ISO/IEC JTC 1/SC 27/WG 3 **N 2400**

ISO/IEC JTC 1/SC 27/WG 3 "Security evaluation, testing and specification"
Convenorship: **UNE**
Convenor: **Bañón Miguel Mr**

ISO/IEC JTC 1/SC 27/WG 3 Recommendations, Virtual (via Zoom) October 3rd – 6th, 2022

Document type	Related content	Document date	Expected action
Meeting / Other	Meeting: VIRTUAL 3 Oct 2022	2022-10-18	**INFO**

ISO/IEC JTC 1/SC 27/WG 3 Recommendations

78th Meeting, Virtual (via Zoom)

October 3rd – 6th, 2022

All recommendations are approved UNANIMOUSLY unless otherwise noted.

WG Recommendation 1.   Acceptance of minutes

ISO/IEC JTC 1/SC 27/WG 3 resolves to accept the minutes of ISO/IEC JTC 1/SC 27/WG 3 of the 72nd virtual meeting, April 4th – 8th 2022, in document WG 3 N2338.

WG Recommendation 2.   Appointment of the Drafting Committee

ISO/IEC JTC 1/SC 27/WG 3 resolves to appoint Kwangwoo Lee, Hongsong SHI and Junning Yao as Drafting Committee of the meeting and instructs them to prepare the draft WG recommendations document for WG 3.

WG Recommendation 3.   PWI registration

ISO/IEC JTC 1/SC 27/WG 3 resolves to request SC 27 to register the following PWI:

Title (and N-Nr, if any)	Project Editors: Name (Country)	WG	Project Number
Investigation of the feasibility and implementation of changes to ISO/IEC 15408 and ISO/IEC 18045	Tony Boswell (GB) * Yao Junning (CN) * Carolina Lavateli (FR) * Kwangwoo Lee (KR) * David Martin (GB) Susanne Pingel (DE) * Jade Stewart (US) * Heebong Choi (KR) * Hin Chan (AU) *	3	

*Co-Editor

WG Recommendation 4.   Cancellation of Project

ISO/IEC JTC 1/SC 27/WG 3 resolves to request SC 27 to cancel the following project listed below.

Title (and N-Nr, if any)	Justification
PWI 7677 Roadmap for the maintenance of ISO/IEC 15408 and ISO/IEC 18045	Document to become an internal WG3 working document while the work that it describes will be progressed instead via PWI.

WG Recommendation 5.   Call for contributions

ISO/IEC JTC 1/SC 27/WG 3 resolve to circulate a call for expert participation and contributions for the following projects. Submissions should reach the WG 3 Secretariat by the due date identified below.

Document	Project	Title	To be sent to/by
WG 3 N2364	PWI 5896	Cybersecurity assurance of systems and system of systems (SoS) *	WG 3 Secr/ 2023-03-03
WG 3 N2374	PWI TS 20540	Information technology — Security techniques — Testing cryptographic modules in their operational environment	WG 3 Secr/ 2023-03-03

* Subject to approval of title change

WG Recommendation 6.   Call for editors

ISO/IEC JTC 1/SC 27/WG 3 resolve to circulate a call for editors for the following projects. Submissions should reach the WG 3 Secretariat by the due date identified below.

Project	Title	To be sent to/by
19896-1	IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements	WG 3 Secr/ 2023-03-03
19896-3	IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators	WG 3 Secr/ 2023-03-03

WG Recommendation 7.   Approval of Project Editors/Co-Editors

ISO/IEC JTC 1/SC 27/WG 3 resolves to request SC 27 to approve the appointment of the experts listed below as Editors/Co-Editors.

Project	Name (Country)
ISO/IEC 19790	Carolyn FRENCH (CA) Heebong CHOI (KR) * Jean-Pierre QUÉMARD (FR)* Graham Costa (GB) * Randall Easter (US) *
ISO/IEC 24759	Heebong CHOI (KR) Carolyn FRENCH (CA)* Jean-Pierre QUÉMARD (FR)* Graham Costa (GB) * Randall Easter (US) *

* Co-editor

WG Recommendation 8.   Preparation of Documents

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the Project Editors/Co-Editors to prepare a 1st WD for the projects listed below.

