Versione aggiornata ad ottobre 2013

Le nuove norme della famiglia 27000

e il lavoro degli enti normativi italiani

UNINFO

Introduzione al ISO/IEC JTC1 SC27

Il sottocomitato 27 (SC27), da cui nascono tutte le norme della famiglia 27000 e anche altre degne di nota, è delegato ad occuparsi, in seno al Joint Technical Committee (JTC1) di ISO/IEC, della **sicurezza delle informazioni**.

I suoi 5 Working Groups (WG) hanno i seguenti mandati:

- **WG1**: sistemi di gestione per la sicurezza delle informazioni, controlli, accreditamento, certificazione e audit, governance
- **WG2**: crittografia e meccanismi di sicurezza
- **WG3**: criteri, metodologie e procedure per la valutazione, il test e la specifica della sicurezza
- **WG4**: servizi di sicurezza collegati all'attuazione dei sistemi di gestione per la sicurezza delle informazioni
- **WG5**: aspetti di sicurezza di gestione delle identità, biometria e privacy

ISO/IEC JTC1 SC27: i 5 Working Group

UNINFO

Standard principali pubblicati dal WG1

27000: Information security management systems overview and vocabulary	**27001: Information security management systems - requirements**	**27002: Code of practice for information security controls**	27003: Information security management systems implementation guidance
27004: Information security management – Measurements	27005: Information security risk management	**27006: Requirements for bodies providing audit and certification of information security management systems**	27007: Guidelines for information security management systems auditing
27008: Guidelines for auditors on information security controls	27010: Information security management for inter-sector and inter-organisational communications	27011: Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	27013: Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
27014: Governance of information security	27015: Information secuirty management guidelines for financial services	27016: Information security management – Organizational economics	27019: Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

UNINFO

Standard principali pubblicati dal WG2

7064: Check character systems	**9796-2: Digital signature schemes giving message recovery**	9797: Message authentication codes (3 parts)	**9798: Entity authentication (6 parts)**
10116: Modes of operation for an n-bit block cipher algorithm	**10118: Hash functions (4 parts)**	11770: Key management (5 parts)	13888: Non repudiation (3 parts)
14888: Digital signatures with appendix (3 parts)	15946: Cryptography based on elliptic curves	18014: Time stamping services (4 parts)	18032: Prime number generation
18033: Encryption algorithms (5 parts)	18730: Blind digital signatures (2 parts)	19772: Authenticated encryption	29150: Sigcryption
	29192: Lightweight cryptography (4 parts)		

UNINFO

Standard principali pubblicati dal WG3

11889: Trusted platform module	**15408: Evaluation criteria for IT security**	15443: A framework for IT security assurance
15446: Guide for the production of protection profiles and security targets	**18045: Methodology for IT security evaluation**	19790: Security requirements for cryptographic modules
19791: Security assessment of operational systems	19792: Security evaluation of biometrics	20004: Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045
21827: Systems security engineering capability maturity model (SSE-CMM)	24759: Test requirements for cryptographic modules	29128: Verification of cryptographic protocols

Standard principali pubblicati dal WG4

14516: Guidelines for the use and management of Trusted Third Party services	15816: Security information objects for access control	15945: Specification of TTP services to support the application of digital signatures
18043: Selection, deployment and operations of intrusion detection systems	24762: Guidelines for information and communication technology disaster recovery services	**27031: Guidelines for ICT readiness for business continuity**
27032: Guidelines for cybersecurity	**27033: Network security (5 parts)**	27034: Application security
27035: Information security incident management	27037: Guidelines for identification, collection, acquisition and preservation of digital evidence	29149: Best practice on the provision and use of time-stamping services

Standard principali pubblicati dal WG5

24761: Authentication context for biometrics

24745: Biometric information protection

24760: A framework for identity management

29100: Privacy framework

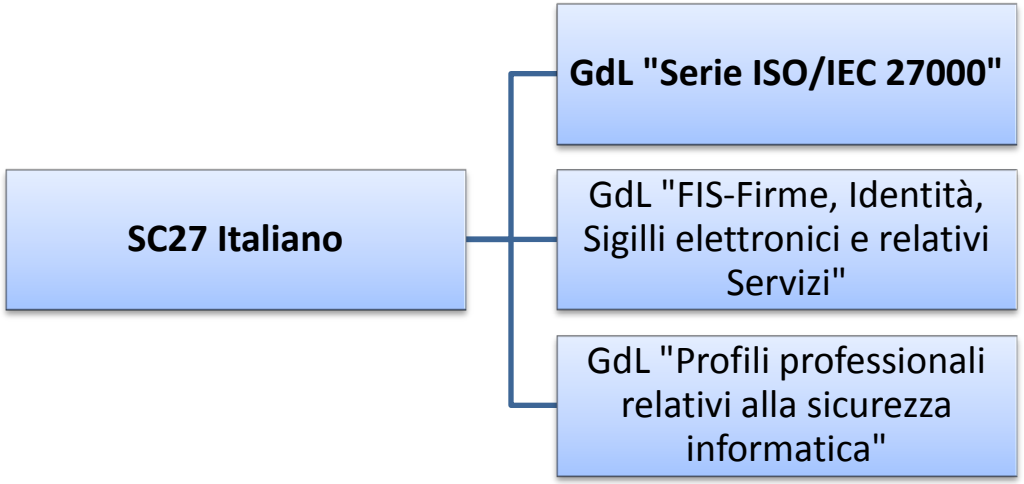
29191: Requirements for partially anonymous, partially unlinkable authentication

UNINFO

Partecipanti al ISO/IEC JTC1 SC27

Alle attività del SC27 partecipano 50 nazioni con diritto di voto e 19nazioni come osservatori, per un totale di **69 paesi** a cui si aggiungono 35 enti, soggetti e progetti internazionali attraverso liaison.

