REPLACES:N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: liaison statement

TITLE: **Liaison statement from ISO/IEC JTC 1/SC 27/WG 4 to ETSI TC MTS**

SOURCE: JTC 1/SC 27 Secretariat

DATE: **2017-03-28**

PROJECT: **1.27.63.01/07 (ISO/IEC 27034-1/7)**

STATUS: **In accordance with Resolution 10 (as contained in N16841) of the 23rd SC 27/WG 4 meeting held in Abu Dhabi, United Arab Emirates, 23rd – 27th October 2017, this document has been sent to ETSI TC MTS. It is being circulated within SC 27 for information.**

ACTION ID: **Info**

DUE DATE:

DISTRIBUTION: P-, O-, L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-Chair
E. J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors

MEDIUM: http://isotc.iso.org/livelink/livelink/open/jtc1sc27

NO. OF PAGES: 1 + 11

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Am DIN-Platz, Burggrafenstr. 6, D-10787 [D-10772 postal] Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-4-2652; E-mail: krystyna.passia@din.de;
HTTP://www.din.de/go/jtc1sc27

1. Introduction

ISO/IEC JTC 1/SC 27 thanks ETSI TC MTS for its continued interest in the work of SC 27.

2. Topic WG4 "Application Security" - ISO/IEC 27034

SC 27 would like to inform ETSI TC MTS about

Progress report on ISO/IEC 27034 – Application Security Project during the last SC27 meeting

General

An Information Technology (IT) application includes software, processes and technology, together supporting business needs. Application Security addresses the protection of information involved by the utilization on an application.

The framework proposed by the ISO/IEC 27034 addresses the security of IT application as mitigating all risks that can affect information integrity, confidentiality and availability involved by the application. These risks can come from peoples, processes and technology, and can be evaluated from three perspectives: business context, regulatory context and technological context. This project presents an overview, processes and components of the application security framework to help an organization to determine a measurable and verifiable Level of Trust necessary for using an application in a specific environment.

Progress table projects overview

Agreement of stade progression for all actives 27034 project parts.

Part	Actual stade	Next stade	To be release on
27034-1 : Concepts and overview	IS	-	Published: 2011-10
27034-2 : ONF Management	IS	-	Published: 2015-09
27034-3 : AS Management Process	CD3	DIS	Expected in 2017
27034-4 : AS Validation	NWI 2	NWI 3	Expected in 2019
27034-5 : Protocols and ASC data structure	DIS	FDIS	Expected in 2017
27034-5-1 : Protocols and ASC data structure – XML schemas	PDTS3	PDTS4	Expected in 2017
27034-6 : Case Studies	IS	-	Published: 2016-09
27034-7 : AS assurance prediction framework	DIS	DIS2	2017

Progress made during this International meeting

ISO/IEC 27034-3: Application Security Management Process

Title:	Information technology – Security techniques – Application security – Part 3: Application Security Management Process
Co-editors:	Luc Poulin, CA; Shaun Gilmore, US; David Paladini Fr, and Katie Moussouris, US.
Current stage:	CD3
Next stage:	DIS

General

Part 3 presents an in-depth discussion of the processes involved in an application project: determining the application requirements and environment, assessing the application security risks, creating and maintaining the Application Normative Framework, realizing and operating the application and validating its security throughout its life cycle.

This part explains the relationships among these processes, their activities and interdependencies, and how they introduce security into an application project. It presents how an organization should implement the standard on an application project-level and integrate it into its existing processes.

The purpose of Part 3 is to assist organizations to create, maintain and validate secure applications in a uniform way across an organisation. It was developed to help application team to implement and reuse organization's approved application security elements into their application project.

Attendees

- National Bodies: CA, DE, CH, CN, JP, LU, TU, US
- Liaisons: ISACA.