Document	Project No.	Title	To be sent to/by
WG 3 N2192	19792	Information technology — Security techniques — Security evaluation of biometrics	WG 3 Secr. 2023-01-13
WG 3 N2294	19896-1	IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements	WG 3 Secr. 2023-01-13
WG 3 N2295	19896-2	IT security techniques — Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers	WG 3 Secr. 2023-01-13
WG 3 N2296	19896-3	IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators	WG 3 Secr. 2023-01-13

WG Recommendation 9.   Updating of documents

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the Project Editors/Co-Editors of the projects identified below to update the following drafts and send them to the SC 27 or WG 3 Secretariat by the due dates.

Document	Project No.	Title	To be sent to/by	DoC Doc. No.
WG 3 N2383	9569	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045 *	SC 27 Secr. 2023-01-13	WG 3 N2373
WG 3 N2384	17825	Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	SC 27 Secr. 2022-11-18	WG 3 N2375
WG 3 N2385	19790	Information technology — Security techniques — Security requirements for cryptographic modules	SC 27 Secr. 2022-12-13	WG 3 N2376

WG 3 N2387	23837-1	Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements *	SC 27 Secr. 2023-01-13	WG 3 N2388
WG 3 N2389	23837-2	Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods *	SC 27 Secr. 2023-01-13	WG 3 N2395
WG 3 N2397	24462	Information Security — Security Techniques — Ontology Building Blocks Covering Assessment of Security, Privacy, Governance and Risks *	SC 27 Secr. 2023-01-13	WG 3 N2396
WG 3 N2386	24759	Information technology — Security techniques — Test requirements for cryptographic modules	SC 27 Secr. 2023-01-13	WG 3 N2377
WG 3 N2391	29128-1	Information security, cybersecurity and privacy protection — Verification of cryptographic protocols — Part 1: Framework	SC 27 Secr. 2023-01-13	WG 3 N2354
WG 3 N2382	--	WG 3 Roadmap	WG 3 Secr. 2023-01-13	WG 3 N2381

* Subject to approval of title change

WG Recommendation 10.   Documents for Study and Comment

ISO/IEC JTC 1/SC 27/WG 3 resolves to circulate the following documents to experts for study and comment.

Document	Project	Title	Comments Due date
WG 3 N2192	19792	Information technology — Security techniques — Security evaluation of biometrics	2023-03-03
WG 3 N2294	19896-1	IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements	2023-03-03
WG 3 N2295	19896-2	IT security techniques — Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers	2023-03-03
WG 3 N2296	19896-3	IT security techniques — Competence	2023-03-03

		requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators	
WG 3 N2397	24462	Information Security — Security Techniques — Ontology Building Blocks Covering Assessment of Security, Privacy, Governance and Risks *	2023-03-03
WG 3 N2382	--	WG 3 Roadmap	2023-03-03

 * Subject to approval of title change

WG Recommendation 11.   New Work Items

ISO/IEC JTC 1/SC 27/WG 3 resolves to invite the SC 27 Secretariat to submit the following NP with the ballot period indicated.

Title (and N-Nr, if any)
Information security, cybersecurity and privacy protection — Verification of Cryptographic Protocols — Part 2: Evaluation Methods and Activities for Cryptographic Protocols (WG 3 N2393) *
Information security, cybersecurity and privacy protection — Verification of cryptographic protocols — Part 3: Evaluation Methods and Activities for Protocol Implementation Verification (WG 3 N2394) *

* Following experts have expressed their interest to actively participate in the development of 29128-2 and 29128-3 should these projects be approved through an NP ballots: Carolyn French (CA), Sylvain Guilley (FR), Naruki Kai (JP), Heebong Choi (KR) and Yi Mao (US)

WG Recommendation 12.   Document for DTR

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the SC 27 Secretariat to register the following document as DTR to circulate for balloting.

Document	Project	Title
WG 3 N2297	5891	Information security, cybersecurity and privacy protection — Hardware monitoring technology for hardware security assessment

WG Recommendation 13.   Document for DTS

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the SC 27 Secretariat to register the following document as DTS to circulate for balloting.

Document	Project	Title
WG 3 N2383	9569	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045 *

* subject to approval of title change

WG Recommendation 14.   Document for CD

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the SC 27 Secretariat to register the following documents as CD to circulate for balloting.

