THE Open GROUP

The Open Group® Certification for People: Credentials Program

Integrating Risk and Security Conformance Requirements

Version 1.0
July 2019

The Open Group® Certification for People: Credentials Program
Integrating Risk and Security Conformance Requirements

Document Number: X193

Published by The Open Group, July 2019.

Comments relating to the material contained in this document may be submitted to:

The Open Group, 800 District Avenue, Suite 150, Burlington, MA 01803, United States

or by electronic mail to:

ogspecs@opengroup.org

Contents

1. Introduction

This document, the Integrating Risk and Security Conformance Requirements, is an integral part of The Open Group® Certification for People: Credentials Program (the Program).

This document defines the requirements for issuance of credentials to individuals within the Program, which in turn form the learning requirements for Accredited Training Courses.

1.1 Terminology and Definitions

This table defines terms or clarifies the meaning of words used within this document. Where an acronym is also used, it is provided in parentheses.

Accredited Training Course (ATC)	A training course, operated by a training course provider, that has successfully completed the accreditation process and which is listed in the register of Accredited Training Courses on the Certification Authority's website.
Body of Knowledge (BoK)	The set of information within the subject area that a Candidate is expected to have understanding of in order to earn the credential within the Program.
Candidate	A person seeking to earn the credential.
Certification Authority	The organization that manages the day-to-day operations of the Program. The Open Group is the Certification Authority for the Program.
Credential	Recognition of an achievement earned by a Candidate. A credential is backed by metadata providing detailed information about it. A credential is earned by passing an Indicator of Compliance.
Examination Provider	The organization(s) contracted by The Open Group to provide and administer examinations.
Indicator of Compliance	The assessment used to determine if a Candidate has met the criteria to earn the credential.
Key Learning Point (KLP) (terminal objective)	A self-contained learning objective, derived from the Body of Knowledge with a unique reference, typically ranging from 2 to 15 minutes' study time.
Learning Outcome (supporting objective)	What the Candidate should know, understand, or be able to do on completion of learning about one or more Key Learning Points. Each Learning Outcome defines the learning level (depth of knowledge) required to achieve the Key Learning Point.
Learning Unit	A related set of Learning Outcomes. It is expected that a Learning Unit would equate to between 30 and 90 minutes of taught learning equivalence.

2. Conformance Terminology

The Conformance Requirements are specified as sets of Learning Units. To earn a credential, Candidates are required to complete the applicable Learning Units and successfully pass the corresponding Indicator of Compliance (see Section 4).

The definition of the Learning Units does not dictate the structure, order, or time duration that topics should be taught in an Accredited Training Course. Training organizations are free to structure their courses as they see fit, so long as Candidates have the mandatory Learning Outcomes at the end of a course for the target credential.

2.1 Learning Unit Format

Each Learning Unit is defined in a table organized as follows:

	UNIT Number	Requirement, Terminal Objective(s), Supporting Objective(s)		Bloom's Taxonomy Level	Literature Reference
(A)	1.	….		(E)	(F)
(B)		1.1	The Candidate ...		
			The Candidate is able to:		
(C)		1.1.1			
		1.1.2			
		1.1.3			
		1.1.4			
		1.1.5			
(D)	Assessment terms:		…		

Notes

(A) Exam requirement; i.e., Learning Unit. Typically this corresponds with a chapter or major section of a document in the Body of Knowledge.

(B) Terminal objective; the high-level part of the Key Learning Point(s).

(C) Supporting objective; the actual Learning Outcomes.

(D) Key terms from the low-level part of the Key Learning Point(s) (*aka* "exam terms").

(E) Bloom's Taxonomy Level; defined using "Bloom" action verbs (see Section 6.1).

(F) Literature reference; this is a reference back to chapters, paragraphs, diagrams, tables, etc. within the Body of Knowledge. **This is required for traceability.**

3. Conformance Requirements

To earn this credential Candidates must complete all Learning Units defined in this section and successfully pass the corresponding Indicator of Compliance (see Section 4).

