



ISO/IEC JTC 1 N 9549
ISO/IEC JTC 1
Information Technology

2009-03-18

Document Type: Other (Defined)

Document Title: SC 27 Proposed Modifications to JTC 1/SC 27 Programme of Work

Document Source: SC 27 Secretariat

Reference:

Document Status: This document is forwarded to JTC 1 National Bodies for a 45 day default letter ballot. If the JTC 1 Secretariat receives no objections to the SC 27 Proposed changes to Programme of Work, it will be forwarded to ITTF for processing.

Action ID: ACT

Due Date: 2009-05-02

No. of Pages: 19

Lisa Rajchel
Secretariat ISO/IEC JTC 1
ANSI
New York, NY 10036
USA

ISO/IEC JTC 1/SC 27
Information technology -- Security techniques

Date: 2009-03-17

Proposed Modifications to JTC 1/SC 27 Programme of Work

Dear Lisa,

At the recent Working Group meetings of SC 27 held in Limassol (Cyprus), October 2008, the following modifications to SC 27 Programme of Work are proposed:

Proposed modifications to SC 27 Programme of Work:

SUBDIVISION by additional Part 5 of ISO/IEC 11770 (WG 2 resolution 10 in SC 27 N7303)

<u>Project</u>	<u>ISO/IEC number</u>	<u>Title</u>
1.27.18.05	11770-5	Key management — Part 5: Group key management

SUBDIVISION and renumbering of ISO/IEC 27033 Parts 5 - 7 (WG 4 resolution 1 in SC 27 N6904)

<u>Project</u>	<u>ISO/IEC number</u>	<u>Title</u>
1.27.58.05	27033-5	Network security — Part 5: Securing virtual private networks – Risks, design techniques and control issues (RENUMBERED from 27033-6 to 27033-6) (REVISION of ISO/IEC 18028-5:2006)
1.27.58.06	NP 27033-6	Network security — Part 6: IP convergence
1.27.58.07	NP 27033-7	Network security — Part 7: Wireless

CHANGE OF TITLE (WG 1 resolution 13 in SC 27 N7295)

<u>Project</u>	<u>ISO/IEC number</u>	<u>Title</u>
1.27.68	27010	<u>from</u> "Information security management: sector-to-sector interworking and communications for industry and government" <u>to</u> "Information security management guidelines for inter-sector communications"

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

Postal address
DIN
Deutsches Institut f. Normung e. V.
10772 Berlin
Germany

Office address
DIN
Deutsches Institut f. Normung e. V.
Burggrafenstraße 6, 10787 Berlin
Germany

ORGANISATION INTERNATIONALE DE NORMALISATION

Telephone
+49 30 2601-2652

Telefax
+49 30 2601-1723

E-mail
krystyna.passia@din.de

HTTP://www.jtc1sc27.din.de/en



CHANGE OF TITLE (WG 5 resolutions 10 and 11 in SC 27 N7097rev1)

Project	ISO/IEC number	Title
1.27.54	29100	<u>from</u> "A privacy framEwork" <u>to</u> "Privacy framework"

Project	ISO/IEC number	Title
1.27.55	29101	<u>from</u> "A privacy reference architecture" <u>to</u> "Privacy reference architecture"

CHANGE OF ISO/IEC REFERENCE NUMBER (WG 1 resolution 12 in SC 27 N7295)

Project	ISO/IEC number	Title
1.27.70	<u>from</u> "29165" <u>to</u> "27008"	Guidance for auditors on ISMS controls

AMENDMENT BY SUBDIVISION (WG 2 resolution 13 in SC 27 N7303)

Project	ISO/IEC number	Title
1.27.33.01.01	18033-1/Amd.1	Encryption algorithms – Part 1: General – AMENDMENT 1

The SC 27 Programme of Work (SD4) contained in document SC 27 N7444 to reflect on these modifications is enclosed with this letter.

We would greatly appreciate your circulating the above-mentioned proposal to the National Bodies of JTC 1 for their endorsement at your earliest convenience.

We thank you for your cooperation.

Best regards,

Krystyna Passia
JTC 1/SC 27 Secretariat

Encls: SC 27 N7444

cc: Dr. Walter Fumy, SC 27 Chairman
Dr. Marijke De Soete, SC 27 Vice-Chair

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

Postal address
DIN
Deutsches Institut f. Normung e. V.
10772 Berlin
Germany

Office address
DIN
Deutsches Institut f. Normung e. V.
Burggrafenstraße 6, 10787 Berlin
Germany

