INTRODUZIONE ALLA NUOVA EDIZIONE DELLA UNI CEI EN ISO/IEC 27002:2022

7 APRILE 2022

UNI
UN MONDO FATTO BENE

UNITRAIN
Conoscere e applicare gli standard

PRESENTAZIONE

La UNI CEI EN ISO/IEC 27002, vera capostipite dell'attuale famiglia di norme della serie 27000 e catalogo indispensabile di controlli referenziato nell'appendice A della UNI CEI EN ISO/IEC 27001:2017, ha origine all'inizio degli anni 90 ed è ora incipiente una sua quarta edizione, da cui esce tanto diversa come mai prima d'ora è avvenuto, introducendo insieme cambiamenti strutturali e sostanziali. I controlli sono inoltre finalmente aggiornati rispetto ai nuovi trend tecnologici e organizzativi.

OBIETTIVI

Il corso è finalizzato a spiegare la nuova struttura della norma e il corretto uso dei nuovi elementi da essa introdotti, i temi e gli attributi, in modo da dare ai partecipanti tutti gli strumenti per applicarla in modo corretto in qualsiasi ambito. Per fare questo la norma è presentata in modo agnostico rispetto alla classica formazione legata all'auditing o all'implementazione, fornendo indicazioni utili in entrambe le direzioni.

DESTINATARI

Il corso è principalmente rivolto a:

- Chief Information Security Officers (CISO)
- Dirigenti delle funzioni IT e Security/Cybersecurity
- Responsabili di sistemi di gestione per la sicurezza delle informazioni
- Consulenti e specialisti operanti nella Security/Cybersecurity

DOCENTE

FABIO GUASCONI –

UNINFO - Chairman UNI/CT 510 "Sicurezza" e Membro UNI/CT 043/GL 05 "Organizzazione e gestione della sicurezza"

CONDIVIDIAMO IL NOSTRO PATTO D'AULA

-Conosciamoci: iniziamo con un giro di presentazione. Ognuno di noi potrà dire di cosa si occupa, in quale ambito lavora, quali aspettative ha rispetto al corso. Se il corso si svolge da remoto rendiamoci riconoscibili scrivendo il nostro nome e cognome nella nostra finestra di Zoom

-Partecipiamo attivamente e confrontiamoci: il corso è un momento di apprendimento che passa anche dal confronto con il docente e i partecipanti. Facciamo domande, chiediamo chiarimenti, ascoltiamo i contributi di tutti

-Utilizziamo gli strumenti in modo consapevole: se il corso si svolge da remoto teniamo preferibilmente accesa la webcam; silenziamo il microfono quando non stiamo parlando; alziamo la mano per richiedere la parola; usiamo la chat se indicato dal docente. Se il corso si svolge in presenza, alziamo la mano per richiedere la parola

-Stabiliamo insieme le pause e rispettiamole

-Evitiamo distrazioni: per quanto possibile, silenziamo il telefono ed evitiamo di leggere mail o messaggi. Durante le pause avremo modo di gestire eventuali urgenze

-Contribuiamo al miglioramento dei corsi UNITRAIN: al termine del corso, compiliamo il questionario di customer satisfaction e forniamo eventuali suggerimenti di miglioramento

-Per il rispetto della privacy di tutti, non ci è permesso effettuare registrazioni audio, video o acquisire screenshot

IL TEAM UNITRAIN SI IMPEGNA A:

-Inviarvi il materiale didattico

-Elaborare ed inviare l'attestato di partecipazione a chi abbia frequentato almeno il 90% dell'ammontare ore del corso. UNITRAIN si riserva la facoltà di verificare, a campione, l'effettiva partecipazione al corso attraverso appelli intermedi .

ISO/IEC 27002:2022

Introduzione alla nuova edizione della UNI CEI EN ISO/IEC 27002 "Sicurezza delle informazioni, cybersecurity e protezione della privacy - Controlli per la sicurezza delle informazioni"

7 aprile 2022

UNI
UN MONDO FATTO BENE

UNITRAIN
Conoscere e applicare gli standard

CONDIVIDIAMO IL NOSTRO PATTO D'AULA

-Conosciamoci: iniziamo con un **giro di presentazione**. Ognuno di noi potrà dire di cosa si occupa, in quale ambito lavora, quali aspettative ha rispetto al corso, ecc. (30" circa). Se il corso si svolge da remoto rendiamoci riconoscibili scrivendo il nostro nome e cognome nella nostra finestra di Zoom

-Partecipiamo attivamente e confrontiamoci: il corso è un momento di apprendimento che passa anche dal **confronto con il docente** e i partecipanti. Facciamo domande, chiediamo chiarimenti, ascoltiamo i contributi di tutti

-Utilizziamo gli strumenti in modo consapevole: se il corso si svolge da remoto **teniamo preferibilmente accesa la webcam; silenziamo il microfono** quando non stiamo parlando; alziamo la mano per richiedere la parola; usiamo la chat se indicato dal docente. Se il corso si svolge in presenza, alziamo la mano per richiedere la parola

-Stabiliamo insieme le **pause** e rispettiamole

Evitiamo distrazioni: per quanto possibile, **silenziamo il telefono ed evitiamo di leggere mail o messaggi**. Durante le pause avremo modo di gestire eventuali urgenze

-Contribuiamo al miglioramento dei corsi UNITRAIN: al termine del corso, compiliamo il questionario di **customer satisfaction** e forniamo eventuali suggerimenti di miglioramento

-Per il rispetto della privacy di tutti, non ci è permesso effettuare registrazioni audio, video o acquisire screenshot

IL TEAM UNITRAIN SI IMPEGNA A:

-Inviarvi il materiale didattico

-Elaborare ed inviare l'attesto di partecipazione a chi abbia frequentato almeno il 90% dell'ammontare ore del corso

Relatore

Fabio GUASCONI

- ✓Presidente del CT 510 di **UNINFO** "Sicurezza"
- ✓Direttivo **CLUSIT**
- ✓Esperto **SBS**
- ✓Esaminatore UNI 11697
- ✓Certificazioni CISA, CISM, PCI-QSA/3DS/QPA/P2PE/CPSA, ITIL, PRINCE2, ISFS, LA 27001/22301/9001, LI 27001, DPO

UNINFO

Clusit
Associazione Italiana per la Sicurezza Informatica

UNI
UN MONDO FATTO BENE

UNITRAIN
Conoscere e applicare gli standard

Giro di presentazione

Oltre a presentarvi brevemente (nome, cognome, ruolo ricoperto), vi invitiamo a dirci:

1) Che esperienze avete in materia di sicurezza delle informazioni?
2) Qual è il vostro livello di dimestichezza con la ISO/IEC 27001?
3) Se avete già letto o utilizzato la nuova ISO/IEC 27002?

