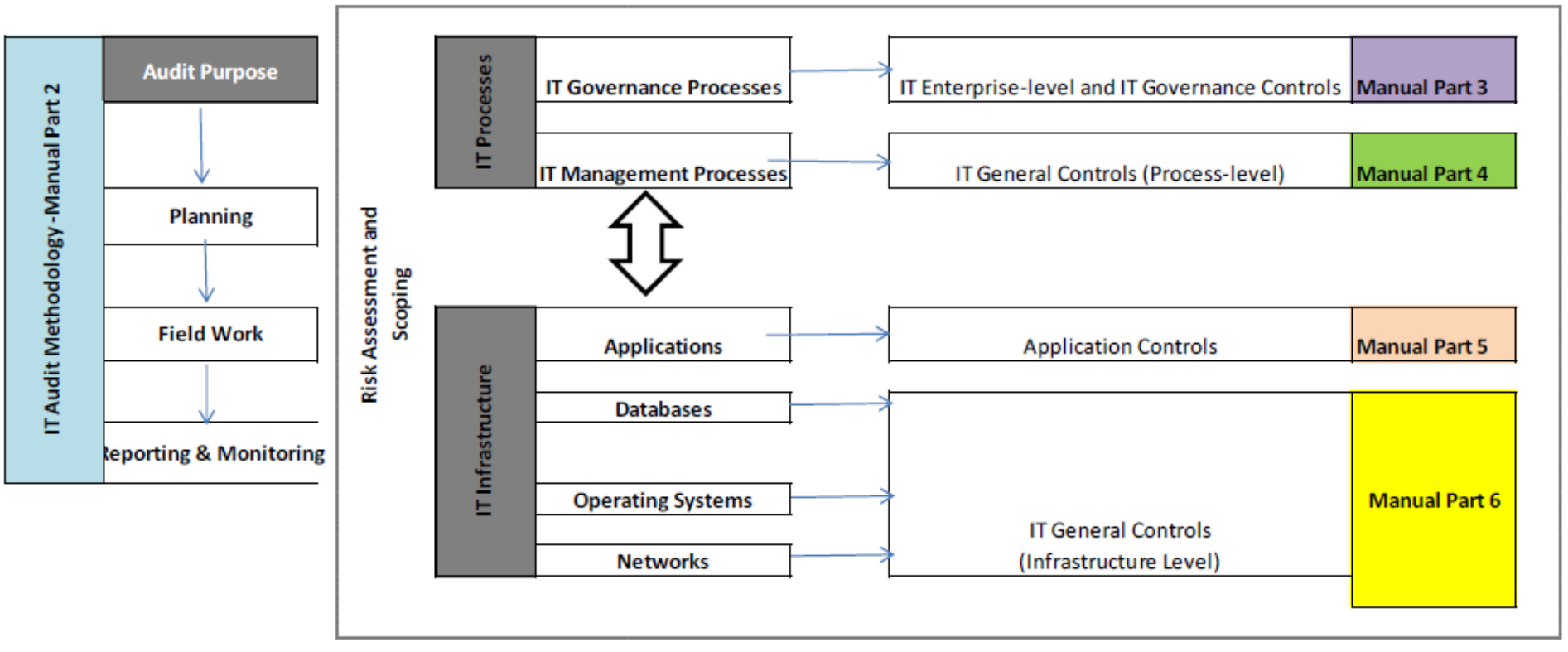
Application-level Risk Assessment Form

#	Risk assessment questions for applications	Possible Answers and Their Weights*							Application (Example)	
		Answer	Weight	Answer	Weight	Answer	Weight	Question Coefficient	Answer (Exp)	Score(Exp)
1	Importance of application in terms of forming financial accounts, updating financial statements and financial reporting	Low	20%	Medium	60%	High	100%	7	Medium	4,2
2	Application's level of support to the main activity fields and business processes of the organisation	Low	20%	Medium	60%	High	100%	7	Medium	4,2
3	Impact of the application on the organisation's services and activities	Low	20%	Medium	60%	High	100%	7	Medium	3,6
4	Application's level of criticality in terms of the services provided to the citizens	Low	20%	Medium	60%	High	100%	7	Medium	4,2

Possible Answers and Their Weights*						Application (Example)	
Answer	Weight	Answer	Weight	Answer	Weight	Question Coefficient	Answer (Exp)	Score(Exp)
Low	20%	Medium	60%	High	100%	7	Medium	4,2
Low	20%	Medium	60%	High	100%	7	Medium	4,2
Low	20%	Medium	60%	High	100%	7	Medium	3,6
Low	20%	Medium	60%	High	100%	7	Medium	4,2
Low	20%	Medium	60%	High	100%	5	Medium	3

