IIAI Open Conference Publication Series
IIAI Letters on Institutional Research
Vol. 005, LIR457
DOI: https://doi.org/10.52731/lir.v005.457

Mapping ISO 15408 Security Functions to SDLC Phases: Insights from a Questionnaire-Based Study

Samodi Fernando [*], Shigeaki Tanimoto [†],
Hideto Ogasawara [*]

Abstract

The ISO/IEC 15408 standard provides a systematic approach to defining security functions that are essential for software systems, yet integrating these security functions into the Software Development Life Cycle (SDLC) phases remains challenging. This research aims to establish connections between ISO 15408 security functions and SDLC phases by using survey data from software professionals. The survey collected 144 responses from software developers together with quality assurance engineers and security professionals. The analysis shows patterns of security function implementation, which reveal both early-phase adoption gaps and inconsistent audit-related practices. The research evidence demonstrates how better integration of ISO 15408 functions with SDLC would enhance secure software development practices. This research provides practical insights about uniting security standards with actual development workflows.

Keywords: Downstream, Midstream, Security Families, Security targets, Upstream

1 Introduction

Software security essential in cyberattacks, data leaks, and unauthorized access, indicating comprehensive security functions throughout the software development lifecycle. ISO/IEC 15408 has established a security evaluation criterion for judging whether products and systems related to information technology have been appropriately designed and whether their designs have been correctly implemented [1] [2]. ISO/IEC 15408 (Common Criteria, CC) is an intentional standard for the security evaluation of information systems, it can be applied throughout the software life cycle to improve the security of information systems. [3].

Software security is an essential requirement in cyberattacks, data leaks, and unauthorized access, indicating comprehensive security functions throughout the software development lifecycle. ISO/IEC 15408 has established a security evaluation criterion for judging whether products and systems related to information technology have been adequately designed and whether their designs have been correctly implemented [1] [2]. ISO/IEC 15408 (Common Criteria, CC) is an international standard for the security evaluation of information systems and can be applied throughout the software life cycle to improve the security of information systems. [3].

A Security Target (ST) [4] [5], which contains specifications of the security functions of the target system, is the most important document in the development of the system according to ISO/IEC 15408. [6]. It is a challenge for software development teams, including project managers and

[*] Chiba Institute of Technology, Chiba, Japan
[†] Japan International University, Tsukuba, Japan

quality assurance engineers, to maintain and implement those security targets into the Software Development Lifecycle (SDLC) phases. This lack may lead to severe damages like Data privacy and integrity, data recoverability and vulnerability, Improper media refinement [7], cyberattacks, and data leaks. It may take a lot of effort and time to rework the security functions.

By using the Common Criteria can be made of information technology products with more systematic security standardization. [8] [9]. This research aims to develop a structured mapping between the functional requirements of the ISO/IEC 15408 CC security and the phases of the software development process. By reviewing the ISO/IEC 15408 security function classes and their families based on questionnaire responses from the security specialists and decision makers based in the Japanese IT sector.

This research will contribute to secure software engineering by offering a systematic approach to implementing standardized security functions during software development. The proposed mapping framework can support developers, security analysts, project managers, and software quality assurance engineers in integrating, testing, and maintaining appropriate security controls at the right development phases.

2 Research Methodology

The study utilized a quantitative research approach where a structured questionnaire was distributed and a Chi-Square statistical test was used. The target participants were security experts and stakeholders from Japan's IT industry.

The questionnaire was created to collect practical information about the use of individual ISO/IEC 15408 security functional families at various stages of the SDLC, categorized as upstream (design), midstream (development), and downstream (testing). Every participant chooses the phases in which they tend to apply every security function family.

A total of 144 answers were available. The Chi-square test of independence was used to examine the relationship among security function families and SDLC phases. This statistical method answered the question: Was the distribution of the responses for each of the security functions significantly associated with any of the development activities? Afterward, color-coded heatmaps were drawn to show the prevalence of mappings.

3 Analysis and Findings

3.1 Initial Questionnaire Observation

In the first phase, a structured questionnaire was distributed to a group of professionals (software developers, project managers, security experts, and quality assurance engineers) working in the IT sector all over Japan. This questionnaire aimed to collect real-world scenario experience on the use of ISO/IEC 15408 CC security functional requirements in the various stages of the SDLC.