L'Italia ha diritto di voto ed è rappresentata da **UNINFO**, Ente federato di UNI per l'intero settore delle tecnologie informatiche. All'interno di UNINFO è strutturato un SC27 nazionale per garantire adeguata partecipazione alle attività internazionali, così strutturato:



UNINFO

Attività del SC27 Italiano

Oltre a fornire un costante e ricco contributo italiano ai lavori normativi dei WG1, 3, 4 il comitato italiano ha condotto nel tempo le seguenti iniziative:

- Traduzione in italiano della 27001 (2006)
- Creazione di GdL verticali (2009-2012)
- Organizzazione del meeting internazionale del SC27 a Roma (2012)
- Pubblicazione del quaderno "La gestione della Sicurezza delle Informazioni e della Privacy", liberamente scaricabile **qui** (2012)
- **Traduzione allineata delle 27000, 27001 e 27002 in italiano (in corso)**
- Pubblicazione del quaderno "Guida alla realizzazione di una soluzione di firma grafometrica sicura" (in corso)
- Definizione dei profili professionali legati alla sicurezza informatica (in corso)

Lo standard ISO/IEC 27000

- Fornisce una visione ad alto livello dei Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI) che sono trattati dalle norme della famiglia 27000
- Definisce i termini e le definizioni di cui tutte le suddette norme fanno uso
- Fornisce inoltre una breve descrizione di tutti gli standard della famiglia 27000
- Applicabile a tutti i tipi di realtà organizzative di qualunque dimensione (imprese commerciali, enti governativi, organizzazioni no-profit, ecc.)
- Indispensabile per una piena comprensione dei requisiti della ISO/IEC 27001 e dei controlli di sicurezza della ISO/IEC 27002

La nuova ISO/IEC 27000

Highlights

- E’ una norma in continuo divenire: da quando è stata approvata la prima versione del 2009 si è iniziato a lavorare a una *early revision* che è stata pubblicata l'anno scorso
- Ora la norma è nuovamente in fase di revisione: dovendo recepire i nuovi termini di tutte le norme della famiglia 27000 è soggetta a cambiamenti molto frequenti
- La prossima uscita è prevista ad aprile 2014

Struttura

1 Scope

2 Terms and definitions

3 Information security management system

4 ISMS family of standard

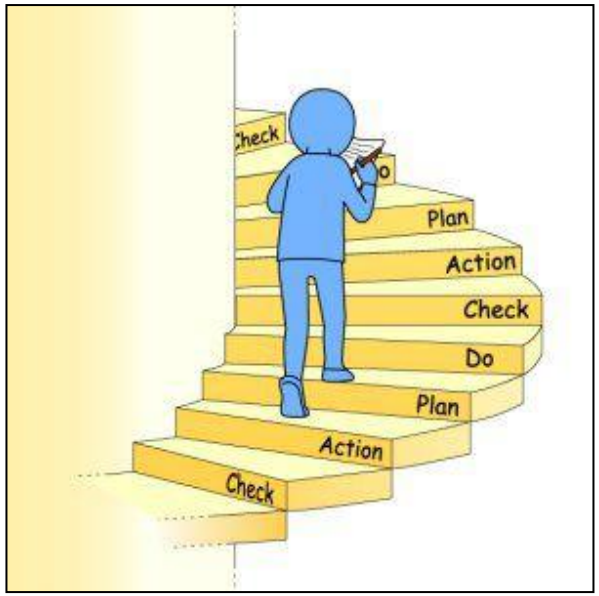
La struttura dalla versione 2012 alla versione 2014 rimane invariata e la norma rimarrà pubblicamente disponibile su:

http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

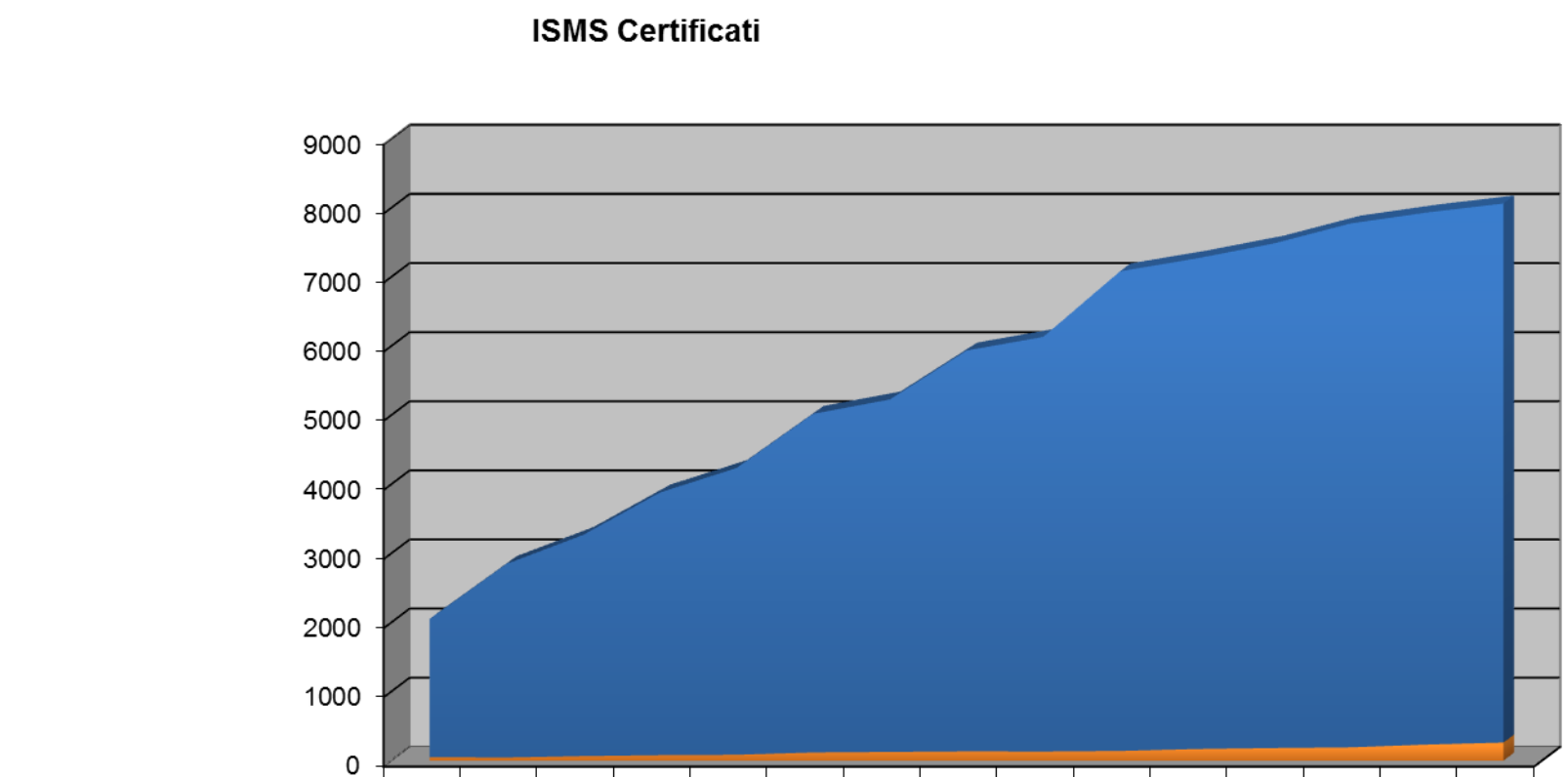
Lo standard ISO/IEC 27001

Sistema di Gestione per la Sicurezza delle Informazioni (**SGSI o ISMS**).

- Applicabile a realtà di ogni dimensione
- quasi 20 anni di esistenza sul mercato
- Ambito definibile a piacimento
- Approccio ciclico (**PDCA**)
- Costituisce un framework completo
- Dice **cosa** fare, non **come** farlo
- Rivolto al miglioramento continuo
- E' un riferimento universale e **certificabile**



Diffusione della ISO/IEC 27001



	gen-06	lug-06	gen-07	lug-07	gen-08	lug-08	gen-09	lug-09	gen-10	lug-10	gen-11	lug-11	gen-12	lug-12	gen-13
ISO 27001:2005 (Worldwide)	2000	2800	3200	3800	4150	4900	5100	5800	6000	6940	7100	7300	7580	7700	7800
ISO 27001:2005 (Italy)	50	45	66	79	84	118	126	134	132	140	168	182	192	232	262

La nuova ISO/IEC 27001

Highlights

- utilizzata la nuova «High level structure (HLS)» per i sistemi di gestione (ex ISO Guide 83) richiesta dalle Direttive ISO dal 2012
- stravolte struttura e impostazione
- aggiunti requisiti derivanti dal common text (rischi all'ISMS, formalizzazione degli obiettivi, comunicazione)
- allineamento alla ISO 31000
- aumentati i requisiti sulla valutazione delle performance
- ridotti i requisiti sul risk assessment (no asset, minacce, vulnerabilità)
- rimosse le azioni preventive