Overview of Comments and contributions received

NB/Liaison	General	Editorial	Technical	Totals	Percentage
CA Canada	0	33	27	**60**	76,9%
CN China	0	0	15	**15**	19,2%
JP Japan	1	0	2	**3**	3,8%
Totals	**1**	**33**	**44**	**78**	**100,0%**
Percentage	1,3%	42,3%	56,4%	**100,0%**	

Disposition Type	Count	Percertage
Accepted	63	80,8%
Accepted in principle	7	9,0%
Not accepted	6	7,7%
Withdrawn	0	0,0%
Overtaken by events	1	1,3%
Deferred	0	0,0%
Noted	1	1,3%
Total	**78**	**100,0%**

Focus of comments and discussions

- Discussion and comments as work in progress to produce a FDIS version of this international standard.
- Comments provided were mainly editorials, addressing text clarity improvement and simplification to improve document coherence and text readability was disposed.
- Some minor technical comments to improve clarity and directives alignment was also proposed and accepted.
- Alignment to 27005 was under the scope of some comments and contributions received from experts. For consistency, all referenced to 31000 will be removed form the text.
- No main discussion occurs during this disposition of comments session and experts agree to move the document to FDIS.

Recommendations resulting from the meeting

- Recommendation to move 27034-3 at FDIS stage.

ISO/IEC 27034-4: Application security validation

Title:	Information technology – Security techniques – Application security – Part 4: Application security validation
Co-editors:	Luc Poulin, CA; and René St-Germain, LU.
Current stage:	SP2
Next stage:	SP3

General

Part 4 presents an in-depth discussion of the application security validation, audit and certification process for organizations, applications and peoples.

It presents what and how the implementation of this IS should be verified and audited on a three (3) levels, as:

1) Organization level – where it will frame and guide auditors to validate the organization's AS objectives and audit/verify how an organization comply with its AS objectives and criteria.
2) Application level – where it will frame and guide auditors to measures the application's Actual Level of Trust and compares it with the application's Targeted Level of Trust

previously selected by the organization, to certify this application as secure as expected.

3) Peoples level – where it will frame and guide the development and the implementation of an ISO/IEC 27034 AS professional certification.

The purpose of Part 4 is to assist organizations to declare conformance to the 27034 by providing guidance and elements verify and audit organization, application and persons on the application security framework. It was developed to help an authority to define an application security verification scope, help organization to implement it, and help auditors to verify the compliance of organizations and applications to a AS verification scope.

Attendees

- National Bodies: CA, DE, CH, CN, JP, LU, TU, US.
- Liaisons: ISACA.

Overview of Comments and contributions received

NB/Liaison	General	Editorial	Technical	Totals	Percentage
IS ISACA	1	114	0	**115**	100,0%
	0	0	0	**0**	0,0%
Totals	**1**	**114**	**0**	**115**	**100,0%**
Percentage	0,9%	99,1%	0,0%	**100,0%**	

Disposition Type	Count	Percertage
Accepted	114	99,1%
Accepted in principle	1	0,9%
Not accepted	0	0,0%
Withdrawn	0	0,0%
Overtaken by events	0	0,0%
Deferred	0	0,0%
Noted	0	0,0%
Total	**115**	**100,0%**

Focus of comments and discussions

- Contribution received form Canada for this NWI was presented and accepted by the experts for discussion, and will be use as the main draft for the document.
- Comments received form ISACA was disposed and mainly accepted.
- The document, structure, concepts and elements that was presented in previous meeting was agreed by experts as the scope and elements that will apply to this project.
- Experts also agree to keep this project on Study Period one last stage to let everyone time to contribute.

Recommendations resulting from the meeting

- Recommendation to keep this project on SP stage for another cycle, and move directly to CD stage in 6 month if the document is mature enough.

ISO/IEC 27034-5: Protocols and application security control data structure

Title:	Information technology – Security techniques – Application security – Part 5: Protocols and application security control data structure
Co-editors:	Luc Poulin, CA; and Daniel Sinnig, CA.
Current stage:	CD4
Next stage:	DIS

General

Part 5 presents the minimal set of essential attributes of ASCs and further details the Application Security Life Cycle Reference Model in order to facilitate the implementation of the 27034 AS framework and the communication and exchange of ASCs.