However, the responses have not been as expected. Around 70–80% of the respondents say that they are not aware of or do not use the ISO 15408 CC security mechanisms in their design processes. This reflects an overall lack of awareness and use of standard security capabilities within everyday development practices. Table 1 is a sample of responses to the questionnaire.

Table 1: A Sample data table of Initial Questionnaire responses

Cryptographic Support Function

	Which phases of the Software Development Life Cycle (SDLC) cover the following (FCS) cryptography requirements? For each requirement, select all that apply.	Total	1	2	3	4	
			Upstream (design stage)	Midstream (Development stage)	Downstream (Testing Phase)	Not applicable	No answer
Q6S1	FCS_CKM - Cryptographic Key Management Example: Generation and secure storage of cryptographic keys	120 100.0	12 10.0	16 13.3	10 8.3	90 75.0	0 -
Q6S2	FCS_COP - Cryptographic Operation Example: Using cryptography to protect sensitive information	120 100.0	16 13.3	17 14.2	12 10.0	88 73.3	0 -
Q6S3	FCS_RBG - Random Bit Generation Example: Generating random bits for cryptographic protocols	120 100.0	11 9.2	14 11.7	9 7.5	93 77.5	0 -
Q6S4	FCS_RNG - Generation of Random Numbers (Example: Random number generation for cryptographic key generation)	120 100.0	11 9.2	11 9.2	6 5.0	96 80.0	0 -

3.2 Questionnaire Refinement and Focused Sampling

Because the results were not as we expected, we adapted the questions to receive more clear feedback. The questionnaire was redesigned, and the "Not Applicable" alternative was to prompt a more decisive response. The target audience was narrowed down to security professionals and IT decision-makers who are directly responsible for or involved in security measures within their respective businesses. These modifications guaranteed that the collected data would reflect reasoned views regarding when and how to integrate security activities into the SDLC. Table 2 is a sample of responses to the redesigned questionnaire.

Table 2: A sample data table of restructured questionnaire responses

Cryptographic Support Function

Q5	In which phases of your Software Development Life Cycle (SDLC) do you cover the following (FCS) cryptographic requirements? Please select the single most relevant phase where you currently apply security features. If you are not currently using security features, please select the phase where you think you should apply them.	Total	1 Up-stream (design stage)	2 Mid-stream (Development stage)	3 Down-stream (Testing Phase)
Q5S1	FCS_CKM - Cryptographic Key Management Example: Generation and secure storage of cryptographic keys	144	63	43	38
Q5S2	FCS_COP - Cryptographic Operation Example: Using cryptography to protect sensitive information	144	70	37	37
Q5S3	FCS_RBG - Random Bit Generation Example: Generating random bits for cryptographic protocols	144	51	40	53
Q5S4	FCS_RNG - Generation of Random Numbers (Example: Random number generation for cryptographic key generation)	144	49	44	51

3.3 Statistical Analysis and Mapping Criteria

Using the refined responses (n = 144), we performed the Chi-Square test of independence to examine whether there is a statistically significant association between each ISO 15408 cc security function family and specific SDLC phases.

- If the Chi-Square test showed a significant dependency (p-value < 0.05) between a security family and a particular SDLC phase, that phase was considered the primary phase for mapping the security family.
- If no significant dependency was found, we considered the phases by frequency of selection:
  - ✓ The phase with the highest response count was marked as High relevance.
  - ✓ The second highest is Medium, and
  - ✓ The lowest is Low relevance.

4 Mapping ISO 15408 Security Functions to SDLC Phases

The study results. Map the ISO/IEC 15408 (CC) security functional families in a practical manner with the SDLC phases is being demonstrated in this chapter. The map is developed by correlating the structure of the standard ISO/IEC 15408 part 2 and practical information obtained from a 144-respondent empirical survey of Japanese IT professionals such as security experts and decision-makers.

In cases where statistical dependence was observed through Chi-Square analysis, the relevant SDLC phase was directly mapped to the corresponding security function. Where no significant dependence was found, the development phase with the highest number of responses was proposed as the most suitable phase for implementation. This choice is justified by the collective professional judgment of experienced security personnel, reflecting practical feasibility and current industry trends. Assigning the security function to the phase where it is most frequently applied ensures that the mapping aligns with real-world practices, thereby increasing the likelihood of adoption and effectiveness in securing software systems.