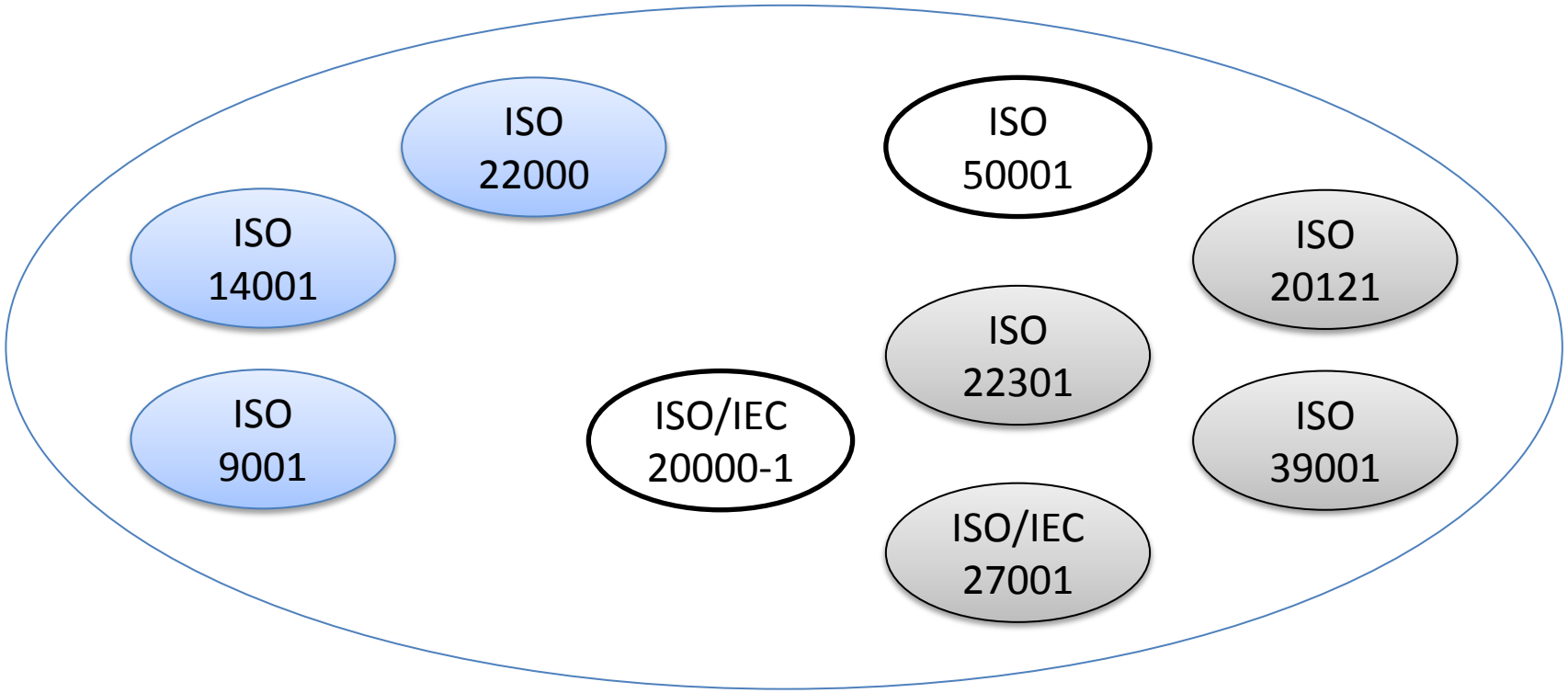
L'High level structure

- Nel 2009, il Technical Management Board (TMB) della ISO ha chiesto al Joint Technical Coordination Group (JTCG) di stabilire un nuovo standard per sviluppare gli standard sui sistemi di gestione (management system standards).
- Si cominciò così a sviluppare il «Common Structure and Identical Text for Management System Standards of the Joint Technical Coordination Committee (JTCG)».
- Nell'ottobre 2010 il testo della common structure fu fatto circolare e l'SC27 decise di adottare la common structure per la ISO/IEC 27001.
- Nel 2012 è stato pubblicato come parte dell'Allegato SL delle ISO/IEC Directives, Part 1, Consolidated ISO Supplement.
  - Non più una guida, ma una direttiva.
  - È anche noto, impropriamente, come "Annex SL".
- Il testo presenta molte innovazioni rispetto a quanto consolidato negli ultimi 10 anni a partire dalla ISO 9001:2000.

Perché l'HLS

- Uniformazione e miglioramento dell'efficacia nella redazione degli standard per i Comitati tecnici dell'ISO.
- Migliore allineamento e compatibilità tra gli standard.
- Massimo beneficio per le organizzazioni che realizzano un sistema di gestione integrato
  - E' stata pubblicata una nuova versione della BS PAS 99 come linea guida per l'interpretazione dell'HLS.