Agenda

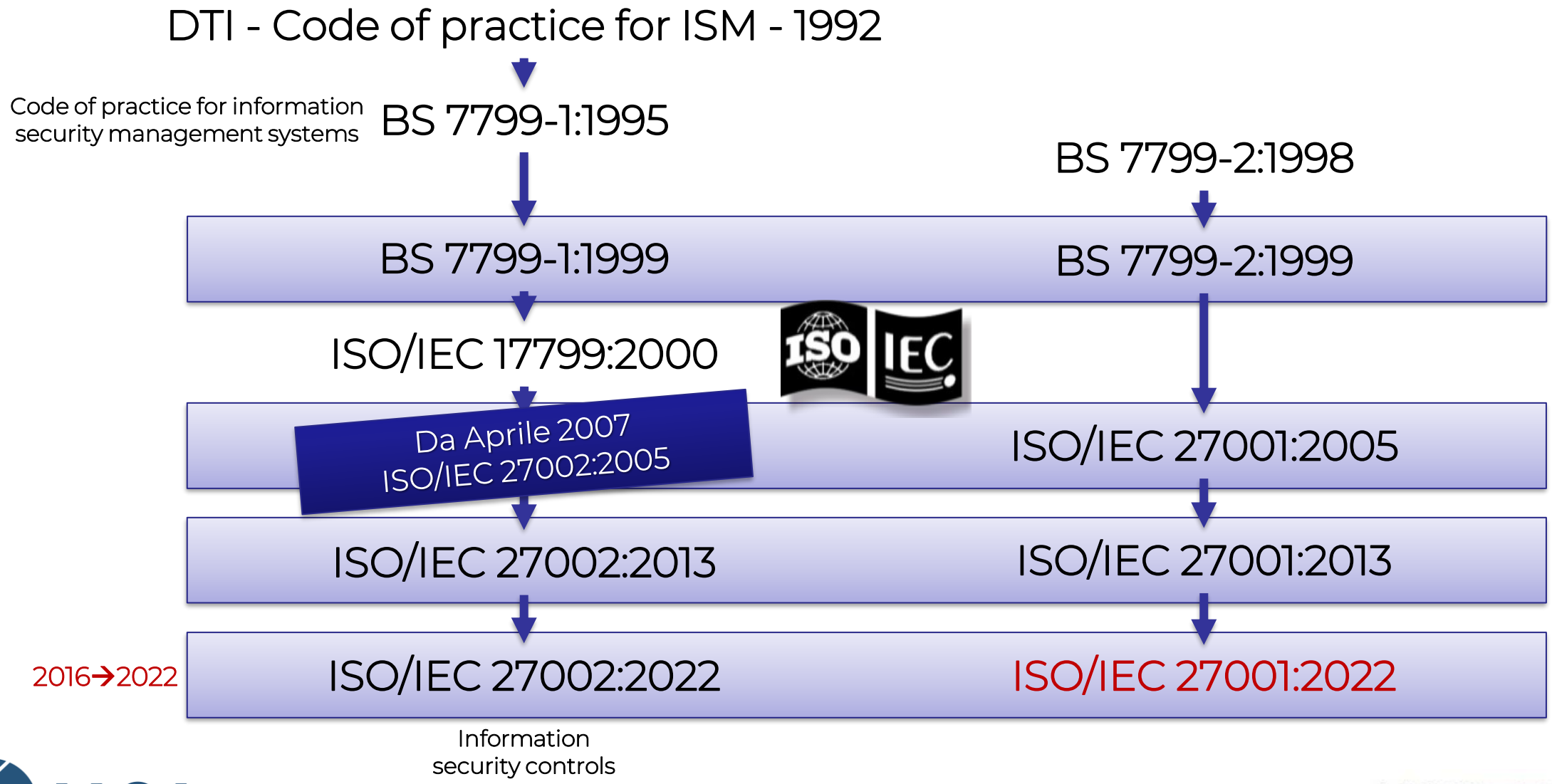
- Breve storia della norma
- Problemi principali della versione del 2013
- Nuova struttura della norma
- Temi, attributi e loro impiego
- Cambiamenti ai controlli
- Conseguenze dei cambiamenti
- Allineamento atteso con la UNI CEI EN ISO/IEC 27001
- Periodi e modalità di transizione alla nuova versione

Pausa

Agenda

- Breve storia della norma
- Problemi principali della versione del 2013
- Nuova struttura della norma
- Temi, attributi e loro impiego
- Cambiamenti ai controlli
- Conseguenze dei cambiamenti
- Allineamento atteso con la UNI CEI EN ISO/IEC 27001
- Periodi e modalità di transizione alla nuova versione