This proposed mapping not only operationalizes a complex standard but also offers actionable guidance to development teams, project managers, and security architects striving to incorporate recognized security measures within their existing SDLC models.

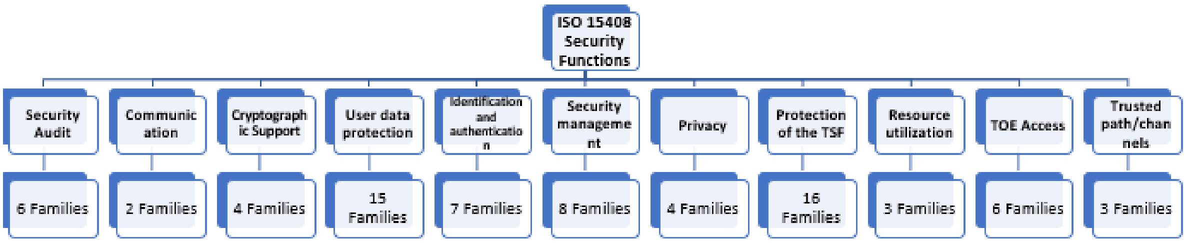

Figure 1: Overview of ISO 15408 Security Functions

4.1 Security Audit Function (FAU)

Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. [10]

Table 3: Security Audit Function Map

Security Function	Upstream	Midstream	Downstream
Automatic Response (FAU_ARP)	High		
Data Generation (FAU_GEN)	High	Medium	Low
Audit Analysis (FAU_SAA)	Medium	Low	High
Audit Review (FAU_SAR)	Medium	Low	High
Event Selection (FAU_SEL)	Medium	Low	High
Data Storage (FAU_STG)	Medium	Low	Medium

4.2 Communication Function (FCO)

The FCO class provides two families that are explicitly concerned with assuring the identity of a party participating in a data exchange. These families are related to assuring the identity of the originator of transmitted information (proof of origin) and assuring the identity of the recipient of transmitted information (proof of receipt) [10].

Table 4: Communication Function Map

Security Function	Upstream	Midstream	Downstream
Non-repudiation of origin (FCO_NRO)	High	Medium	Low
Non-repudiation of Receipt (FCO_NRR)	High	Low	Medium

4.3 Cryptographic Support Function (FCS)

The TSF may employ cryptographic functionality to help satisfy several high-level security objectives. These include but are not limited to, identification and authentication, nonrepudiation, trusted path, trusted channel, and data separation. [10]

Table 5: Cryptographic Support Function Map

Security Function	Upstream	Midstream	Downstream
Cryptographic Key Management (FCS_CKM)	High		
FCS_COP - Cryptographic Operation	High		
FCS_RBG - Random Bit Generation	Medium	Low	High
FCS_RNG - Generation of Random Numbers	Medium	Low	High

4.4 User Data Protection (FDP)

The FDP addresses user data within a TOE during import, export, and storage, as well as security attributes directly related to user data. [10]

Table 6: User Data Protection Function Map

Security Function	Upstream	Midstream	Downstream
Access Control Policy (FDP_ACC)	High		
Access Control Functions / Cryptographic Operation (FDP_ACF)	High	Medium	Low
Data Authentication (FDP_DAU)	Medium	Medium	High
Export from the TOE (FDP_ETC)	Medium	Low	Medium
Information Flow Control Policy (FDP_IFC)	High	Medium	Low
Information Flow Control Functions	High	Medium	Low
FDP_IRC - Information Retention Control (FDP_IFF)	High	Low	Medium
Import from outside of the TOE (FDP_ITC)	Low	High	Medium
Internal TOE Transfer (FDP_ITT)	High	Medium	Low
Residual Information Protection (FDP_RIP)	High	Medium	Low
Rollback (FDP_ROL)	High	Low	Medium
Stored Data Confidentiality (FDP_SDC)	High	Low	Medium
Stored Data Integrity (FDP_SDI)	Medium	High	Low
Inter-TSF User Data Confidentiality Transfer Protection (FDP_UCT)	High	Medium	Low

Inter-TSF User Data Integrity Transfer Protection (FDP_UIT)	Medium	High	Low

4.5 Identification and Authentication (FIA)

The FIA contains requirements for defining values for some unsuccessful authentication attempts and TSF actions in cases of authentication attempt failures. [10]