Standard e HLS

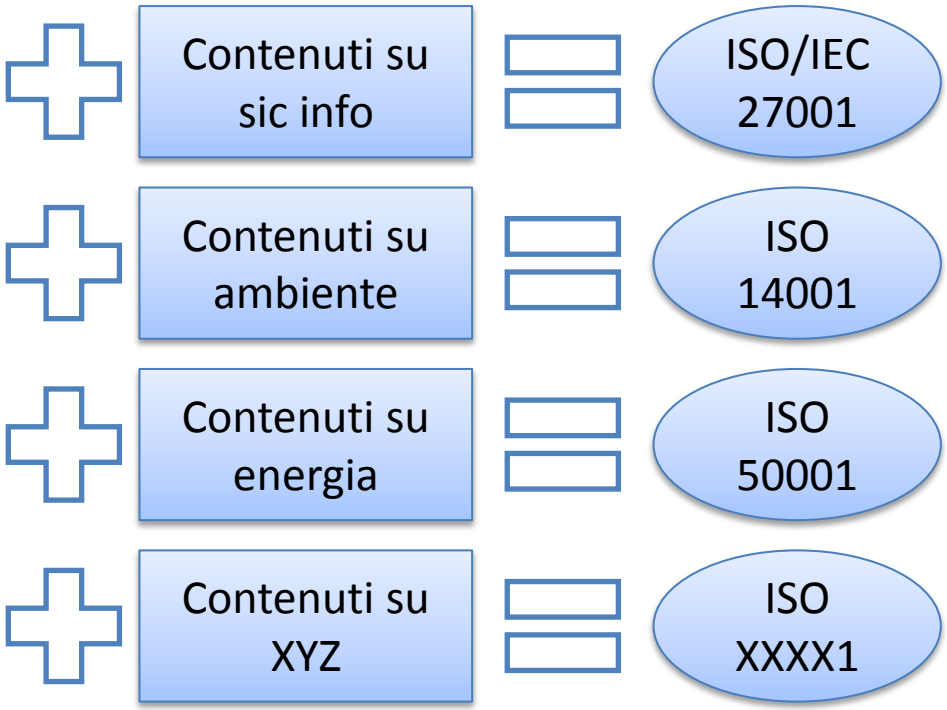


In revisione con adozione HLS

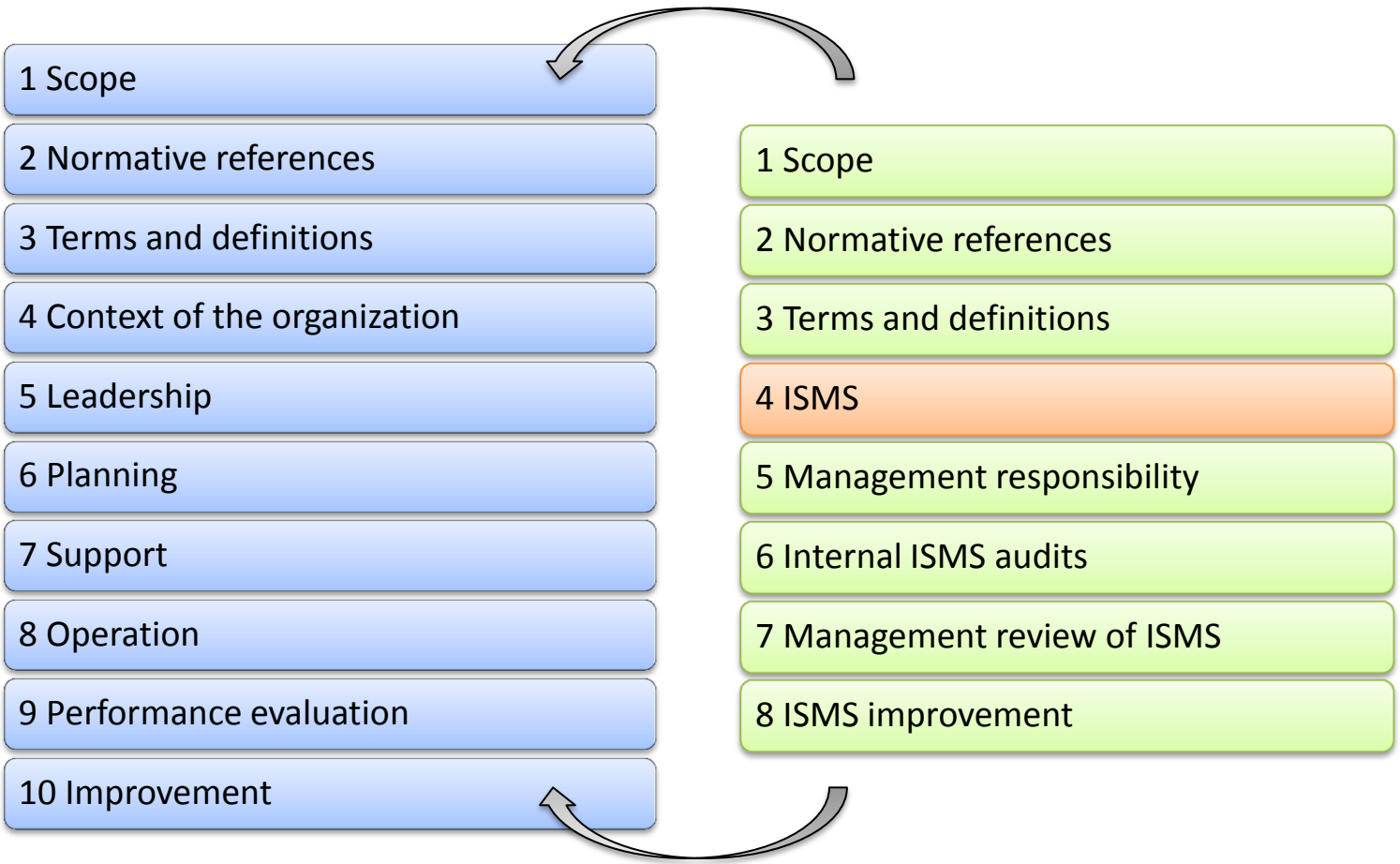
Pubblicate con adozione HLS

Lo schema dell'HLS

- Context
- Leadership & commitment
- Policy
- Roles & responsibilities
- Actions to address risks & opportunities
- Plan and objectives
- Resources
- Competences
- Awareness
- Communication
- Documented information
- Internal audit
- Management review
- Improvement



Nuova struttura ISO/IEC 27001



Nuova 27001 – Context (§4)

- Da HLS: Introdotta una valutazione dei rischi a livello di sistema di gestione (da applicare anche per la ISO 9001).
- Richiesta la comprensione del contesto interno ed esterno dell'organizzazione, nonché l'identificazione degli stakeholder e delle loro aspettative.
- I requisiti per la descrizione dell'ambito sono ridotti (perché "impliciti").
- Informazioni documentate (procedure, registrazioni):
  - scope (come nella ISO/IEC 27001:2005)

Nuova 27001 – Leadership (§5)