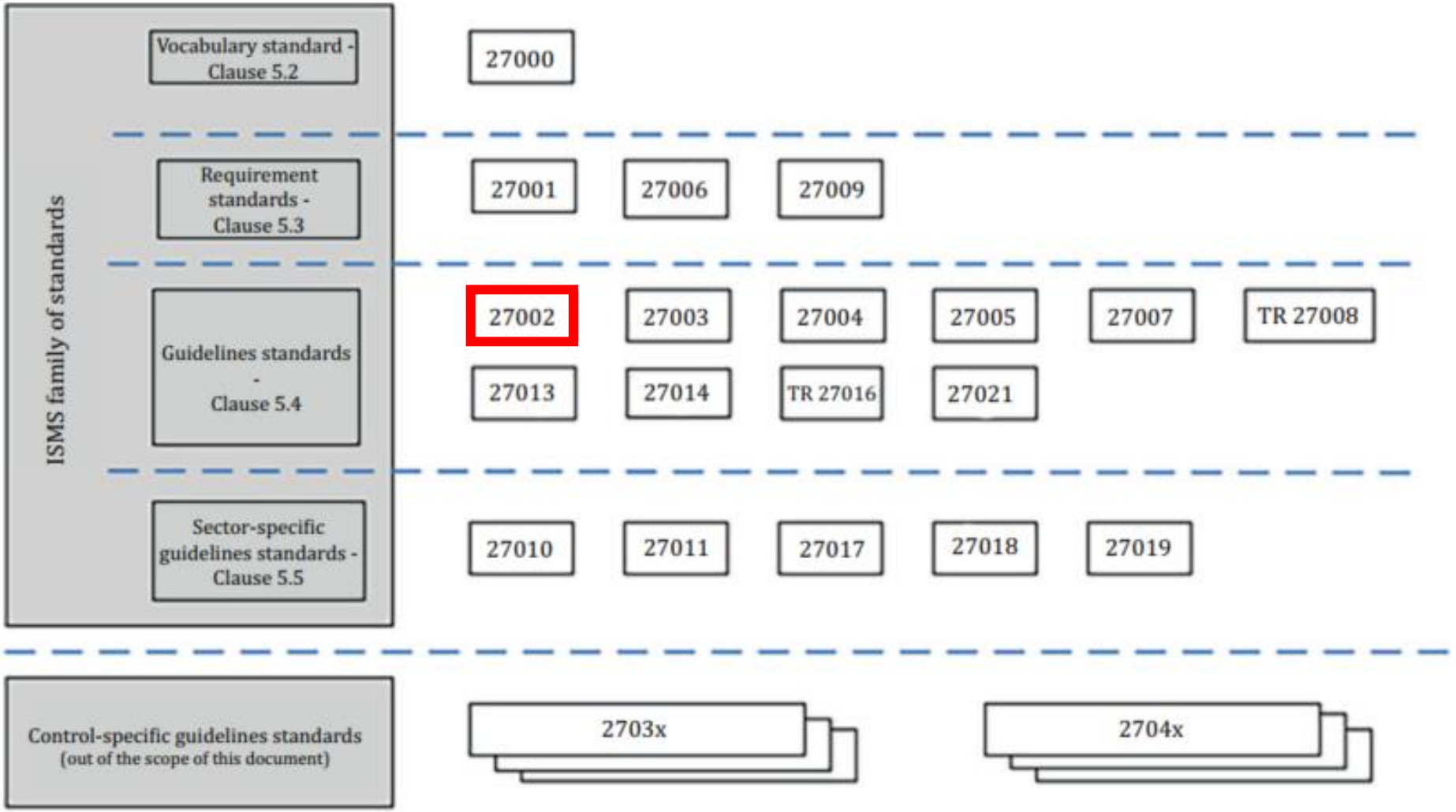
Breve storia della norma



UNI UN MONDO FATTO BENE

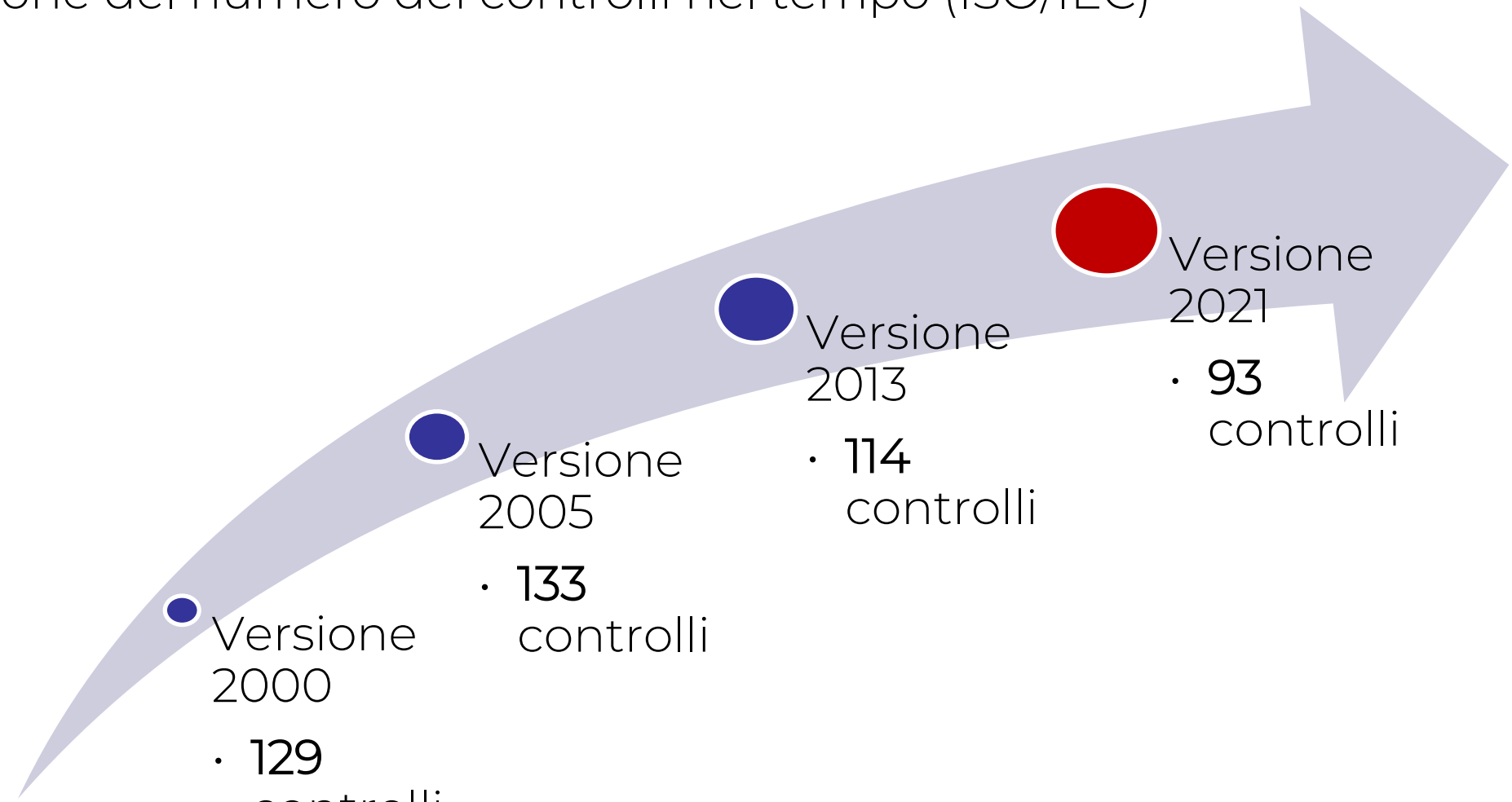
UNITRAIN Conoscere e applicare gli standard

Breve storia della norma



Breve storia della norma

Evoluzione del numero dei controlli nel tempo (ISO/IEC)



Breve storia della norma

Section number of 1998 edition	
	Introduction
1	General
1.1	Scope
1.2	Definitions
2	Information security management system requirements
2.1	General
2.2	Establishing a management framework
2.3	Implementation
2.4	Documentation
2.5	Document control
2.6	Records
3	Detailed controls
3.1	Information security policy
3.2	Security organization
3.3	Assets classification and control
3.4	Personnel security
3.5	Physical and environmental security
3.6	Computer and network management
3.7	System access control
3.8	Systems development and maintenance
3.9	Business continuity planning
3.10	Compliance

L'intenzione originale della norma era di avere un **catalogo esaustivo di controlli** da utilizzare come riferimento per poter verificare di non essersi "dimenticati" nulla di importante.