Document	Project	Title
WG 3 N2385	19790	Information technology — Security techniques — Security requirements for cryptographic modules
WG 3 N2386	24759	Information technology — Security techniques — Test requirements for cryptographic modules

WG Recommendation 15.   Document for DIS

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the SC 27 Secretariat to register the following document as DIS to circulate for balloting.

Document	Project	Title
WG 3 N2384	17825	Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

WG Recommendation 16.   Document for Publication

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the SC 27 Secretariat to publish the following documents.

Document	Project	Title
WG 3 N2387	23837-1	Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements *
WG 3 N2389	23837-2	Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods *
WG 3 N2391	29128-1	Information security, cybersecurity and privacy protection — Verification of cryptographic protocols — Part 1: Framework

* subject to approval of title change

WG Recommendation 17.   Title Changes

ISO/IEC JTC 1/SC 27/WG 3 resolves to change the title of following projects.

Project	Current Title	New Title	Justification
ISO/IEC PWI 5896	Cybersecurity assurance of systems and system of systems (SoS) based on ISO/IEC 15408	Cybersecurity assurance of systems and system of systems (SoS)	PWI is currently being structured with strong alignment to several relevant standards (i.e.,

			security, architecture, governance), not only for ISO/IEC 15408
ISO/IEC TS 9569	Information security, cybersecurity and privacy protection — Towards Creating an Extension for Patch Management for ISO/IEC 15408 and ISO/IEC 18045	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045	The title should be changed to reflect the scope of the document appropriately, as requested by ISO/CS
ISO/IEC 23837-1	Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements	Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements	Change the title to reflect the technical scope of the document appropriately
ISO/IEC 23837-2	Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods	Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods	Change the title to reflect the technical scope of the document appropriately
ISO/IEC TS 24462	Ontology for ICT Trustworthiness Assessment	Information Security — Security Techniques — Ontology Building Blocks Covering Assessment of Security, Privacy, Governance and Risks	Change the title to match the approved scope and content of the TS.

WG Recommendation 18.   Scope Change of ISO/IEC TS 9569

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the SC 27 Secretariat to change the scope of ISO/IEC TS 9569 from:

"ISO/IEC 15408 allows the evaluation of the assurance of IT products. However, while the standard can be used to perform an initial evaluation of an IT product, it does not support a differential security evaluation of that product subsequent to one or several patches being applied to it. Neither ISO/IEC 15408 nor ISO/IEC 18045 contain dedicated methods or evaluation activities which would support the evaluation of changes or updates.
Some of these aspects were addressed by users of the standards, in particular evaluation authorities, but also within the mutual recognition agreements (e.g. CCRA). In a lot of real-world use-cases developers provide updated or patched TOEs but the effort to re-certify these versions is mostly avoided.
The concept is to target the initial TOE evaluation and provide guidance to facilitate the re-evaluation of the TOE thereafter.
Note that the security assurance requirements proposed in Chapter 5 of this document do not include evaluation or test activities on the final TOE, but on the initial TOE and on the life cycle processes used by manufacturers.
The application of this document is not mandatory and there is nothing in the ISO/IEC 15408

standard that mandates updatability in the TSF in every product.

Finally, this document contains in Chapter 7 options for evaluation authorities (or mutual recognition agreements) how to utilize the additional assurance and additional evidence in their processes to support developer to consistently re-certify their updated or patched TOEs to the benefit of the users of these TOEs. The implementation of these options in an evaluation scheme is out of the scope of this document."

to

"This document specifies an extension for the ISO/IEC 15408 series and ISO/IEC 18045 to specify patch management requirements.

The document focuses on the initial TOE. The security assurance requirements specified in this document do not include evaluation or test activities on the final TOE, but on the initial TOE and on the life cycle processes used by manufacturers. Additionally, this document gives guidance to facilitate the evaluation of the TOE including the patch and development processes which support the patch management.

This document lists options for evaluation authorities (or mutual recognition agreements) on how to utilize the additional assurance and additional evidence in their processes to enable the developer to consistently re-certify their updated or patched TOEs to the benefit of the users of these TOEs. The implementation of these options by an evaluation scheme is out of the scope of this document."

Justification: Scope should be changed to give a clear and concise purpose of the document, as requested by ISO/CS.

WG Recommendation 19.   Extension of Project Duration

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the SC 27 Secretariat to extend the total project duration for the following projects by 9 months.