- Da HLS: Introdotta la “Leadership” al posto del “Impegno della Direzione”.
- Informazioni documentate (procedure, registrazioni):
  - information security policy (come nella ISO/IEC 27001:2005)

Nuova 27001 – Planning (§6)

- Risk assessment non più esplicitamente legato ad asset, minacce e vulnerabilità.
  - Si chiede di identificare i rischi relativi alla sicurezza delle informazioni e associati alla perdita di riservatezza, integrità e disponibilità.
  - La valutazione e il trattamento del rischio sono nel planning perché contribuiscono alla pianificazione del sistema di gestione per la sicurezza delle informazioni.
  - Il metodo deve sempre garantire la coerenza, validità e comparabilità dei risultati.
  - La definizione di rischio e quelle ad essa correlate (per esempio quella di “Livello di rischio”) porta comunque ad individuare asset, minacce e vulnerabilità (la “completezza” del risk assessment è un requisito “implicito”).
- Si chiede di identificare i “proprietari dei rischi", responsabili delle decisioni in merito (non più solo la Direzione).
- Rimangono l’Annex A e il SoA.
- Più dettagli su come affrontare gli obiettivi del sistema di gestione.
- Informazioni documentate (procedure, registrazioni):
  - risk assessment process, risk treatment process, security objectives (simile alla precedente)

Nuova 27001 – Support (§7)

- Tratta delle risorse, delle risorse umane, della comunicazione e delle informazioni documentate.
- Maggiore rilievo alla consapevolezza del personale.
- Più dettagli su come devono essere affrontate le comunicazioni.
- Non si parla più di “Documenti” e “Registrazioni”, ma di “**Informazioni documentate**” (la necessità di un documento deve essere fatta risalire ai rischi a livello di sistema di gestione), cambia anche pertanto la documentazione "obbligatoria".
- In generale, sembra ci siano meno richieste di documenti e registrazioni rispetto alla precedente edizione; ma attenzione che molti requisiti possono essere ritenuti “impliciti” (i documenti sono quindi necessari per chi vuole essere oggetto di audit).
- Informazioni documentate (procedure, registrazioni):
  - evidence of competence (come nella ISO/IEC 27001:2005).

Nuova 27001 – Operations (§8)

- Sono richiamati la valutazione e il trattamento del rischio.
- Informazioni documentate (procedure, registrazioni):
  - confidence on operational planning and control
  - risk assessment results
  - result of information security risk treatment

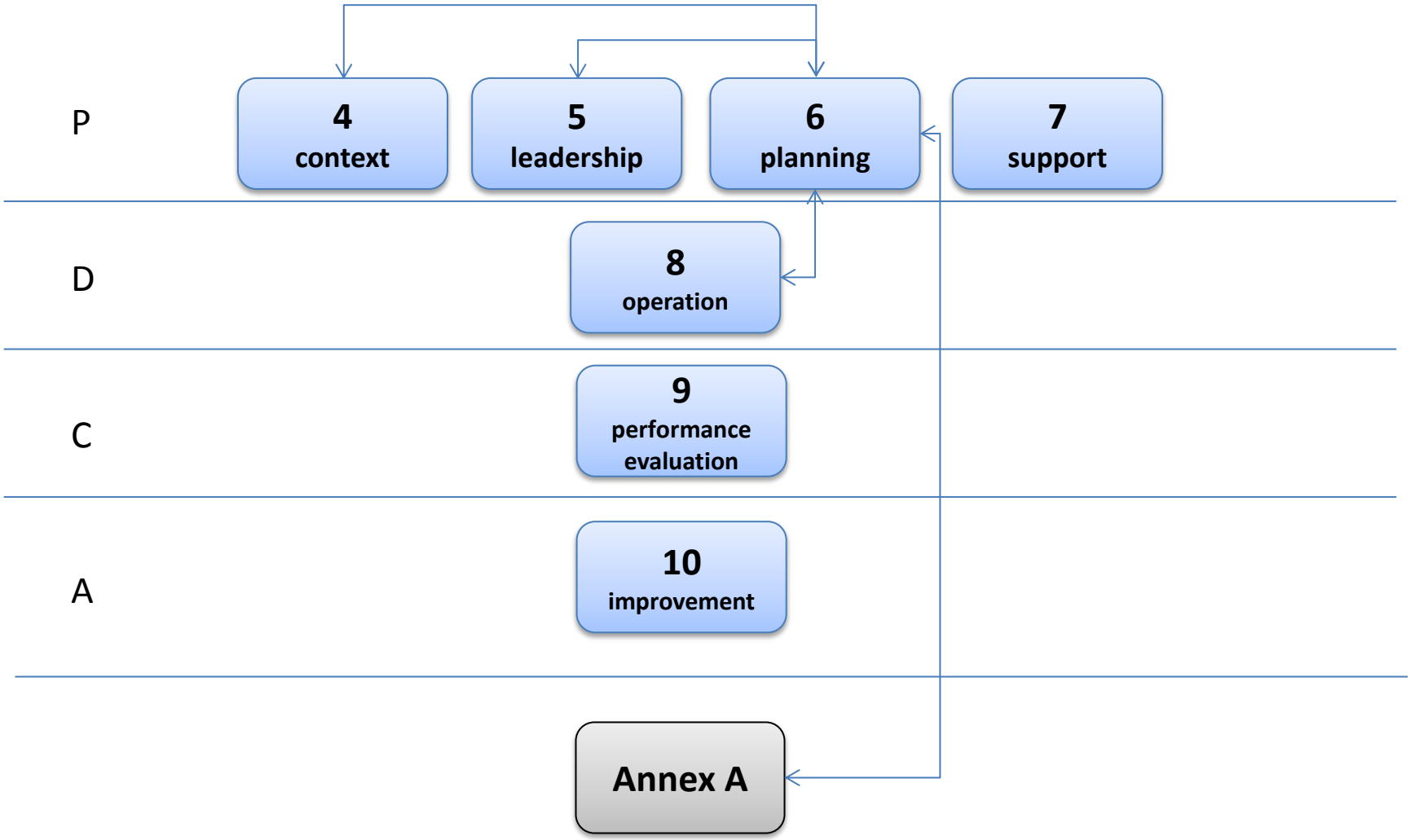
Nuova 27001 – Performance evaluation (§9)