Lo "statement of applicability", collante principale con la ISO/IEC 27001, nasceva in questo contesto per formalizzare questo ragionamento e dichiarare cosa veniva applicato e cosa no, tenendo traccia delle motivazioni inerenti.

Breve storia della norma

Versione del 2013

Agenda

- Breve storia della norma
- Problemi principali della versione del 2013
- Nuova struttura della norma
- Temi, attributi e loro impiego
- Cambiamenti ai controlli
- Conseguenze dei cambiamenti
- Allineamento atteso con la UNI CEI EN ISO/IEC 27001
- Periodi e modalità di transizione alla nuova versione

Problemi principali della versione 2013

La versione del 2013 soffriva di una serie di problemi ben noti che hanno permesso ad altri schemi (NIST in primis) di prendere delle significative fette di mercato, tra cui:

- Durante i lavori di revisione si sono create notevoli confusioni che non hanno permesso un sostanziale miglioramento dalla versione del 2005
- Si sono volutamente esclusi controlli tecnologici non legati al "sistema di gestione" e si è mantenuto lo stesso approccio sul linguaggio utilizzato
- L'impostazione finale risulta poco immediata e oltremodo stratificata
- Non è stato compiuto un vero aggiornamento dei controlli
- La norma è disponibile solo a titolo oneroso, spesso viene letta solo come "Annex A"

Problemi principali della versione 2013

Oltre a quanto già citato, è degno di nota il fatto che diversi controlli erano ormai formulati in modo difficilmente comprensibile e spesso venivano male interpretati, soprattutto:

- 6.2.2 Teleworking
- 11.2.5 Removal of asset
- 12.5.1 Installation of software on operational systems
- 12.7.1 Information systems audit controls
- 17.1.2 Implementing information security continuity
- 18.1.5 Regulation of cryptographic controls

Agenda

- Breve storia della norma
- Problemi principali della versione del 2013
- Nuova struttura della norma
- Temi, attributi e loro impiego
- Cambiamenti ai controlli
- Conseguenze dei cambiamenti
- Allineamento atteso con la UNI CEI EN ISO/IEC 27001
- Periodi e modalità di transizione alla nuova versione

Nuova struttura della norma

Un aiuto al miglioramento della norma è arrivato dall'introduzione in ISO/IEC delle "design specifications" approvate nel 2017 che indicavano quanto segue:

Revised ISO/IEC 27002 should provide:

- Support of ISO/IEC 27001, but keep the option to be used standalone document
- A comprehensive list of controls
- Explanation of these controls
- Implementation guidance on these controls

Structure of document:

A new approach to the structure emerged from the study period; it can be described as the following:

- The set of controls will be organised according to 4 "Themes": Organisational; People; Physical; Technical
- Each control will have a list of Attributes
- Controls can be associated with one another and grouped by these defined Attributes

Definition:

- "Theme" is the categorisation of controls such that every control fits into just single theme title
- Theme title is a category of controls in which a group of controls can be organised with the same property defined by the theme
- An attribute is a piece of information used to describe a characteristic of a control based on a defined property. It will be used to tag controls in order to facilitate filtering for attributes.

Nuova struttura della norma

E' stato poi immediatamente evidente che il pur famoso titolo precedente

"**Code of practice for information security controls**"

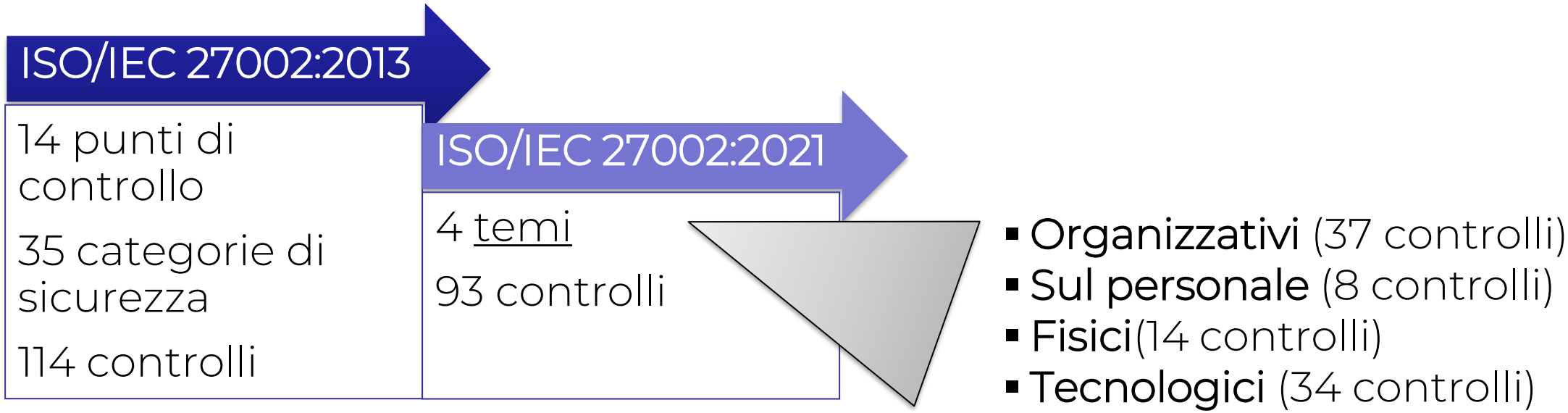
aveva ormai fatto abbondantemente il suo corso e si è quindi iniziato a modificarlo, per poi arrivare dopo alcuni passaggi a quello finale, decisamente più semplice e diretto:

"Information security controls"

Nota: nel mentre dal 2013 è anche variato il "nome" ufficiale di ISO/IEC JTC 1 SC 27, da "**Information technology — Security techniques**" a "**Information security, cybersecurity and privacy protection**"