Table 7: Identification and Authentication Map

Security Function	Upstream	Midstream	Downstream
Authentication Failures - Detect and log authentication failures (FIA_AFL)	High		
Authentication Proof of Identity (FIA_API)	High	Medium	Low
User Attribute Definition (FIA_ATD)	High	Low	Medium
Specification of Secrets (FIA_SOS)	High	Medium	Low
User Authentication (FIA_UAU)	High	Low	Medium
User Identification (FIA_UID)	Low	Medium	High
User-Subject Binding (FIA_USB)	High	Low	Medium

4.6 Security Management (FMT)

The FMT is intended to specify the management of several aspects of the TSF: security attributes, TSF data, and functions. [10]

Table 8: Security Management Function Map

Security Function	Upstream	Midstream	Downstream
Limited Capabilities and Availability (FMT_LIM)	High	Medium	Low
Management of Functions in TSF (FMT_MOF)	High	Medium	Low
Management of Security Attributes (FMT_MSA)	High	Low	Medium
Management of TSF Data (FMT_MTD)	High	Low	Medium
Revocation (FMT_REV)	High	Low	Medium
Security Attribute Expiration (FMT_SAE)	High	Low	Medium
Specification of Management Functions (FMT_SMF)	High		
Security Management Roles (FMT_SMR)	High	Low	Medium

4.7 Privacy (FPR)

The FPR contains privacy requirements. These requirements provide user protection against discovery and misuse of identity by other users. [10]

Table 9: Privacy Function Map

Security Function	Upstream	Midstream	Downstream
Anonymity (FPR_ANO)	High	Medium	Low
Pseudonymity (FPR_PSE)	High	Medium	Low
Unlinkability (FPR_UNL)	High	Medium	Low
Unobservability (FPR_UNO)	Medium	High	Low

4.8 Protection of the TSF (Trusted Security Functions) (FPT)

The FPT contains families of functional requirements relating to the integrity and management of the mechanisms that constitute the TSF and the integrity of TSF data. [10]

Table 10: Protection of the TSF Function Map

Security Function	Upstream	Midstream	Downstream
TOE Emanation (FPT_EMS)	High	Medium	Low
Fail Secure (FPT_FLS)	High	Low	Medium
FPT_INI - Initialization	High	Low	Medium
Availability of Exported TSF Data (FPT_ITA)	High	Medium	Low
Confidentiality of Exported TSF Data (FPT_ITC)	Medium	Medium	Low
Integrity of Exported TSF Data (FPT_ITI)	High	Low	Medium
Internal TOE TSF Data Transfer (FPT_ITT)	Medium	High	Low
TSF Physical Protection (FPT_PHP)	High	Medium	Low
Trusted Recovery (FPT_RCV)	High	Medium	Low
Replay Detection (FPT_RPL)	Medium	High	Low
State Synchrony Protocol (FPT_SSP)	Medium	High	Low
Time Stamps (FPT_STM)	Medium	High	Low
Inter-TSF TSF Data Consistency (FPT_TDC)	High	Low	Medium
Testing of External Entities (FPT_TEE)	Low	Medium	High
Internal TOE TSF Data Replication Consistency (FPT_TRC)	High	Medium	Low
TSF Self-Test (FPT_TST)	Medium	Low	High

4.9 Resource Utilization (FRU)

The FRU provides three families that support the availability of required resources, such as processing capability and/or storage capacity. [10]

Table 11: Resource Utilization Function Map

Security Function	Upstream	Midstream	Downstream
Fault Tolerance (FRU_FLT)	High	Low	Medium
Priority of Service (FRU_PRS)	High		
Resource Allocation (FRU_RSA)	High	Medium	Medium

4.10 TOE Access (FTA)

The FTA specifies functional requirements for controlling the establishment of a user's session. [10]

Table 12: TOE Access Function Map

Security Function	Upstream	Midstream	Downstream
Limitation on Scope of Selectable Attributes (FTA_LSA)	High	Medium	Medium
Limitation on Multiple Concurrent Sessions (FTA_MCS)	Medium	Medium	Low
Session Locking and Termination (FTA_SSL)	Medium	High	Low
TOE Access Banners (FTA_TAB)	High	Low	Medium
TOE Access History (FTA_TAH)	High	Medium	Low
TOE Session Establishment (FTA_TSE)	High	Low	Medium