- Tratta di:
  - monitoraggio, misurazioni, analisi e valutazione;
  - audit interni;
  - riesame di Direzione.
- La valutazione delle performance specifica ora maggiori elementi, riferendosi a controlli e processi.
- Non più esplicitamente richiesta una valutazione del “fabbisogno di risorse” nel riesame di Direzione (il quale resta comunque richiesto).
- Aggiunta la richiesta di considerazione del raggiungimento degli obiettivi di sicurezza nel riesame di Direzione.
- Informazioni documentate (procedure, registrazioni):
  - evidence of monitoring and measurement results;
  - evidence of audit programme and results;
  - evidence of results of management reviews.

Nuova 27001 – Improvement (§10)

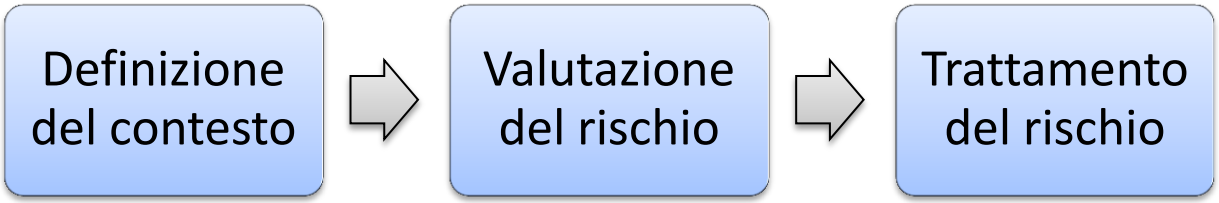
- Tratta di:
  - non conformità e azioni correttive;
  - miglioramento continuo.
- Eliminate le azioni preventive (da vedere come caso particolare di trattamento dei rischi a livello di sistema di gestione che, quindi, non ha solo valenza strategica, ma anche più operativa).
- Informazioni documentate (procedure, registrazioni):
  - nature and actions resulting from nonconformities
  - results of corrective actions.

Nuova struttura e PDCA



Lo standard ISO/IEC 27002

Il vero "motore" della ISO/IEC 27001 è il processo di gestione del rischio relativo alla sicurezza delle informazioni, così specificato genericamente nella ISO 31000:



Uno dei modi più diretti per effettuare un "trattamento del rischio" è quello di ridurlo ad un livello accettabile adottando dei controlli di sicurezza, dei quali la 27002 può essere considerata come un **esteso catalogo**.

La nuova ISO/IEC 27002

Highlights

- mantenimento come annex A della 27001
- ristrutturazione in **clauses** (aree)**, control categories** (obiettivi) e **controls** (controlli)
- rimozione della parte di risk assessment
- passaggio da 133 controlli a 114 accorpando diversi controlli tecnici
- aggiunta di controlli su **sviluppo sicuro, testing, supply chain e PM**
- miglioramento soprattutto delle implementation guidance
- revisione della terminologia e adattamento alle nuove tecnologie

Nuova struttura ISO/IEC 27002

5 Information Security Policies	4 Risk assessment
6 Organisation of Information Security	5 Security policy
7 Human Resources Security	6 Organization of information security
8 Asset Management	7 Asset management
9 Access control	8 Human resources security
10 Cryptography	9 Physical and environmental security
11 Physical and environmental Security	10 Communications and operations management
12 Operations Security	11 Access control
13 Communications Security	12 IS acquisition, development and maintenance
14 Systems acquisition, development and maintenance	13 Information security incident management
15 Supplier relationships	14 Business continuity management
16 Information Security Incident Management	15 Compliance
17 IS aspects of Business Continuity	
18 Compliance	

Nuovi controlli e categorie

Alcuni nuovi controlli derivano da un focus di gestione, altri dal mutato ambiente di rischio rispetto al 2005.