The purpose of Part 5 is to document and explain the minimal set of essential attributes of ASCs and related ONF elements. It allows organizations to form, validate and communicate standardized basic, specialized or customized ASCs, which may be used inside and outside the scope of ISO/IEC 27034.

Attendees

- National Bodies: CA, DE, CH, CN, JP, LU, TU, US.
- Liaisons: ISACA, $(ISC)^2$.

Overview of Comments and contributions received

NB/Liaison	General	Editorial	Technical	Totals	Percentage
AR Argentina	0	9	2	**11**	28,2%
CA Canada	0	2	8	**10**	25,6%
JP Japan	3	14	1	**18**	46,2%
Totals	**3**	**25**	**11**	**39**	**100,0%**
Percentage	7,7%	64,1%	28,2%	**100,0%**	

Disposition Type	Count	Percertage
Accepted	32	82,1%
Accepted in principle	6	15,4%
Not accepted	0	0,0%
Withdrawn	0	0,0%
Overtaken by events	0	0,0%
Deferred	0	0,0%
Noted	1	2,6%
Total	**39**	**100,0%**

Focus of comments and discussions

- Content contribution from CA and ISACA were review during the Part 5 working session.

- Comments mainly addressing syntax correction and alignment with part 3, part 5-1 and the ISO directives.

Recommendations resulting from the meeting

- Editors mainly received editorials comments to improve the documents, no other comments was received form the other countries' experts.
- Experts agreed to continue to keep this part 5 aligned with part 5-1.
- Because everyone were happy with the document, it was decided to move this document at FDIS stage for approbation.

ISO/IEC 27034-5-1: Protocols and application security control data structure: XML Schemas

Title:	Information technology – Security techniques – Application security – Part 5-1: Protocols and application security control data structure: XML Schemas
Co-editors:	Luc Poulin, CA; and Daniel Sinnig, CA.
Current stage:	PDTS2
Next stage:	PDTS3

General

Part 5-1 presents and explains a XML Schemas example, describing the Application Security Control (ASC) and the Application Security Life Cycle Reference Model (ASLCRM) components.

The purpose of Part 5-1 is to define XML schemas that implement the essential information and data structure requirements for ASCs as well as the Application Security Lifecycle Reference Model (ASLCRM). It was developed to provide an implementation example of part 5.

Attendees

- National Bodies: CA, DE, CH, CN, JP, LU, TU, US.
- Liaisons: ISACA, $(ISC)^2$.

Overview of Comments and contributions received

NB/Liaison	General	Editorial	Technical	Totals	Percentage
JP Japan	2	21	0	**23**	100,0%
	0	0	0	**0**	0,0%
Totals	**2**	**21**	**0**	**23**	**100,0%**
Percentage	8,7%	91,3%	0,0%	**100,0%**	

Disposition Type	Count	Percertage
Accepted	21	91,3%
Accepted in principle	1	4,3%
Not accepted	0	0,0%
Withdrawn	0	0,0%
Overtaken by events	0	0,0%
Deferred	0	0,0%
Noted	1	4,3%
Total	**23**	**100,0%**

Focus of comments and discussions

- The updated XML Schemas file v1.0RC (Release Candidate), was received from CA as contribution.
- Comments mainly addressing syntax correction and alignment with the ISO directives.

- No significant issues were raised by the group and experts agreed to continue to improve the content of the XML schema for the next meeting.
- Only two comments was concerning improving two lists of activities improvement, and they were accepted.
- Expert recommend to publish this document right after part 5 will be published.

Recommendations resulting from the meeting

- Recommendation to move 27034-5-1 at PDTS3 stage but still accepting Ge, Te and Ed comments.

ISO/IEC 27034-7: AS Assurance prediction framework

Title:	Information technology – Security techniques – Application security – Part 7: Application security assurance prediction framework
Editor:	David Grawrock, US.
Current stage:	DIS
Next stage:	DIS2

General

Part 7 presents a prediction framework that codifies the requirements and processes for making predictive security claim statements to replace ASCs reimplementation and retesting in an application project.