3.1 UNIT 1: Introduction

UNIT Number	Requirement, Terminal Objective(s), Supporting Objective(s)		Bloom's Taxonomy Level	Literature Reference
1.	The purpose of this Learning Unit is to create an understanding of the topic of Enterprise Security Architecture and how it relates to Enterprise Architecture within a TOGAF context.			§1
	1.1	The Candidate understands the essential concepts of security and risk, and can relate them to the TOGAF standard.		
		The Candidate is able to:		
	1.1.1	Describe essential security and risk concepts and their position in the TOGAF ADM.	2_Understanding	§1.1, Fig.1
	1.1.2	Explain the difference between the Enterprise Risk Management, which is largely focused on current operations, and risk within the TOGAF standard that focuses on: • Architecture iteration/project risk (delivering the target/ roadmap) • Being able to meet an organizational target in the Target Architecture, and its implementation	2_Understanding	§1.2
	1.1.3	Explain the relationship between security controls, security services, and how these are described in the TOGAF ADM.	2_Understanding	§1.3
	1.1.4	Explain definition of risk (the effect of uncertainty on reaching objectives), usage within enterprise risk and financial risk standards, and the impact on assessing risk in the most important assessment activities in Phase A, Phase E, and Phase G of the TOGAF ADM.	2_Understanding	§3.1.1
Assessment terms:	Enterprise Architecture, Security Architecture, Information Security Management (ISM), Enterprise Risk Management (ERM), concepts in Fig.1, architecture project risk, ISO 31000, Architecture Building Block (ABB), Solution Building Block (SBB), Security Services, Services Catalog, SABSA®			

3.2 UNIT 2: IT Security and Risk Standards

UNIT Number	Requirement, Terminal Objective(s), Supporting Objective(s)		Bloom's Taxonomy Level	Literature Reference
2.	The purpose of this Learning Unit is to create an understanding of the relationship with other IT security and risk standards.			
	2.1	The Candidate understands how international IT security and risk standards are related to the TOGAF standard.		
		The Candidate is able to:		
	2.1.1	Summarize the relationship of the TOGAF standard to IT security and risk standards.	2_Understanding	§2.1-2.8
Assessment terms:		ISO/IEC 27000 family of standards, ISO 31000, National Cybersecurity Frameworks, NIST, COBIT®, O-ESA, O-ISM3, Open FAIR™, SABSA		

3.3 UNIT 3: Enterprise Security Architecture

UNIT Number	Requirement, Terminal Objective(s), Supporting Objective(s)		Bloom's Taxonomy Level	Literature Reference
3.	The purpose of this Learning Unit is to create an understanding of the concept of Enterprise Security Architecture in detail.			§3
	3.1	The Candidate understands the concept of Enterprise Security Architecture.		
		The Candidate is able to:		
	3.1.1	Describe the concept of Enterprise Security Architecture.	2_Understanding	§3
Assessment terms:		Enterprise Security Architecture, risk, ADM, ISM, ERM		
	3.2	The Candidate understands the concept of Enterprise Risk Management (ERM).		
		The Candidate is able to:		
	3.2.1	Explain the concept of ERM.	2_Understanding	§3.1
	3.2.2	Explain the concept of business risk in relation to the concept of cyber risk areas.	2_Understanding	§3.1.1, Fig.2-3
	3.2.3	Discuss the core concepts of ERM.	2_Understanding	§3.1.2
	3.2.4	Illustrate how a Security Architect can address risk (the effect of uncertainty) in developing and communicating a Target Architecture.	2_Understanding	§3