4.11 Trusted Path/Channels (FTP)

Families in this class provide requirements for a trusted communication path between users and the TSF and for a trusted communication channel between the TSF and other trusted IT products. [10]

Table 13: Trusted Path/Channels Function Map

Security Function	Upstream	Midstream	Downstream
Inter-TSF Trusted Channel (FTP_ITC)	High		
Trusted Channel Protocol (FTP_PRO)	High		
Trusted Path (FTP_TRP)	High	Medium	Low

5 Conclusion

This research aimed to map the ISO/IEC 15408 cc security function families to the phases of the SDLC through data-based analysis. Recognizing the importance of integrating security functions early and effectively into software processes, we seek to bridge the gap between formal security standards and practical software engineering workflows.

Initially, a questionnaire was distributed among various stakeholders, including developers, project managers, security specialists, and quality assurance engineers. The results, however, revealed a concerning trend—approximately 75–80% of respondents indicated that they do not actively consider ISO 15408 CC security functions in their work. This outcome high-lighted the importance of a significant awareness and implementation gap in real-world development environments.

In response, the study methodology was refined. The questionnaire was updated to remove ambiguous response options and focus on security-aware roles such as security specialists and decision-makers. Using the responses from 144 participants, a Chi-Square analysis was performed to evaluate the relationship between each ISO 15408 cc security function family and SDLC phases. Where statistically significant dependencies were found, security families were mapped to corresponding SDLC phases. According to the results in the security audit function FAU_ARP family, in the cryptographic support function FCS_CKM - Cryptographic Key Management family and FCS_COP - Cryptographic Operation family, in user data protection function FDP_ACC - Access Control Policy family, in the identification and authentication family FIA_AFL - Authentication Failures family, in resource utilization function FRU_PRS - Priority of Service and trusted path function FTP_ITC - Inter-TSF Trusted Channel and FTP_PRO - Trusted Channel Protocol families were significantly dependent, and other families were not dependent. A weighted frequency method was used for cases without statistical significance to rank the phases as High, Medium, or Low relevance.

The findings of this research contribute a data-driven model for aligning ISO/IEC 15408 cc security functions with SDLC phases. This model can serve as a practical guideline for organizations aiming to enhance the security posture of their software systems from the early stages of development. Furthermore, it underscores the urgent need to raise awareness and improve training on standardized security practices among all software professionals, not just those in security-specific roles.

References

[1] K. Y. J. M. K. S. Y. G. a. J. C. Gefei Sunl, "A Supporting Tool for Creating and Maintaining Security Targets According to ISO/IEC 15408," 2012.

[2] A. I. H. S. Y. G. a. J. C. Ning Zhang, "An Analysis of Software Supportable Tasks Related with ISO/IEC 15408," International Conference on Computational Intelligence and Security, 2013.

[3] J. M. N. Z. Y. G. a. J. C. Da Bao, "Supporting Verification and Validation of Security Targets with ISO/IEC 15408," International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC), 2013.

[4] H.-k. k. S.-m. H. Eun-Ser Lee, "Analysis the priority of security requirement items for the process improvement by ISO/IEC 15504 and ISO/IEC 15408," Fifth International Conference on Software Engineering Research, Management and Applications, 2007.

[5] N. M. S. J. Tahereh Nayerifard, "An Approach for Software Security Evaluation Based on ISO/IEC 15408 in the ISMS Implementation," International Journal of Computer Science and

Information Security, 2013.

[6] J. M. N. Z. Y. G. a. J. C. Da Bao, "Supporting Verification and Validation of Security Targets with ISO/IEC 15408," International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC), 2013.

[7] S. Patnaik, "A Study on Data Storage Security Issues in Cloud Computing," 2nd International Conference on Intelligent Computing, Communication & Conference, 2016.

[8] R. Y. Yoso Adi Setyoko, "Security Protection Profile on Smart Card System," International Conference on Information and Communication Technology, 2018.

[9] R. Y. Yoso Adi Setyoko, "Security Protection Profile on Smart Card System Using ISO 15408 Case Study: Indonesia Health Insurance Agency," International Conference on Information and Communication Technology (ICoICT), 2018.

[10] "Common Criteria for Information Technology Security Evaluation," November 2022.