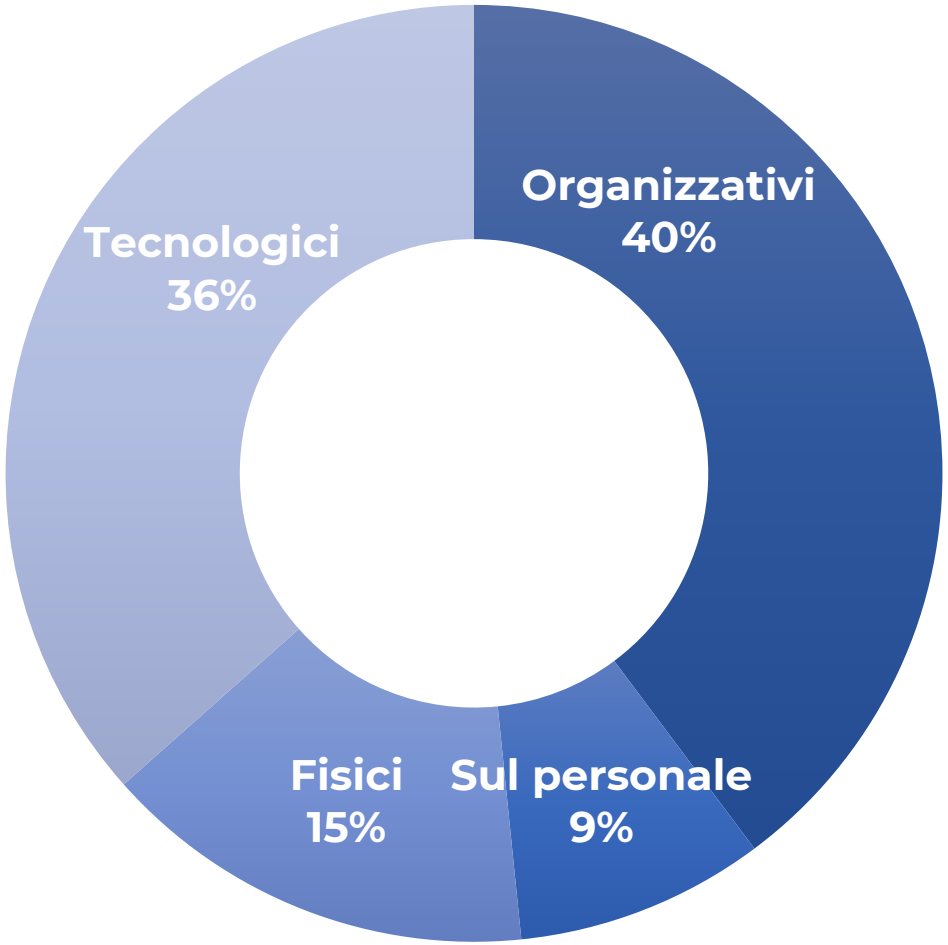
Nuova struttura della norma

La ISO/IEC 27002 è stata quindi oggetto di una ristrutturazione significativa, che ha portato a mantenere l'impostazione basata sui controlli ma modificandone diversi aspetti e riorganizzandoli completamente, cosa che avrà riverbero anche sulla ISO/IEC 27001:



Nuova struttura della norma

Distribuzione dei controlli



Nuova struttura della norma

I controlli, pur mantenendo la struttura cui siamo abituati nella ISO/IEC 27002 del 2013, hanno alcuni elementi di innovazione.

Nuova struttura della norma

Oltre ai controlli vi sono diversi altri capitoli nelle 160+ pagine della norma:

Premessa
0 Introduzione
1 Campo d'applicazione
2 Riferimenti normativi
3 Termini, definizioni e abbreviazioni
4 Struttura del documento
4.1 Punti
4.2 Temi ed attributi
4.3 Schema dei controlli
5 Controlli organizzativi
6 Controlli sul personale
7 Controlli fisici
8 Controlli tecnologici
Annex A – Usare gli attributi
Annex B – Corrispondenze con la ISO/IEC 27002:2013

Nuova struttura della norma

38 nuovi termini e definizioni degni di nota, reintrodotte rispetto alla 27000:

Asset: qualsiasi cosa cha ha valore per l'organizzazione

Controllo: misura che mantiene e/o modifica il rischio

Endpoint: dispositivo ICT di tipo hardware connesso in rete

Entità: elemento rilevante ai fini dell'operatività di un dominio che ha un'esistenza distinta riconoscibile

Incidente relativo alla sicurezza delle informazioni Uno o più eventi relativi alla sicurezza delle informazioni correlati e identificati che possono danneggiare gli asset di un'organizzazione o comprometterne l'operatività

Informazioni sensibili: informazioni che devono essere protette da indisponibilità, accesso non autorizzato, modifica o divulgazione pubblica a causa di potenziali effetti negativi su un individuo, su un'organizzazione, sulla sicurezza nazionale o sulla pubblica sicurezza

Nuova struttura della norma

Politica specifica [per argomento]: Intenti e indirizzi per un argomento o tema specifico, come formalmente espresso dal livello manageriale appropriato*

Regola: principio accettato o istruzione che afferma le aspettative dell'organizzazione su ciò che deve essere fatto, ciò che è consentito o non è consentito

* Nella versione del 2013 si potevano incontrare diversi controlli relativi, anche già nel loro "nome", al concetto di "policy", creando potenziale confusione. Per questo motivo nella nuova versione la situazione è stata riprogettata e il controllo 5.1 introduce le "topic specific policy" riprese all'interno dei singoli controlli ove rilevante.

Agenda

- Breve storia della norma
- Problemi principali della versione del 2013
- Nuova struttura della norma
- Temi, attributi e loro impiego
- Cambiamenti ai controlli
- Conseguenze dei cambiamenti
- Allineamento atteso con la UNI CEI EN ISO/IEC 27001
- Periodi e modalità di transizione alla nuova versione

Temi, attributi e loro impiego

Nella nuova versione della norma, oltre ai 4 temi principali, sono presentati 5 attributi per i controlli:

Tipo
- Preventivo
- Detettivo
- Correttivo

Proprietà
- Riservatezza
- Integrità
- Disponibilità

Concetto
- Identifica
- Protegge
- Individua
- Risponde
- Ripristina

Dominio di sicurezza
- Governance ed ecosistema
- Protezione
- Difesa
- Resilienza