UNIT Number	Requirement, Terminal Objective(s), Supporting Objective(s)		Bloom's Taxonomy Level	Literature Reference
Assessment terms:		Risk, risk area, secure behavior, ADM, ISM, ERM, IT security, risk management, business stack, cyber risk area, SABSA, operational risk model (SABSA), risk appetite, ISO 31000, key risk areas, BIA, risk assessment, business risk model, risk register, risk mitigation plan, risk treatment plan		
	3.3	The Candidate understands the concept of Information Security Management (ISM).		
		The Candidate is able to:		
	3.3.1	Translate the three core pillars (the CIA triad: Confidentiality, Integrity, Availability) of security into business terms.	2_Understanding	§3.2.1
	3.3.2	Illustrate how a Security Architect can address the generally accepted areas of concern with regard to Information Security.	3_Applying	§3.2.1
	3.3.3	Discuss the core concepts of ISM.	2_Understanding	§3.2.3
Assessment terms:		ISM, security incident, security triad (CIA), availability, availability status, SABSA, business attribute model, areas for concern (asset protection, risk assessment, access control, audit, availability), privacy, ISO/IEC 27000 family of standards, ISO/IEC 27001 main categories, operational security processes, services catalog		

3.4 UNIT 4: Security as a Cross-Cutting Concern

UNIT Number	Requirement, Terminal Objective(s), Supporting Objective(s)		Bloom's Taxonomy Level	Literature Reference
4.	The purpose of this Learning Unit is to illustrate why Security Architecture is a cross-cutting concern, pervasive through the whole Enterprise Architecture.			§4
	4.1	The Candidate understands why security is a cross-cutting concern through the architecture.		
		The Candidate is able to:		
	4.1.1	Illustrate areas in the architecture where a stakeholder's security concern is expressed in more than one domain.	3_Applying	§4
Assessment terms:		Security as a cross-cutting concern, business, data, application, technology		

3.5 UNIT 5: Security and Risk Concepts in the TOGAF ADM

UNIT Number	Requirement, Terminal Objective(s), Supporting Objective(s)	Bloom's Taxonomy Level	Literature Reference
5.	The purpose of this Learning Unit is to learn how to apply core security concepts to the phases of the TOGAF ADM.		§5

UNIT Number	Requirement, Terminal Objective(s), Supporting Objective(s)		Bloom's Taxonomy Level	Literature Reference
	5.1	The Candidate can apply core security concepts to the TOGAF ADM.		
		The Candidate is able to:		
	5.1.1	Choose security artifacts to build the security context.	3_Applying	§5.1.1-5
	5.1.2	Compare stakeholder analysis outcomes.	4_Analysing	§5.2
	5.1.3	Explain how the stakeholder requirements can be applied to the security blueprint.	2_Understanding	§5.2
	5.1.4	Explain security-related Business Architecture artifacts.	2_Understanding	§5.3.1-7
	5.1.5	Select the required security controls for a specific scenario.	4_Analysing	§5.5
	5.1.6	Illustrate how the concepts of security services catalogs and security building blocks enable reuse.	3_Applying	§5.6
	5.1.7	Write a risk mitigation plan.	3_Applying	§5.6.1
	5.1.8	Describe the artifacts of Security Architecture implementation governance.	2_Understanding	§5.8
	5.1.9	Describe the key concepts of the Architecture Change Management phase.	2_Understanding	§5.9
Assessment terms:		Artifacts, core security concepts, business drivers/business objectives, security principles, risk appetite, key risk areas, BIA, risk classification, security resource plan, risk-related concerns, Architecture Vision, stakeholders, stakeholder requirements, Business Attribute Profile (SABSA), viewpoint, business case, Business Architecture, secure policy architecture, security domain model, trust framework, risk assessment, business risk model, risk register, legislation and regulations, control framework register, ISO/IEC 27001, security audit, ISAs, security services catalog, business services catalog, security services, security classification, data quality, Technology Architecture, opportunities and solutions, risk mitigation plan, baseline Security Architecture, migration planning, mitigation strategy, security impact analysis, implementation governance, security audit, training and awareness, Architecture Change Management, ERM, architecture governance, change, requirements management		
	5.2	The Candidate understands the relationship between the Architecture Content Metamodel and ISM and ERM, respectively.		
		The Candidate is able to:		
	5.2.1	Describe how concepts from the Architecture Content Metamodel can be used to model ISM and ERM.	2_Understanding	§5.11
Assessment terms:		TOGAF Architecture Content Metamodel, ISM, ERM		