The purpose of part 7 is to provide the criteria and guidance for the extension of security attributes in one application to a different but related application. Additionally organization will have to state the conditions under which it is valid and invalid to use Prediction Application Security Rational (PASR) to 'replace' the implementation/verification of an Application Security Control (ASC). This part was developed to help organization to diminish the security cost of an application project under reasonably security expectations.

Attendee

- National Bodies: CA, DE, CH, CN, JP, LU, TU, US.
- Liaisons: ISACA.

Overview of Comments and contributions received

NB/Liaison	General	Editorial	Technical	Totals	Percentage
CA Canada	0	13	29	**42**	71,2%
JP Japan	0	17	0	**17**	28,8%
Totals	**0**	**30**	**29**	**59**	**100,0%**
Percentage	0,0%	50,8%	49,2%	**100,0%**	

Disposition Type	Count	Percertage
Accepted	31	52,5%
Accepted in principle	20	33,9%
Not accepted	3	5,1%
Withdrawn	0	0,0%
Overtaken by events	4	6,8%
Deferred	1	1,7%
Noted	0	0,0%
Total	**59**	**100,0%**

Focus of comments and discussions

- Long discussion how Levels of trust definition and each them should be used in this application security framework to be as clear and comprehensible to the industries and organizations as possible. One concern was how should be used the "Target Level of Trust" in relation with the "Actual Level of Trust" and the "Expected Level of Trust".
- Many comments were very controversial and the team required 3.5h supplemental working session to be able to finish to disposed all comments.
- A document title name change was approved form "Application security assurance prediction model" with "Application security assurance prediction framework"

  The rational supporting this request is:
  - The 27034 part 7 document does not present a prediction model but a prediction framework. Like all others documents provided by the 27034 series (e.g. 27034-1, 27034-2, 27034-4 and 27034), the 27034 part 7 presents processes, actors and other elements guiding how to implement Predicted Application Security Rational (PASR) to replace Application Security Control (ASC). That's why this document should not be introduced as a Model, but as a Framework.
  - Also, this change will improve cohesion inside the 27034 series as:
    - Part 2 presents the Organization Normative Framework,
    - Part 3 presents the Application Normative Framework,
    - Part 4 presents the Verification Scope Framework, and
    - Part 7 presents the Prediction Framework.
  - This final minor but important title change for the 27034 series documents alignment will be the last one before the publication of the document.
- Many technical contributions was proposed and accepted and NBs require a round to be able to revise the document before allowing it to go to FDIS.
- Intermediary meeting mid November 2016 at Quebec city, and on WebEx
- Editors what to tank all NBs for their great participation, work and patience to address all controversial comments presented and disposed during this meeting.

Recommendations resulting from the meeting

- Recommendation to move 27034-7 at a 2nd DIS stage, for another round.

SP Application Security Validation

Recommendations resulting from the meeting

SO/IEC JTC 1/SC 27/WG 4 agrees to continue the following study periods for the periods as indicated, 6 months.
WG 4 requests its Management Team to distribute a **Call for Contributions** (CfC) to experts and liaisons via the applicable channels.
Rapporteurs : Luc Poulin (CA), René St Germain (LU)

SC 27 looks forward to your consideration of this matter.

3. Future Meetings

The future meetings schedule for SC 27 Working Groups is:

a) Hamilton, NZ – April 2017

All SC 27 Working Groups simultaneously meet at the same location.

4. Future Contributions

SC 27 very much appreciates the valuable input of ETSI TC MTS to the work of SC 27 and welcomes feedback to this Liaison Statement be sent to the SC 27 Secretariat by 20th March 2017 before the next SC 27 meetings, scheduled for April 2017 in Hamilton, NZ.

5. Attachments

Please find enclosed relevant attachments related to the projects included in the liaison statement.