ORGANISATION INTERNATIONALE DE NORMALISATION

Telephone
+49 30 2601-2652

Telefax
+49 30 2601-1723

E-mail
krystyna.passia@din.de

HTTP://www.jtc1sc27.din.de/en

1.27.02	IS	10116:2006-02-01 (3rd edition)	Modes of operation for an n -bit block cipher	2			1st pre- review in 2009				
1.27.02	Cor.1	10116:2006/Cor.1: 2008-03-15	Technical Corrigendum 1	2							
1.27.03.01	1st CD N7139	9798-1 (revision of the 2nd edition 1997-08-01)	Entity authentication - Part 1: General (revision started in April 2008 as recommended in N6664)	2	Riaal Domingues	Recomm. N6664	08-05	08-11	09-11	10-05	
1.27.03.02	IS	9798-2:2008-12-15 (3rd edition) (revision of 2nd edition- 1999-07-15 + Cor. 1:2004-02-01 + Draft Amd. 1)	Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms (revision started in April 2005 as recommended in N4569)	2		Recomm. N4569	1st pre- review in 2011				
1.27.03.02	Cor.1	9798-2:1999-07-15/ Cor.1:2004-02-01	Technical Corrigendum 1 (withdrawn)	2							
1.27.03.02	DCOR1 N7149rev1	9798-2:2008-12-15/ DCOR1	Draft Technical Corrigendum 1	2	Chris Mitchell						
1.27.03.02.01	1st WD N5148	9798-2/Amd.1	Amendement 1 (merged into 8798-2 (3rd edition))	2		Recomm. N5171					
1.27.03.03	IS	9798-3:1998-10-15 (2nd edition)	Entity authentication - Part 3: Mechanisms using digital signature techniques (3rd confirmation in 2008)	2		Recomm. N7129	4th pre- review in 2011				
1.27.03.03	DCOR1 N7150	9798-3:1998-10-15/ DCOR1	Draft Technical Corrigendum 1	2	Chris Mitchell						
1.27.03.03.01	PDAM N7134	9798-3/Amd.1	Amendment 1: Three-party entity authentication	2	Xiaolong Lai	Recomm. N6182	07-11	08-11	09-11	10-05	
1.27.03.04	IS	9798-4:1999-12-15 (2nd edition)	Entity authentication - Part 4: Mechanisms using a cryptographic check function (2nd confirmation in 2006)	2		Recomm. N5143	3rd pre- review in 2009				
1.27.03.04	DCOR1 N7151	9798-4:1999-12-15/ DCOR1	Draft Technical Corrigendum 1	2	Chris Mitchell						
1.27.03.05	FCD N7136	9798-5 (revision of 2nd ed. 2004- 12-01)	Entity authentication - Part 5: Mechanisms using zero knowledge techniques (revision started in May 2007 as recommended in N5823)	2	Jean-François Misarsky Michael Ward	Recomm. N5823	07-11	08-11	09-11	10-05	

1.27.03.06	1st WD N7307	9798-6 (revision of 1st edition 2005-08-01)	Entity authentication - Part 6: Mechanisms using manual data transfer <i>(revision started in October 2008 as recommended in N7130)</i>	2	Long Nguyen ³⁾	Recomm. N7130	08-11	09-11	10-11	11-05
1.27.03.06	DCOR1 N7152	9798-6:2005-08-01/ DCOR1	Draft Technical Corrigendum 1	2	Chris Mitchell					
1.27.04.01	FCD N6704	9797-1 (revision of 1st edition 1999-12-15)	Message authentication codes (MACs) - Part 1: Mechanisms using a block cipher <i>(revision started in May 2003 as recommended in N3562)</i>	2	Bart Preneel Chris Mitchell ²⁾	Recomm. N3562	03-11	06-11	09-05	09-11
1.27.04.02	FCD N7124	9797-2 (revision of 1st edition 2002-06-01)	Message authentication codes (MACs) - Part 2: Mechanisms using a dedicated hash-function <i>(revision started in May 2005 as recommended in N4551rev1)</i>	2	Bart Preneel Liqun Chen ²⁾	Recomm. N4551rev1	06-11	08-05	09-05	09-11
1.27.04.03	3rd WD N7126	9797-3	Message authentication codes (MACs) - Part 3: Mechanisms using a universal hash-function	2	Bart Preneel Michael Ward ²⁾	Recomm. N4551rev1	06-11	09-05	10-11	11-05
1.27.06.01	IS	13888-1 (revision of 2nd edition 2004-06-01)	Non-repudiation - Part 1: General <i>(awaiting publication)</i>	2		Recomm. N5834				
1.27.06.02	1st CD N7255	13888-2 (revision of 1st edition 1998-04-01)	Non-repudiation - Part 2: Mechanisms using symmetric techniques <i>(revision started in May 2006 as recommended in N5144)</i>	2	Nataša Živić	Recomm. N5144	06-05	08-11	10-05	10-11
1.27.06.03	FCD N7168	13888-3 (revision of 1st edition 1997-12- 01)	Non-repudiation - Part 3: Mechanisms using asymmetric techniques <i>(revision started in May 2006 as recommended in N5144)</i>	2	Hajime Watanabe	Recomm. N5144	06-05	08-05	09-11	10-05
1.27.07.02	1st WD N7145	9796-2 (revision of 2nd edition 2002-10-01 + Amd1:2008-01-15)	Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms <i>(revision started in April 2008 as recommended in N6659)</i>	2	Chris Mitchell ³⁾	Recomm. N6659	08-11	09-11	10-11	11-05
1.27.07.02.01	Amd.1	9796-2:2002/Amd.1: 2008-01-15	Amendment 1	2		Recomm. N4570				