Capacità operativa
- Governance
- Gestione degli asset
- Protezione delle informazioni
- Sicurezza delle risorse umane
- Sicurezza fisica
- Sicurezza di sistemi e reti
- Sicurezza delle applicazioni
- Configurazione sicura
- Gestione di identità ed accessi
- Gestione di minacce e vulnerabilità
- Continuità
- Sicurezza nei rapport con i fornitori
- Legale e conformità
- Gestione degli eventi relative alla sicurezza delle informazioni
- Garanzie in tema di sicurezza delle informazioni

Temi, attributi e loro impiego

L'**annex A** riprende il concetto degli attributi introdotto nel capitolo 4.2, illustrando come i 5 attributi definiti nella norma possono essere utilizzati , riportando:

1) una matrice completa di controlli ed attributi
2) una matrice filtrata (vista) per tutti i controlli con l'attributo #Corrective

Inoltre si suggerisce un approccio per definire attributi specifici aggiuntivi ai controlli, con l'esempio di 9 possibili eventi (minacce) da associare ai controlli. Altri esempi suggeriti sono:

- maturità
- priorità
- stato di implementazione
- aree organizzative
- asset
- service lifecycle

... ulteriori informazioni in arrivo nella ISO/IEC 27028 ...

Agenda

- Breve storia della norma
- Problemi principali della versione del 2013
- Nuova struttura della norma
- Temi, attributi e loro impiego
- Cambiamenti ai controlli
- Conseguenze dei cambiamenti
- Allineamento atteso con la UNI CEI EN ISO/IEC 27001
- Periodi e modalità di transizione alla nuova versione

Cambiamenti ai controlli

Esempio

7.10 Storage media

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

Storage media should be managed through its lifecycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.

Purpose

To ensure only authorized disclosure, modification, removal or destruction of information stored on media.

Guidance

Removable media

The following guidelines for the management of removable media should be considered:

a) the organization should establish a topic-specific policy on the management of removable media and communicate such topic- specific policy to anyone who uses or handles removable media;

Cambiamenti ai controlli

Controlli aggiunti

- 5.7 Threat intelligence
- 5.23 Information security for use of cloud services
- 5.30 ICT readiness for business continuity
- 7.4 Physical security monitoring
- 8.9 Configuration management
- 8.10 Information deletion
- 8.11 Data masking
- 8.12 Data leakage prevention
- 8.16 Monitoring activities
- 8.23 Web filtering
- 8.28 Secure coding

Cambiamenti ai controlli

Nuovo controllo **5.7 Threat intelligence**

Information relating to information security threats should be collected and analysed to produce threat intelligence.

Elementi salienti:

- Informazioni sulle "emerging threats"
- Processo per raccogliere, analizzare e infine utilizzare tali informazioni
- Scambio di informazioni con altre organizzazione

Cambiamenti ai controlli

Nuovo controllo **5.23 Information security for use of cloud services**

Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.

Elementi salienti:

- Topic-specific policy per l'uso dei servizi in cloud
- Suddivisione di responsabilità
- Accordi con i cloud service provider

Cambiamenti ai controlli

Nuovo controllo **5.30 ICT readiness for business continuity**

ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

Elementi salienti:

- Business Impact Analysis (BIA) con RTO ed RPO
- ICT continuity plans
- Richiami alla famiglia 22301

Cambiamenti ai controlli

Nuovo controllo **7.4 Physical security monitoring**

Premises should be continuously monitored for unauthorized physical access.

Elementi salienti:

- CCTV
- Sensori di movimento
- Sensori di effrazione
- Gestione dell'allarmistica generata

Cambiamenti ai controlli

Nuovo controllo **8.9 Configuration management**

Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.

Elementi salienti:

- Hardening tramite l'uso di "standard template"
- Controllo di configurazione
- Monitoraggio delle configurazioni

Cambiamenti ai controlli

Nuovo controllo **8.10 Information deletion**

Information stored in information systems, devices or in any other storage media should be deleted when no longer required.

Elementi salienti:

- Innesco della cancellazione
- Modalità di cancellazione
- Cancellazione e cloud service provider

Cambiamenti ai controlli

Nuovo controllo **8.11 Data masking**

Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific, and business requirements, taking applicable legislation into consideration.

Elementi salienti:

- Tecniche per il mascheramento dei dati
- Gestione sicura del processo di mascheramento
- Richiamo a pseudonimizzazione e anonimizzazione dei dati personali

Cambiamenti ai controlli

Nuovo controllo **8.12 Data leakage prevention**

Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.

Elementi salienti:

- Richiami a classificazione e monitoraggio dei canali
- Uso di strumenti di tipo DLP
- Controllo sulle operazioni effettuabili sulle informazioni

Cambiamenti ai controlli

Nuovo controllo **8.16 Monitoring activities**

Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

Elementi salienti:

- Impostazione di baseline di "normalità" e verifica della situazione
- Tipologie di anomalie da considerare
- Strumenti di monitoraggio continuo

Cambiamenti ai controlli

Nuovo controllo **8.23 Web filtering**

Access to external websites should be managed to reduce exposure to malicious content.

Elementi salienti:

- Identificazione della navigazione lecita e illecita
- Tecniche per il filtraggio della navigazione web
- Formazione del personale

Cambiamenti ai controlli

Nuovo controllo **8.28 Secure coding**

Secure coding principles should be applied to software development

Elementi salienti:

- Processo complessivo di secure coding
- Attività prima della scrittura del codice
- Tecniche e modalità per la scrittura di codice sicuro
- Manutenzione del codice
- Gestione di elementi di terze parti

Cambiamenti ai controlli

Controlli rimossi

- 11.2.5 Removal of asset

Controlli uniti (principali)

- 5.1 Policies for information security (5.1.1, 5.1.2)
- 5.14 Information transfer (13.2.1, 13.2.2, 13.3.3)
- 5.17 Authentication information (9.2.4, 9.3.1, 9.4.3)
- 5.18 Access rights (9.2.2, 9.2.5, 9.2.6)
- 5.29 Information security during disruption (17.1.1, 17.1.2, 17.1.3)
- 7.10 Storage media (8.3.1, 8.3.2, 8.3.3)
- 8.15 Logging (12.4.1, 12.4.2, 12.4.3)
- 8.32 Change management (12.1.2, 14.2.2, 14.2.3, 14.2.4)

Cambiamenti ai controlli

Controlli rinominati

ISO/IEC 27002:2013	ISO/IEC 27002:2022
6.2.2 Teleworking	6.7 Remote working
9.2.1 User registration and de-registration	5.16 Identity management
9.2.3 Management of privileged access rights	8.2 Privileged access rights
9.4.2 Secure log-on procedures	8.5 Secure authentication
9.4.5 Access control to program source code	8.4 Access to source code
7.3.1 Termination or change of employment responsibilities	6.5 Responsibilities after termination or change of employment
11.1.1 Physical security perimeter	7.1 Physical security perimeters
11.2.6 Security of equipment and assets off-premises	7.9 Security of assets off-premises