- *6.1.5 Information security in project management*
- *12.6.2 Restrictions on software installation*
- *14.2.1 Secure development policy*
- *14.2.5 Secure system engineering principles*
- *14.2.6 Secure development environment*
- *14.2.8 System security testing*
- *15.1.3 Information and communication technology supply chain*
- *16.1.4 Assessment of and decision on information security events*

Vi sono inoltre 3 nuove categorie:

- *14.3 Test data*
- *17.2 Redundancies*
- *18.2 Information security reviews*

Controlli scorporati

Diversi controlli della versione precedente sono stati incorporati nel testo della nuova 27001 o sono stati inglobati in altri controlli di ampliato ambito:

6.1.1 Management commitment to information security

6.1.2 Information security coordination

6.1.4 Authorization process for information processing facilities

6.2.1 Identification of risks related to external parties

6.2.2 Addressing security when dealing with customers

10.2.1 Service delivery

10.4.2 Controls against mobile code

10.7.4 Security of system documentation

10.8.5 Business information systems

10.9.3 Publicly available information

10.10.2 Monitoring system use

10.10.5 Fault logging

11.4.2 User authentication for external connections

11.4.3 Equipment identification in networks

11.4.4 Remote diagnostic and configuration port protection

11.4.6 Network connection control

11.4.7 Network routing control

11.5.2 User identification and authentication

11.5.5 Session time out

11.5.6 Limitation of connection time

11.6.2 Sensitive system isolation

12.2.2 Control of internal processing

14.1.5 Testing, maintaining and re5assessing business continuity plans

15.1.5 Prevention of misuse of information processing facilities

15.3.2 Protection of information systems audit tools

Nuova 27002

Information security policies (§5)

- La numerazione e l'intento dell'area rimane uguale a quella precedente
- Il focus si sposta su tutte le policy, non solo su quella per la sicurezza delle informazioni

Organization of information security (§6)

- La parte relativa alle parti esterne (vecchia 6.2) viene spostata nella nuova sezione 15
- La parte relativa all'uso dei dispositivi portatili e al telelavoro (vecchia 11.7) viene spostata nell'area 6
- Nuovo controllo
  - *6.1.5 Information security in project management*

Human resource security (§7)

- Corrisponde all'omonima area 8 della vecchia versione
- I controlli inerenti la restituzione degli asset vengono spostati all'area 8 e quelli relativi alla rimozione dei diritti di accesso all'area 9

Nuova 27002

Asset management (§8)

- Corrisponde all'omonima area 7 della vecchia versione
- Incorpora i controlli inerenti la restituzione degli asset
- Incorpora la categoria inerente la gestione dei supporti (vecchia 10.7)

Access control (§9)

- Corrisponde all'omonima area 11 della vecchia versione
- Non si parla più di "password" ma più generalmente di "informazioni segrete per l'autenticazione"
- Incorpora i controlli inerenti la rimozione dei diritti di accesso
- Cade la distinzione tra controllo di accesso a livello di sistema operativo e a livello di applicazione (vecchie 11.5 e 11.6 rispettivamente)

Nuova 27002

Cryptography (§10)

- Corrisponde alla vecchia categoria 12.3

Physical and environmental security (§11)

- Corrisponde all'omonima area 9 della vecchia versione
- Incorpora i controlli inerenti le apparecchiature incustodite e la politica di schermo e scrivania pulite (vecchia 11.3)

Operations security (§12)

- Nasce dalla scissione della vecchia area 10 (Communications and operations management) mantenendo la parte di procedure, malware, backup, logging e sincronizzazione
- Incorpora la gestione delle vulnerabilità tecniche (sempre 12.6)
- Incorpora i controlli di audit per i sistemi informativi (vecchia 15.3)
- Nuovo controllo
  - *12.6.2 Restrictions on software installation*

Nuova 27002

Communications security (§13)

- Nasce dalla scissione della vecchia area 10 (Communications and operations management) mantenendo la parte di sicurezza delle reti e di scambio di informazioni
- Incorpora i controlli inerenti la separazione delle reti

System acquisition, development and maintenance (§14)

- Corrisponde all'omonima area 12 della vecchia versione ma risulta significativamente arricchita
- Incorpora i controlli inerenti la protezione dei servizi applicativi sia verso l'esterno che non (vecchi 10.9.1 e 10.9.2)
- Nuovi controlli
  - *14.2.1 Secure development policy*
  - *14.2.5 Secure system engineering principles*
  - *14.2.6 Secure development environment*
  - *14.2.8 System security testing*

Nuova 27002

Supplier relationships (§15)

- Questa nuova area incorpora le vecchie categorie 6.2 e 10.2 relative rispettivamente alla gestione delle terze parti e dei servizi da esse forniti
- Nuovo controllo
  - *15.1.3 Information and communication technology supply chain*

Information security incident management (§16)

- Corrisponde all'omonima area 13 della vecchia versione, mantenendone l'impostazione complessiva
- Nuovo controllo
  - *16.1.4 Assessment of and decision on information security events*

Nuova 27002

Information security aspects of business continuity management (§17)

- Corrisponde all'area 14 della vecchia versione, legandosi di più alla nuova impostazione derivante dalla ISO 22301 e dalla ISO/IEC 27031
- Cambia la struttura dei controlli che sono maggiormente legati al PDCA

Compliance (§18)

- Corrisponde all'omonima area 15 della vecchia versione
- Incorpora i controlli inerenti il riesame indipendente della sicurezza delle informazioni

Contatti e ringraziamenti

UNINFO

http://www.uninfo.it/

uninfo@uninfo.it

Corso Trento 13 - 10129 Torino

Tel. +39 011501027 - Fax +39 011501837

Si ringraziano per la preziosa e indispensabile collaborazione alla stesura della presente:

Fabio Guasconi – Presidente SC27 UNINFO

Cesare Gallotti – Chairman WG1 SC27 UNINFO

Mauro Bert – GdL Serie 27000 UNINFO

Riccardo Bianconi – GdL Serie 27000 UNINFO

Fabrizio Cirilli – GdL Serie 27000 UNINFO