1.27.07.03	IS	9796-3:2006-09-15 (2nd edition)	Digital signature schemes giving message recovery Part 3: Discrete logarithm based mechanisms	2			1st pre- review in 2009				
1.27.08.01	IS	14888-1:2008-04-15 (2nd edition)	Digital signatures with appendix - Part 1: General	2			1st pre- review in 2011				
1.27.08.02	IS	14888-2:2008-04-15 (2nd edition)	Digital signatures with appendix - Part 2: Integer factorization based mechanisms	2			1st pre- review in 2011				
1.27.08.03	IS	14888-3:2006-11-15 (2nd edition)	Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms	2			1st pre- review in 2009				
	Cor.1	14888-3:2006/ Cor.1:2007-09-01	Technical Corrigendum 1	2							
	Cor.2	14888-3:2006/ Cor.2:2009-02-15	Technical Corrigendum 2	2							
1.27.08.03.01	PDAM 1 N7157	14888-3:2006/Amd.1	Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms -- Amendment 1	2	Andrey Chmora²⁾ Anatoly Lunin²⁾	Recomm. N5897	07-11	08-11	09-11	10-05	
1.27.09.01	IS	10118-1:2000-06-15 (2nd edition)	Hash-functions -- Part 1: General <i>(2nd confirmation in 2006)</i>	2		Recomm. N5145	3rd pre- review in 2009				
1.27.09.02	2nd CD N7132	10118-2 (revision of 2nd edition 2000-12-15 + Cor2:2007-02-15)	Hash-functions -- Part 2: Hash-functions using an <i>n</i>-bit block cipher <i>(revision started in May 2006 as recommended in N5145)</i>	2	Hiroataka Yoshida Takeshi Chikazawa²⁾	Recomm. N5145	07-05	08-05	10-05	10-11	
1.27.09.02	Cor.2	10118-2:2000/ Cor.2:2007-02-15	Technical Corrigendum 2 <i>(ISO/IEC 10118-2/Cor.2:2007-02-15 cancels and replaces ISO/IEC 10118-2/Cor.1:2006-10-01)</i>	2							
1.27.09.03	IS	10118-3:2004-03-01 (3rd edition)	Hash-functions -- Part 3: Dedicated Hash-functions <i>(1st confirmation in 2007,</i>	2		Recomm. N5836	2nd pre- review in 2010				
1.27.09.03.01	Amd.1	10118-3:2004/ Amd.1:2006-02-15	Amendment 1	2							

1.27.09.04	IS	10118-4: 1998-12-15 (1st edition)	Hash-functions -- Part 4: Hash-functions using modular arithmetic (2nd confirmation in 2006)	2		Recomm. N5151	3rd pre- review in 2009				
1.27.13	ITU-T IS	X.841 15816:2002-02-01 (1st edition)	Security information objects for access control (2nd confirmation in 2008 as per Kyoto 20th Plenary resolution 12 (N6799))	4			3rd pre- review in 2011				
1.27.14.05	TR	13335-5: 2001-11-01 (1st edition)	Guidelines for the management of IT security - Part 5: Management guidance on network security (withdrawn since incorporated into ISO/IEC 18028- 1:2006-07-01)	1		Recomm. N3935					
1.27.16.01	FDIS N7261	15408-1 (revision of 2nd edition 2005-10-01)	Evaluation criteria for IT security -- Part 1: Introduction and general model	3	Fiona Pattinson		06-05	07-05	08-11	09-05	
1.27.16.02	IS	15408-2:2008-08-15 (3rd edition)	Evaluation criteria for IT security -- Part 2: Security functional components	3			1st pre- review in 2011				
1.27.16.03	IS	15408-3:2008-08-15 (3rd edition)	Evaluation criteria for IT security -- Part 3: Security assurance components	3			1st pre- review in 2011				
1.27.18.01	1st CD N7118	11770-1	Key management -- Part 1: Framework (revision started in April 2008 as recommended in N6713)	2	Toshio Tatsuta	Recomm. N6713	08-05	09-05	10-05	10-11	
1.27.18.02	IS	11770-2:2008-06-15 (2nd edition)	Key management -- Part 2: Mechanisms using symmetric techniques	2			1st pre- review in 2011				
1.27.18.02	DCOR1 N7153	11770-2:2008-06-15/ DCOR1	Draft Technical Corrigendum 1	2	Chris Mitchell						
1.27.18.03	IS	11770-3:2008-07-15 (2nd edition)	Key management -- Part 3: Mechanisms using asymmetric techniques	2		1st pre- review in 2011					
1.27.18.03	DCOR1 N7154	11770-3:2008-07-15/ DCOR1	Draft Technical Corrigendum 1	2	Chris Mitchell						
1.27.18.04	IS	11770-4:2006-05-01 (1st edition)	Key management -- Part 4: Mechanisms based on weak secrets	2			1st pre- review in 2009				