UNIT Number	Requirement, Terminal Objective(s), Supporting Objective(s)		Bloom's Taxonomy Level	Literature Reference
	5.3	The Candidate can apply SABSA techniques relevant for developing the Security Architecture.		
		The Candidate is able to:		
	5.3.1	Explain the SABSA Business Attribute Profiling technique.	2_Understanding	§5.10.1
	5.3.2	Understand that the SABSA framework is much broader than Business Attribute Profiling.	2_Understanding	§5.10.1[1]
Assessment terms:		Business Attribute Profile (SABSA), traceability mapping, performance management, business attribute taxonomy, control objectives, security objectives		

[1] Refer to Enterprise Security Architecture: A Business-Driven Approach, J. Sherwood, A. Clark, D. Lynas, CRC Press, 2005.

4. Indicators of Compliance

The Indicator of Compliance for this credential is The Open Group approved assessment delivered by an Accredited Training Course Provider, which covers the breadth of the Learning Outcomes for the credential. This can take the form of a test, in-course assessment of practical exercises, completion of a workbook, or other approved format. Lower-order Learning Outcomes, for example, can be taught using an interactive lecture supplemented by practical exercises like individual tasks to demonstrate application of theory. Higher-order Learning Outcomes, on the other hand, require more complex practical exercises; i.e., in delegate groups or individual analysis of practical cases. The Accredited Training Course Provider will assess the Candidates at each respective learning level, and will provide a copy of the assessment, together with supporting documentation demonstrating that the assessment is objective and fair. The Certification Authority will audit the assessment as part of accreditation of the course.

The learning levels that need to be addressed for this credential range from 2 to 4. Refer to Section 6 for examples of learning activities for each (Bloom) learning level.

5. Body of Knowledge

This section defines the Body of Knowledge for this credential. It provides the list of documents from which Key Learning Points are derived, together with a Document Reference (usually the document number and a chapter/section reference).

5.1 Documents Comprising the Body of Knowledge

The Body of Knowledge for this credential is based on the following documents:

Document Reference	Document Title
G152	Integrating Risk and Security within a TOGAF® Enterprise Architecture, The Open Group Guide, January 2016, published by The Open Group; refer to: www.opengroup.org/library/g152

Supplemental Reading

The following documents are recommended reading for students as supplemental reading.

Document Reference	Document Title
W117	TOGAF® and SABSA® Integration, White Paper, October 2011, published by The Open Group; refer to: www.opengroup.org/library/w117

6. Rationale (Informative)

This section contains informative rationale.

6.1 Bloom's Taxonomy

The terms used to define the depth of learning are drawn from Bloom's Taxonomy.

Bloom's Taxonomy	Level	Cognitive Dimension	Examples of Action Verbs
Lower-order Learning Skills	1	Remembering	Define, list, describe …
	2	Understanding	Explain, summarize …
	3	Applying	Apply, illustrate, classify …
Higher-order Learning Skills	4	Analyzing	Analyze, arrange, select …
	5	Evaluating	Summarize, justify …
	6	Creating	Construct, rewrite, plan …

6.2 Learning Levels

The learning levels that need to be addressed for this credential range from 1-2. The following table shows examples of learning activities for each (Bloom) learning level.

Level	Cognitive Dimension	Examples of Learning Activities
1	Remembering	Lecture, video-clip, examples, illustrations, metaphors, guided reading
2	Understanding	Interactive lecture, Q&A, group discussions, tests
3	Applying	Practice exercises, demonstrations, simple projects, simulations, role play
4	Analyzing	Practical (case-based) exercises, higher-level tests
5	Evaluating	Project, complex case studies, appraisals, debating
6	Creating	Development of plans, complex projects, constructing