100 /4 =25 point

IT Audit Methodology



Field Work

Enterprise-level Controls	
C1	Mechanisms and communication channels are set up and operated so that IT operates in line with the institutional objectives. Accordingly, necessary policies and procedures are established taking into account the objectives, principles and activities.
C2	An institutional architectural structure is established in which all layers of business processes, information, data, applications and technological infrastructure existing within the institution are addressed. Some standards and procedures related to the institutional architecture are established and the relationships between the institution's IT architectural components (e.g. applications, data structures, etc.) are defined.
C3	A project and portfolio management framework is established within the institution. In this context, IT investments are determined and prioritized according to institutional objectives, institutional architecture and resource needs. This framework also includes the master plan, resource planning, identification of outputs, user approvals, quality assurance, test planning, acceptance and review processes.

Field Work

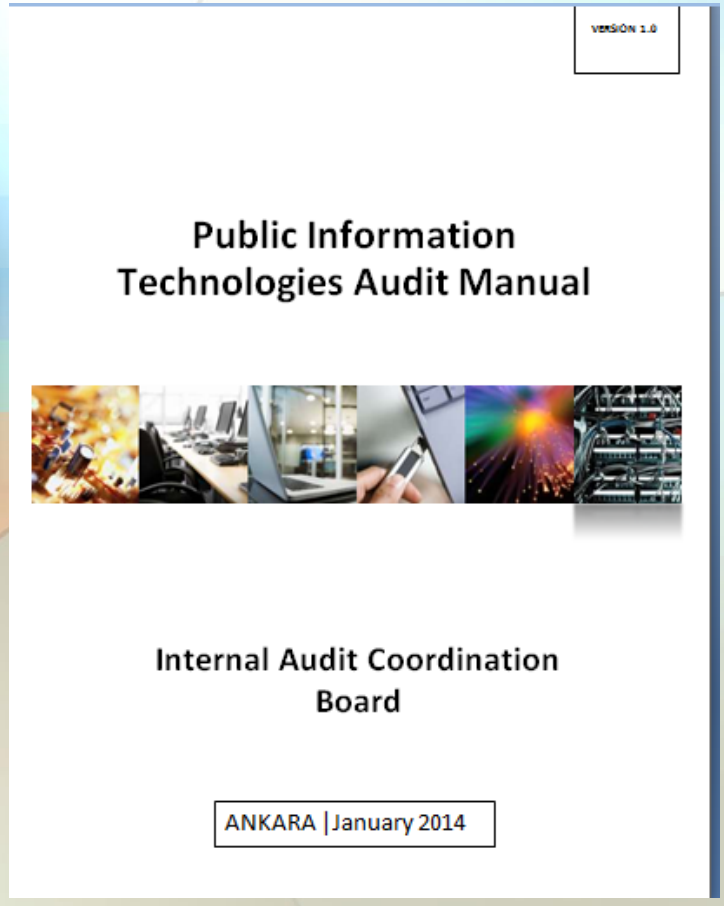
Risk – Control Match

Enterprise-level Controls Risk – Control Match					
Risks	**C1**	**C2**	**C3**	**C4**	**C5**
R1. Inability of IT to understand the management approach of the institution correctly	+			+	
R2. Inability of IT to support the institutional strategies and objectives	+	+	+		
R3. Inability to use the institution's resources efficiently and effectively due to IT structure not working in line with institutional objectives		+	+	+	
R4. Making poor IT investments due to inability to determine investment areas correctly and/or not taking the management's approval		+	+		
R5. Inconsistencies between the institution's technological equipment, software and hardware		+			
R6. Inability to develop IT processes in line with business objectives	+	+	+	+	
R7. IT structure incompliant with applicable legislation and by-laws	+				+

Field Work

Audit Tests				
C1 - Mechanisms and communication channels are set up and operated so that IT operates in line with the institutional objectives. In this direction, the necessary policies and procedures are established taking into account the objectives, principles and activities.				
#	Audit tests	D/O[1]	C/O[2]	CL[3]
C1.T1	The level where IT is positioned in the organisational structure is observed by assessing its importance within the organisation.	D	C	2
C1.T2	IT organisational structure within the organisation is examined and it is checked whether the structure is set up in line with the IT priorities and business objectives.	D	C	2
C1.T3	It is observed within the organization that the roles and responsibilities of all IT personnel are defined and that they are identified in the most appropriate manner to implement the institutional IT objectives.	D	C	2

[1] D/O: Design/Operation
[2] C/O: Compulsory/Optional
[3] CL: Competence Level, (see. Table 1)



QUESTIONS

Ahmet Bora ÖZTEKİN CIA,CGAP
Internal Auditor
Ministry of National Defense-TR