1.27.18.04	DCOR1 N7155	11770-4:2006-07-15/ DCOR1	Draft Technical Corrigendum 1	2	Chris Mitchell						
1.27.18.05 ¹	NP 1st WD N7156	11770-5	Key management -- Part 5: Group key management	2	Christoph Ruland ⁴⁾ Toshiaki Tanaka ^{2) 3)}	Recomm. N7120	08-11	09-11	11-05	11-11	
1.27.19		X.842 TR 14516: 2002-06-15 (1st edition)	Guidelines for the use and management of Trusted Third Party services <i>(2nd confirmation as per April 2008 20th Plenary resolution 12 (N6799))</i>	4		Recomm. N4577	3rd pre- review in 2011				
1.27.20	IS	15292: 2001-12-15 (1st edition)	Protection profile registration procedures <i>(2nd confirmation in 2007)</i>	3		Recomm. N6007	3rd pre- review in 2010				
1.27.21.01	1st WD N/A	TR 15443-1: (revision of 1st edition 2005-02-01)	A framework for IT security assurance -- Part 1: Overview and framework <i>(as per Summary of voting (N6487) early revision started in April 2008)</i>	3	Faud Khan	N6487	09-05	09-11	10-05	10-11	
1.27.21.02	1st WD N/A	TR 15443-2: (revision of 1st edition 2005-09-01)	A framework for IT security assurance -- Part 2: Assurance methods <i>(as per Summary of voting (N6487) early revision started in April 2008)</i>	3	Faud Khan	N6487	09-05	09-11	10-05	10-11	
1.27.21.03	1st WD N/A	TR 15443-3: revision of 1st edition 2007-12-15)	A framework for IT security assurance -- Part 3: Analysis of Assurance Models <i>(as per Summary of voting (N6487) early revision started in April 2008)</i>	3	Faud Khan	N6487	09-05	09-11	10-05	10-11	
1.27.22		TR 15446 (2nd edition)	Guide for production of Protection Profiles and Security Targets (PP/ST)	3		Recomm. N4597	1st pre- review in 2012				
1.27.23	IS	7064: 2003-02-15 (1st edition)	Check character systems <i>(1st confirmation in 2006 as recommended in N5146)</i>	2		Recomm. N5146	2nd pre- review in 2009				
1.27.24	ITU-T IS	X.843 15945:2002-02-01 (1st edition)	Specification of TTP services to support the application of digital signatures <i>(2nd confirmation in 2008 as per Kyoto 20th Plenary resolution 12 (N6799))</i>	4		Recomm. N4578	3rd pre- review in 2011				

1.27.26.01	IS	15946-1:2008-04-15 (2nd edition)	Cryptographic techniques based on elliptic curves -- Part 1: General	2		Recomm. N4553rev1	1st pre- review in 2011				
	DCOR1 N6693rev1	15946-1:2008/ DCOR1	Draft Technical Corrigendum 1	2	Atsuko Miyaji						
1.27.26.03	IS	15946-3:2002-12-01 (1st edition)	Cryptographic techniques based on elliptic curves - Part 3: Key establishment <i>(withdrawn on 2008-07-02 since incorporated into the 2nd edition of ISO/IEC 11770-3:2008-07-15.</i>	2		Recomm. N4553rev1					
1.27.26.05	FCD N7159	15946-5	Cryptographic techniques based on elliptic curves --	2	Atsuko Miyaji	Recomm. N5175	06-05	07-05	09-05	09-11	
1.27.27.01	IS	18014-1:2008-09-01 (2nd edition)	Part 5: Elliptic curve generation Time-stamping services -- Part 1: Framework	2		Recomm. N4554	1st pre- review in 2011				
1.27.27.02	FCD N7172	18014-2 (revision of 1st edition 2002-12-15)	Time-stamping services -- Part 2: Mechanisms producing independent tokens <i>(revision started in May 2005 as recommended in N4554)</i>	2	Jose Mañas	Recomm. N4554	05-05	06-11	09-05	09-11	
1.27.27.03	FCD N7174	18014-3 (revision of 1st edition 2004-02-15)	Time-stamping services -- Part 3: Mechanisms producing linked tokens <i>(revision started in May 2007 as recommended in N5805)</i>	2	Dimitri Andivahis	Recomm. N5805	07-07	08-05	09-05	09-11	
1.27.28.01	IS	18028-1:2006-07-01 (1st edition)	IT network security - Part 1: Network security management <i>(currently under revision as ISO/IEC 27033-1 (1.27.58.01))</i>	4							
1.27.28.02	IS	18028-2:2006-02-01 (1st edition)	IT network security - Part 2: Network security architecture <i>(currently under revision as ISO/IEC 27033-2 (1.27.58.02))</i>	4							