Project	Current Limit Dates	Proposed Limit Dates	Justification
ISO/IEC 17825	DIS: 2023-01-17 IS: 2024-01-17	DIS: 2023-10-17 IS: 2024-10-17	It took time to deal with the complex questions like the assurance, test methods and countermeasures. With these questions solved, the speed of development will accelerate.
ISO/IEC 19790	DIS: 2023-01-17 IS: 2024-01-17	DIS: 2023-10-17 IS: 2024-10-17	With much relevant input from industry, it took time to improve the text at the WD stage, but the speed of development will accelerate at the CD stage.
ISO/IEC 24759	DIS: 2023-01-17 IS: 2024-01-17	DIS: 2023-10-17 IS: 2024-10-17	With much relevant input from industry, it took time to improve the text at the WD stage, but the speed of development will accelerate at the CD stage.
ISO/IEC TS 24462	IS: 2022-12-13	IS: 2023-9-13	This project was moved, mid-execution, to WG13 due to a mis-classification of the topic of the project. It took substantial time to realize the lack of fit in WG13 and

			to move the project to the more appropriate SC27/WG3, but the speed of development will accelerate at the DTS stage.

WG Recommendation 20. Liaison Statements

ISO/IEC JTC 1/SC 27/WG 3 resolves to approve the following liaison statements and requests the WG 3 Secretariat to send these liaison statements to the committees/institutions concerned.

Document	To	Topic	Reference
WG 3 N2378	CCDB	All projects	WG3N2327
WG 3 N2379	CCUF	All projects	WG3N2368
WG 3 N2380	CMUF	19790, 24759	WG3N2361
WG 3 N2390	SC 37	19792	N22562
WG 3 N2392	SC 28	15408, 18045	WG3N2288

Resolution A   Thanks to the SC 27 Committee Manager

ISO/IEC JTC 1/SC 27/WG 3 thanks Sobhi Mahmoud, Christine Fries and Alexander Zimmermann for their efficient support before and during the meeting.

Acclamation

Resolution B   Thanks to the Drafting Committee

ISO/IEC JTC 1/SC 27/WG 3 thanks the members of the drafting committee Kwangwoo Lee, Hongsong SHI and Junning Yao for drafting the recommendations.

Acclamation

Resolution C   Thanks to WG 3 Secretariat and Convenor support

The WG 3 Convener and experts thank its secretary and Convenor Support, Naruki Kai, for his efforts and assistance in developing the WG 3 Meeting Report before, during and after the meeting.

Acclamation

Resolution D   Thanks to the Experts, Rapporteurs and Editors

ISO/IEC JTC 1/SC 27 WG 3 thanks all the SC 27 WG 3 experts, rapporteurs, editors, acting editors and acting rapporteurs for their efforts and continued support in progressing the many SC 27 WG 3 projects.

ISO/IEC JTC 1/SC 27 WG 3 especially thanks the following editors for their efforts in getting the following documents through the standardisation process.

Editor	Project	Title
Dembling Josh Elazari Bar On Amit Ito Tomotaka Shick Deana Vishik Claire	5895	Cybersecurity — Multi-party coordinated vulnerability disclosure and handling
Andrukiewicz Elzbieta Lavatelli Carolina Stewart Fiona Têtu Guillaume	15408-1	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model
Muthambi Nicholas SHI Hongsong Stewart Fiona	15408-2	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components
LEE SOOHYEUN Noetzel Christian	15408-3	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components
Boswell Tony	15408-4	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities
Choi Heebong Stewart Fiona	15408-5	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

		Part 5: Pre-defined packages of security requirements
Lee Kwangwoo Martin David	18045	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation
Guilley Sylvain Hamaguchi Soshi Kang You Sung	20897-2	Information security, cybersecurity and privacy protection — Physically unclonable functions — Part 2: Test and evaluation methods
Stewart Fiona Têtu Guillaume	22216	Information security, cybersecurity and privacy protection — New concepts and changes in ISO/IEC 15408:2022 and ISO/IEC 18045:2022

Acclamation

Resolution E Thanks to the Convenor

ISO/IEC JTC 1/SC 27 WG 3 thanks Miguel Bañón for his excellent work as WG 3 Convener.

Acclamation