1.27.28.03	IS	18028-3: 2005-12-15 (1st edition)	IT network security -- Part 3: Securing communications between networks using security gateways <i>(currently under revision as ISO/IEC 27033-4 (1.27.58.04))</i>	4		N2415					
1.27.28.04	IS	18028-4: 2005-04-01 (1st edition)	IT network security -- Part 4: Securing remote access <i>(currently under revision as ISO/IEC 27033-5 (1.27.58.05))</i>	4		N2415					
1.27.28.05	IS	18028-5:2006-07-01 (1st edition)	IT network security -- Part 5: Securing communications across networks using Virtual Private Networks <i>(currently under revision as ISO/IEC 27033-6 (1.27.58.06))</i>	4		N2415					
1.27.31	1st WD N7142	18031 (revision of 1st edition 2005-11-01 + Cor.1:2009-02-15) 18031:2005/ Cor.1:2009-02-15	Random bit generation <i>(revision started in April 2008 as recommended in N6724)</i>	2	Debby Wallner³⁾ Gen'ya Sakurai^{2) 3)}	Recomm N6724	08-11	09-11	10-11	11-05	
	Cor.1		Technical Corrigendum 1	2							
1.27.32	IS	18032:2005-01-15 (1st edition)	Prime number generation <i>(1st confirmation in 2008 as recommended in N7128)</i>	2		N2457	2nd pre- review in 2011				
1.27.33.01	IS	18033-1:2005-02-01 (1st edition)	Encryption algorithms -- Part 1: General <i>(1st confirmation in 2008 as recommended in SC 27 N7165)</i>	2		N2460rev1	2nd pre- review in 2011				
1.27.33.01.01¹	NP 1st WD N7274	18033-1:2005/Amd.1	Encryption algorithms Part 1: General -- Amendment 1	2	Hans von Sommerfeld³⁾	Recomm. N7165	08-11	09-11	11-05	11-11	
1.27.33.02	IS	18033-2:2006-05-01 (1st edition)	Encryption algorithms -- Part 2: Asymmetric ciphers	2		N2460rev1	1st pre- review in 2009				
1.27.33.03	1st WD	18033-3 (revision of 1st edition 2005-07-01 + Cor.1:2006-08-15 + Cor.2:2007-09-01 + Cor.3:2008-03-15)	Encryption algorithms -- Part 3: Block ciphers <i>(revision started in October 2008 as recommended in N7166)</i>	2	Pil Joong Lee³⁾ Hans von Sommerfeld^{2) 3)}	N2460rev1	08-11	09-11	11-05	11-11	

	Cor.1	18033-3:2005/ Cor.1:2006-08-15	Technical Corrigendum 1	2							
	Cor.2	18033-3:2005/ Cor.2:2007-09-01	Technical Corrigendum 2	2							
	Cor.3	18033-3:2005/ Cor.3:2008-03-15	Technical Corrigendum 3	2							
1.27.33.04	WD N7271	18033-4 (revision of 1st edition 2005-07-15)	Encryption algorithms -- Part 4: Stream ciphers <i>(revision started in October 2008 as recommended in N7166)</i>	2	Atsuko Miyaji³⁾ Hans von Sommerfeld^{2) 3)}	N2460rev1	08-11	09-11	11-05	11-11	
1.27.33.04.01	2nd FPDAM N7162	18033-4:2005/AMD1	Encryption algorithms – Part 4: Stream ciphers – Amendment 1	2	Erik Zenner	Recomm. N5172	06-05	07-11	09-05	09-11	
1.27.34	IS	18043:2006-06-15 (1st edition)	Selection, deployment and operations of intrusion detection systems (IDS)	4		N4029	1st pre- review in 2009				
1.27.35	TR	18044:2004-10-15	Information security incident management <i>(currently under revision as ISO/IEC 27035 (1.27.71))</i>	4		N2699rev1					
1.27.36	IS	18045:2008-08-15 (2nd edition)	Methodology for IT security evaluation	3			1st pre- review in 2011				
1.27.37	1st WD N/A	27002 (revision of 1st edition 2005-06-15)	Code of practice for information security management <i>(as per Kyoto Plenary resolution 13 (see N6799) revision in April 2008)</i>	1	Oliver Weissmann²⁾ ³⁾ Niels Madelung^{2) 3)}		09-05	10-11	11-11	12-05	
1.27.38	Cor.1	17799:2005/ Cor.1:2007-07-01 19772:2009-02-15 (1st edition)	Technical Corrigendum 1 <i>(to indicate renumbering from 17799 to 27002)</i> Authenticated encryption	1 2			1st pre- review in 2012				
1.27.39.01	IS	13335-1: 2004-11-15 (1st edition)	Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management <i>(1st confirmation in 2007 as per resolution 15 of 19th SC 27 Plenary (see SC 27 N5939))</i>	1		N3407	2nd pre- review in 2010				

1.27.39.02	IS	27005: 2008-06-15 (1st edition)	Information security risk management	1		N3407	1st pre-review in 2011				
1.27.40	Preliminary draft	19790 (revision of 1st edition 2006-03-01 + Cor.1:2008-06-15)	Security requirements for cryptographic modules <i>(as per Summary of Voting (N6489) early revision started in April 2008)</i>	3	Randall Easter ³⁾ Jean-Pierre Quemard ^{2) 3)} Junichi Kondo ^{2) 3)}	3309rev1	09-05	10-05	11-05	11-11	
	Cor.1	19790:2006/Cor.1:2008-06-15	Technical Corrigendum 1	3							
1.27.41	PDTR N7264	TR 19791 (revision of 1st edition 2006-05-15)	Security assessment of operational systems <i>(as per Summary of voting (N6488) early revision started in April 2008)</i>	3	Mike Nash	N3394rev1		08-11	09-05	09-11	
1.27.42	FDIS N7265	19792	Security evaluation of biometrics	3	Nils Tekampe Ludovic Merrien ²⁾ Akira Otsuka ²⁾	N3367	03-11	05-11	08-11	09-05	
1.27.43	IS	21827:2008-10-01 (2nd edition)	Systems Security Engineering -- Capability Maturity Model (SSE-CMM)	3		Recomm. N4596	1st pre-review in 2011				
1.27.44	2nd FCD N7189	27004	Information security management -- Measurement	1	Eva Kuiper ²⁾ Paloma Llanaez ²⁾	N4028	04-11	06-11	09-05	09-11	
1.27.45	4th WD N7243	24745	Biometric template protection	5	Myung-Geun Chun Young Jun Lee ^{2) 3)} Jeroen Breebaart ^{2) 3)}	N3928 rev1	05-05	09-05	10-05	10-11	
1.27.46	1st WD N/A	27001 (revision of 1st edition 2005-10-15)	Information security management systems -- Requirements <i>(revision started in October 2008 as recommended by October 2008 HoD meeting)</i>	1	Angelika Plate ^{2) 3)} Matthieu Grall ^{2) 3)}		09-05	10-11	11-11	12-05	

1.27.47	FCD N7187	27003	Information security management system implementation guidance	1	Jan Branzell ²⁾ Uma Chandrashekhar ²⁾ Oliver Weissmann Satoru Yamasaki ²⁾	N4478	05-11	08-05	09-05	09-11
1.27.48	IS	24762:2008-02-01	Guidelines for information and communications technology disaster recovery services	4		N4479	1st pre- review in 2011			
1.27.49	FDIS N7400	24761	Authentication context for biometrics	5	Asahiko Yamada	N4562	05-08	06-05	08-05	08-11
1.27.50	6th WD N7237	24760	A framework for identity management	5	Rosa Garcia Ontoso ²⁾ Christophe Sténuit ²⁾	N4581	05-11	09-06	10-12	11-05
1.27.51	IS	24759:2008-07-01	Test requirements for cryptographic modules	3			1st pre- review in 2011			
1.27.52	FDIS N7385	27000	Information security management systems -- Overview and vocabulary	1	Dale Johnstone ²⁾ Kei Harada ²⁾	N4803ev1	06-05	06-11	08-11	09-05
1.27.53	IS	27006:2007-03-01 (1st edition)	Requirements for bodies providing audit and certification of information security management systems	1		N4933	1st pre- review in 2010			
1.27.54	1st CD N7239	29100	Privacy framework ¹⁾ A privacy framework	5	Stefan Weiss Sue Glueck ^{2) 3)}	N5211	06-11	08-11	09-11	10-05
1.27.55	3rd WD N7241	29101	Privacy reference architecture ¹⁾ A privacy reference architecture	5	Stefan Weiss Yong Nyuo Shin ^{2) 3)}	N5212	07-12	09-05	10-11	11-05
1.27.56	IS ITU-T	X.1051 27011	Information security managment guidelines for telecommunications organizations based on ISO/IEC 27002 (awaiting publication)	1		N5468				
1.27.57	4th WD N7235	X.eaa 29115	Entity authentication assurance	5	Richard Brackney Yoshihiro Satoh ²⁾	N5534	07-05	09-05	10-11	11-05

1.27.58.01	FCD N6919	27033-1 (revision of 18028-1, 1st edition 2006-07-01)	Network security - Part 1: Guidelines for network security <i>(revision started in May 2007 as per resolution 16 of St. Petersburg Plenary (N5939))</i>	4	Laura Kuiper	N5983	07-05	08-05	09-05	09-11
1.27.58.02	4th WD N6920 N/A	27033-2 (revision of 18028-2, 1st edition 2006-02-01)	Network security -- Part 2: Guidelines for the design and implementation of network security <i>(revision started in May 2007 as per resolution 16 of 19th SC 27 St. Petersburg Plenary (N5939))</i>	4	Laura Kuiper	N5983	07-04	09-11	10-11	11-05
1.27.58.03	3rd WD N6921	27033-3	Network security -- Part 3: Reference networking scenarios -- Risks, design technologies and control issues	4	Suhashini Sabnis	N5983	07-10	09-05	10-05	11-05
1.27.58.04	1st WD N/A	27033-4 ¹⁾ (revision of 1st edition of 18028-3 2005-12-15)	Network security -- Part 4: Securing communications between networks using security gateways - Risks, design techniques and control issues	4		N5983	09-11	10-11	11-11	12-05
1.27.58.05	1st WD N/A	27033-5 ¹⁾ (revision of 1st edition of 18028-5:2006-07-01)	Network security -- Part 5: Securing communications across networks using Virtual Private Networks (VPNs) - Risks, design techniques and control issues Securing remote access - Risks, design techniques and control issues	4		N5983	09-11	10-11	11-11	12-05
1.27.58.06	NP	27033-6 ¹⁾ (revision of 1st edition of 18028-5 2006-07-01)	Network security -- Part 6: IP convergence Securing communications across networks using Virtual Private Networks (VPNs) - Risks, design techniques and control issues	4		N5983	09-11	10-11	11-11	12-05
1.27.58.07	NP	27033-7 ¹⁾	Part 7: Wireless Guidelines for securing (specific networking technology topic heading to be inserted) - Risks, design techniques and control issues	4		N5983	09-11	10-11	11-11	12-05
1.27.59	3rd WD N7191	27007	Guidelines for information security management systems auditing	1	Angelika Plate Wang Xinjie ²⁾	N5868	07-05	09-05	11-05	11-11
1.27.60	3rd WD N7266	29128	Verification of cryptographic protocols	3	Kunihiko Miyazaki Akira Otsuka ²⁾ Shinichiro Matsuo ²⁾	N5925	08-04	09-11	10-11	11-05

1.27.61	3rd WD N6917	27031	Guidelines for ICT readiness for business continuity	4	Ron Miller Liong Chuan Ong Philip Sy	N5726	07-11	09-05	10-11	11-05
1.27.62	2nd WD N6918	27032	Guidelines for cybersecurity	4	Koji Nakao ²⁾ Aloysius Cheang ²⁾	N5722	07-05	09-05	10-05	10-11
1.27.63.01	3rd WD N7176	27034-1	Application security -- Part 1: Overview and concepts	4	Luc Poulin ²⁾ Bruno Guay ²⁾	N5729	07-07	09-05	10-05	10-11
1.27.64	Preliminary Draft N7245 N/A	29146	A framework for access management	5	Rosa Garcia Ontoso ²⁾ Christophe Stenuit ²⁾ Ji Hyum Moon ^{2) 3)}	N6256rev1	09-05	10-11	11-11	12-05
1.27.65	2nd WD N7267	29147	Responsible vulnerability disclosure	3	Faud Khan	N6319rev1	08-04	09-04	10-04	10-10
1.27.66	2nd WD N7178	TR 29149	Best practice on the provision of time-stamping services (Technical Report type 2) <i>(as per Kyoto Plenary resolution 27 (N6799) reassigned from WG 2 to WG 4)</i>	4	Jose Mañas	N6205rev1	08-04	09-05	10-05	10-11
1.27.67	1st WD N6688	29150	Signcryption	2	Yuliang Zheng Allen Roginsky ²⁾	Recomm. N6196	08-10	09-10	11-10	12-10
1.27.68	NP	27010	Information security management for inter-sector communication ¹⁾ Information security management : sector to sector interworking and communications for industry and government	1	Benoit Poletti ^{2) 4)}	N6620rev1	09-05	10-11	11-11	12-05
1.27.69	1st WD N7212	27012	Information security management guidelines for e-government services	1	Paloma Llanaez ²⁾ Pierre Saseville ²⁾	N6619	08-10	09-11	10-11	11-05
1.27.70	1st WD N7213	27008 ¹⁾ (29165)	Guidance for auditors on ISMS controls	1	Anders Carlstedt ³⁾	N6621rev1	08-10	09-10	10-10	11-05

1.27.71	1st CD N7177	27035	Information security incident management <i>(revision of ISO/IEC TR 18044:2004-10-15)</i>	4	Yoshihiro Satoh ^{2) 3)} Jing-Hua Min ^{2) 3)}	N6430	08-05	08-10	09-05	09-10
1.27.72.01	IS	11889-1	Trusted computing modul Part 1: Overview <i>(awaiting publication)</i>							
1.27.72.02	IS	11889-2	Trusted computing modul Part 2: Design principles <i>(awaiting publication)</i>							
1.27.72.03	IS	11889-3	Trusted computing modul Part 3: Structures <i>(awaiting publication)</i>							
1.27.72.04	IS	11889-4	Trusted computing modul Part 4: Commands <i>(awaiting publication)</i>							
(1.27.73)	NWIP N7221 ¹⁾ Preliminary Draft N7222 N/A NWIP N7183 ¹⁾ Preliminary Draft N7184		Guidelines for security of outsourcing	4	Laura Kuiper (acting editor)		09-05	10-11	11-11	12-05
(1.27.74)			Guidelines for identification, collection and/or acquisition and preservation of digital evience	4	Maslina Daud Kyung-Seok Lee (acting co-editors)		09-05	10-11	11-11	12-05
(1.27.75) (not yet assigned)										
1.27.76	NP	27013	Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001	1		N7201rev2	09-05	10-11	11-11	12-05
1.27.77	NP	27014	Information security governance framework	1	Kei Harada ^{2) 4)}	N7296rev1	09-05	10-11	11-11	12-05
1.27.78	NP	27015	Information security management system for financial and insurance services sector	1	E. Regan Adams ⁴⁾	N7200rev2	09-05	10-11	11-11	12-05
1.27.79	NP	29193	Secure system engineering principles and techniques	3	Anne Coat ⁴⁾	N7268rev1	09-05	10-11	11-11	12-05

1.27.80	NP	29190	Privacy capability maturity model	5		N7114rev1	09-11	11-05	12-05	12-11
1.27.81	NP	29191	Requirements on relative anonymity with identity escrow	5	Kazue Sako ⁴⁾	N7106rev1	09-11	11-05	12-05	12-11
1.27.82	NP	29192	Lightweight cryptography	2	Riaal Ramingues (acting editor)	N7276rev1	09-05	10-11	11-11	12-05
	1st WD N7275				Shiho Moriai (acting co-editor)					
WG 1 Road Map	N7193	WG 1 SD1	WG 1 Standing Document 1 -- Road Map	1	Dale Johnstone					
	N7195	WG 1 SD 2	WG 1 Standing Document 2 -- Rules and principles for definitions	1	Dale Johnstone					
WG 2 Road Map	N6714 N/A		WG 2 Road Map	2	Takeshi Chikazawa (Rapporteur)					
WG 3 Road Map	N5690		WG 3 Road Map	3	Mats Ohlin (WG 3 Convener)					
WG 4 Road Map	N6907	WG 4 SD1	WG 4 SD 1: WG 4 Road Map	4	Meng-Chow Kang (WG 4 Convener)					
	N7223	WG 4 SD1	WG 4 SD 1: WG 4 Rules and principles for definitions	4	Meng-Chow Kang (WG 4 Convener)					
WG 5 Road Map	N7247	WG 5 SD1	WG 5 SD 1: WG 5 Road Map	5	Kai Rannenber (WG 5 Convener)					
	N7249	WG 5 SD2	WG 5 Standing Document 2 -- Official Privacy Documents References List	5	Benoit Poletti					
	N7306	SC 27 SD 12	Standing Document 12 -- Assessment of Cryptographic algorithms and key lengths		Riaal Ramingues ²⁾ Hans von Sommerfeld ²⁾					
study period			Object identifiers and ASN.1 syntax		Olivier Dubuisson (Rapporteur)					
study period			Information security for Critical Infrastructure (CI) -- Sector -specific guidance (terminated in accordance with WG 1 Cyprus resolution 18 (see N7295))	1						
study period	N7216 (liaison statement)		Sector-specific ISMS standards for the World Lottery Association (terminated in accordance with Cyprus WG 1 resolution 18 (see N7295))	1						

study period		Information security governance <i>(resulted in NP 27014; see project 1.27.77,</i>	1	
study period		Early revision of ISO/IEC 27000 <i>(to broaden its scope to also cover those standards belonging to the ISO/IEC 27000 family of standards being developed in WG 4)</i>	1	Dale Johnstone (Rapporteur)
study period	N7167 (report)	Light-weight cryptographic mechanisms <i>(terminated as per WG 2 Cyprus resolution 25 (see N7303))</i>	2	
study period	N7122 (report)	Key establishment mechanisms for multiple entities <i>(terminated as per WG 2 Cyprus resolution 26 (see N7303))</i>	2	
study period	N7273 (report)	Secret sharing mechanisms <i>(extended as per WG 2 Cyprus resolution 28 (see N7303) until 2009-05)</i>	2	Kouichi Sakurai (Rapporteur)
study period	N7302rev1 (call f. contr.)	Mechanisms supporting anonymity	2	Liqun Chen (Rapporteur)
study period	N6653 (final report)	Secure system design <i>(resulted in NP 29193 (see project number 1.27.79))</i>	3	
study period	N7180 (report)	Security of outsourcing <i>(resulted in NWIP (see N7221))</i>	4	
study period	N7182 (report)	Categorization and classification of information security incident <i>(terminated in accordance with WG 4 Cyprus resolution 4 (see N6904))</i>	4	
study period	N7181 (report)	Evidence acquisition procedure for digital forensics <i>(resulted in NWIP (see N7183))</i>	4	Maslina Daud (Rapporteur)
SC 27 study period ³⁾	N7254 N/A (report)	Access control mechanisms	5	Andreas Fuchsberger ³⁾ (Rapporteur)
study period	N6866 (final report)	Privacy capability maturity model <i>(resulted in NP 29190 (see project number 1.27.80))</i>	5	

¹⁾ subject to JTC 1 endorsement

²⁾ as co-editor

³⁾ subject to sc 27 approval

⁴⁾ subject to WG 1 approval