Cambiamenti ai controlli

Controlli rinominati

ISO/IEC 27002:2013	ISO/IEC 27002:2022
11.2.9 Clear desk and clear screen policy	7.7 Clear desk and clear screen
12.2.1 Controls against malware	8.7 Protection against malware
12.7.1 Information systems audit controls	8.34 Protection of information systems during audit testing
13.1.1 Network controls	8.20 Networks security
13.1.3 Segregation in networks	8.22 Segregation of networks
14.2.1 Secure development policy	8.25 Secure development life cycle
14.2.5 Secure system engineering principles	8.27 Secure system architecture and engineering principles
14.3.1 Protection of test data	8.33 Test information

Cambiamenti ai controlli

Controlli rinominati

ISO/IEC 27002:2013	ISO/IEC 27002:2022
15.1.1 Information security policy for supplier relationships	5.19 Information security in supplier relationships
15.1.2 Addressing security within supplier agreements	5.20 Addressing information security within supplier agreements
15.1.3 Information and communication technology supply chain	5.21 Managing information security in the ICT supply chain
16.1.1 Responsibilities and procedures	5.24 Information security incident management planning and preparation
16.1.4 Assessment of and decision on information security events	5.25 Assessment and decision on information security events
17.2.1 Availability of information processing facilities	8.14 Redundancy of information processing facilities
18.1.4 Privacy and protection of personally identifiable information	5.34 Privacy and protection of PII

Cambiamenti ai controlli

Dall'aggregazione di molti controlli e dal relativo allungarsi del testo della sezione "Guidance" è nata l'esigenza di suddividerla per sotto-argomenti principali, ad esempio:

8.15 Logging ha una guidance articolata in:

- Generale
- Protezione dei log
- Analisi dei log
- 8.24 Use of cryptography ha una guidance articolata in:
- Generale
- Key management

Nota: la maggioranza dei controlli è priva di questa suddivisione

Cambiamenti ai controlli

Esistono tuttavia diverse novità anche nei contenuti dei controlli esistenti:

- ✓5.2 - Suggerimento di un responsabile unico per la sicurezza
- ✓5.12 - Esempio di schema di classificazione a 4 livelli
- ✓5.14 - Linee guida per modalità di trasferimento (elettronico, supporti fisici, verbale)
- ✓5.20 – Estensione di quanto includere negli accordi con terze parti
- ✓6.1 – Controlli compensativi in caso di impossibilità di screening
- ✓6.7 – Estensione delle misure da adottare per il lavoro da remoto
- ✓7.2 – Indirizzamento dedicato del tema della gestione dei visitatori
- ✓7.9 – Linee guida per dispositivi quali ATM, totem etc.
- ✓8.1 – Estensione delle misure da adottare per gli endpoint

Cambiamenti ai controlli

- ✓8.5 – Maggiore risalto alla MFA
- ✓8.7 – Estensione ed ammodernamento delle misure suggerite (v. protezione contro il ransomware)
- ✓8.8 – Ampliamento di dettaglio del processo di gestione delle vulnerabilità per gestirne il ciclo di vita dall'identificazione al rimedio
- ✓8.15 – Linee guida per l'analisi dei log
- ✓8.16 – Esempi di comportamenti anomali che dovrebbero essere individuati tramite il monitoraggio
- ✓8.24 – Sottolineatura sulla scelta degli algoritmi crittografici
- ✓8.26 – Estensione delle misure per la sicurezza delle applicazioni
- ✓8.27 – Strutturazione della progettazione anche con l'aggiunta del principio dello "zero trust"

Cambiamenti ai controlli

L'**annex B** sarà invece molto importante per la transizione dalla vecchia alla nuova versione della ISO/IEC 27002 in quanto riporta una mappatura diretta e una mappatura inversa tra i controlli delle due versioni.

ISO/IEC 27002 control identifier	ISO/IEC 27002:2013 control identifier	Control name
5.1	05.1.1, 05.1.2	Policies for information security
5.2	06.1.1	Information security roles and responsibilities

ISO/IEC 27002:2013 control identifier	ISO/IEC 27002 control identifier	Control name according to ISO/IEC 27002:2013
5		Information security policies
5.1		Management direction for information security
5.1.1	5.1	Policies for information security

Agenda

- Breve storia della norma
- Problemi principali della versione del 2013
- Nuova struttura della norma
- Temi, attributi e loro impiego
- Cambiamenti ai controlli
- Conseguenze dei cambiamenti
- Allineamento atteso con la UNI CEI EN ISO/IEC 27001
- Periodi e modalità di transizione alla nuova versione

Conseguenze dei cambiamenti

I principali benefici attesi da quanto introdotto nella nuova ISO/EC 27002, praticamente tutti applicabili anche alla ISO/IEC 27001, sono:

- ✓Migliorata comprensibilità e fruizione dei controlli
- ✓Più facile applicazione dei controlli in modo atomico
- ✓Più semplice mappatura anche con altri framework
- ✓Maggiore attinenza all'evoluzione tecnologica attuale
- ✓Più forti collegamenti con le altre linee guida a disposizione
- ✓Maggiore espandibilità

Conseguenze dei cambiamenti

Incidentalmente, esistono anche una serie di conseguenze di altro tipo causate dalla nuova versione della ISO/IEC 27002:

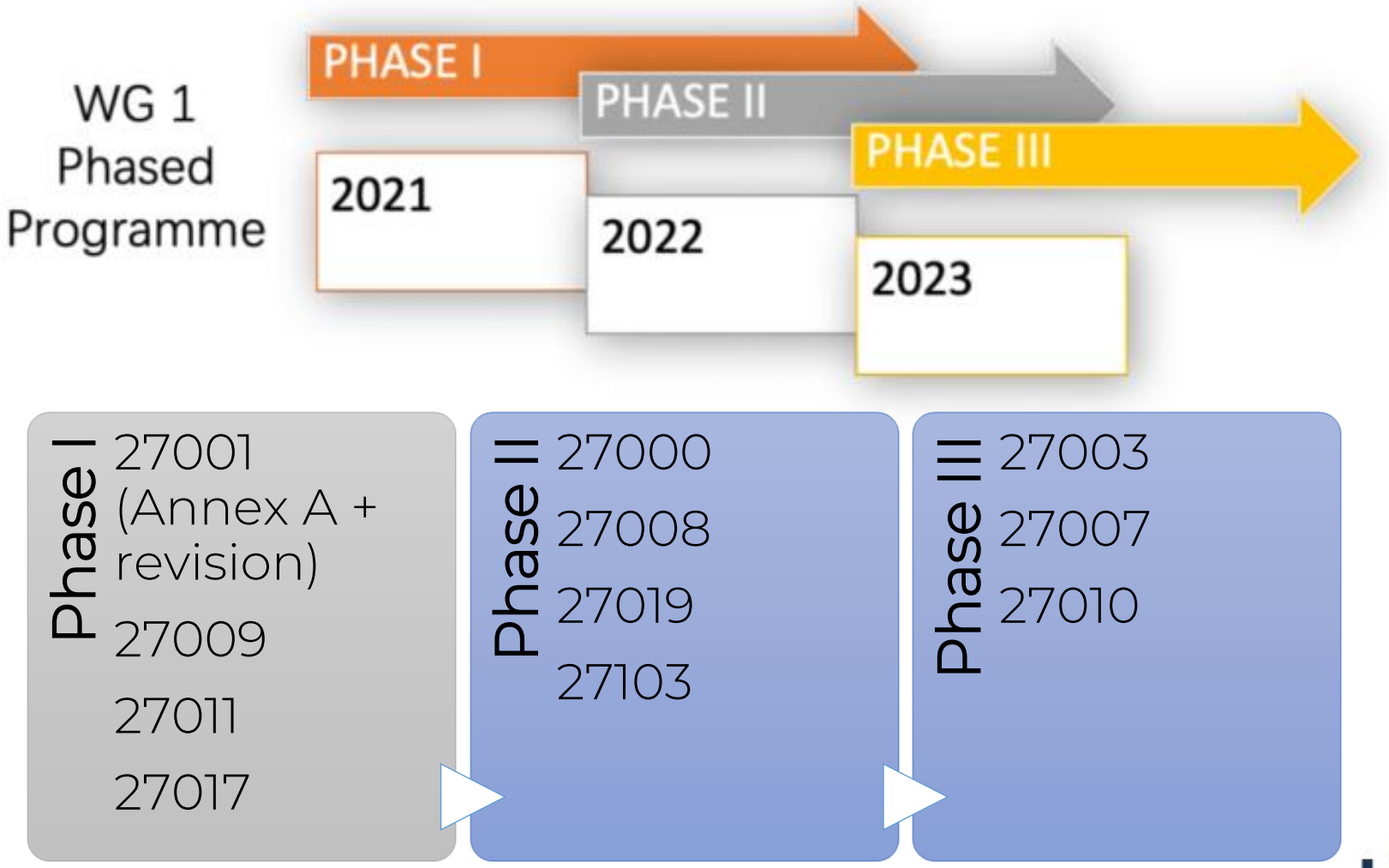
- La ISO/IEC 27001 fa in pratica riferimento normativo a una norma ritirata
- Le norme "*sector specific*" 27011, 27017, 27018, 27019 e 27701 devono essere ricostruite
- La norma ISO/IEC 27008 per l'audit dei controlli tecnici deve essere ricalibrata
- Le traduzioni in italiano delle norme (soprattutto la 27002) devono essere riviste e ripubblicate

Agenda

- Breve storia della norma
- Problemi principali della versione del 2013
- Nuova struttura della norma
- Temi, attributi e loro impiego
- Cambiamenti ai controlli
- Conseguenze dei cambiamenti
- **Allineamento atteso con la UNI CEI EN ISO/IEC 27001**
- Periodi e modalità di transizione alla nuova versione

Allineamento atteso con la ISO/IEC 27001

Il piano di ISO/IEC JTC 1 SC 27 (WG 1) è stato presentato nel seguente modo:



Allineamento atteso con la ISO/IEC 27001

L'idea di partenza era di pubblicare la ISO/IEC 27002 per coerenza assieme alla nuova ISO/IEC 27001 (su cui però non si è ancora di fatto iniziato a lavorare anche a causa della ritardata uscita della nuova HLS)

Feb 2022
- Pubblicazione ISO/IEC 27002:2022

Giu 2022
- Completamento dell'amendment alla ISO/IEC 27001

Nov 2022
- Pubblicazione della 3°ed. della ISO/IEC 27001 (amendment + corrigendum)
- Inizio lavori per minor revision ISO/IEC 27001

Allineamento atteso con la ISO/IEC 27001

Al momento attuale l'amendment alla ISO/IEC 27001 prevede:

- Modifica delle note (non normative) al punto 6.1.3
- Sostituzione integrale dell'annex A (in formato "landscape"!)

NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked.	*NOTE 1 Annex A contains a list of possible information security controls. Users of this International Standard are directed to Annex A to ensure that no necessary information security controls are overlooked.*
NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.	*NOTE 2 The information security controls listed in Annex A are not exhaustive and additional information security controls may be needed.*

Allineamento atteso con la ISO/IEC 27001

Il piano di ISO/IEC JTC 1 SC 27 (WG 5) relativamente alle ISO/IEC 27018 e, soprattutto ISO/IEC 27701 è invece il seguente:

Agenda

- Breve storia della norma
- Problemi principali della versione del 2013
- Nuova struttura della norma
- Temi, attributi e loro impiego
- Cambiamenti ai controlli
- Conseguenze dei cambiamenti
- Allineamento atteso con la UNI CEI EN ISO/IEC 27001
- Periodi e modalità di transizione alla nuova versione

Periodi e modalità di transizione alla nuova versione

A partire da novembre 2022, sarà concesso dagli enti di accreditamento un **periodo di transizione di 1 o più probabilmente 2 anni** per permettere l'adeguamento alla norma modificata, nonostante le differenze possano essere gestite in modo molto poco traumatico.

In questo periodo ci si potrà ricertificare utilizzando, a scelta, la seconda edizione o la terza edizione della ISO/IEC 27001.

Periodi e modalità di transizione alla nuova versione

La traduzione in italiano della voluminosa ISO/IEC 27002 è iniziata a inizio 2022, prima della sua pubblicazione, ed è a cura di un gruppo di esperti volontari che partecipano alle attività della CT 510.

La traduzione deve essere coerente con le altre effettuate in passato (27000, 27001, 27002, 29100) e con le altre norme di sistema di gestione (9001), il che pone alcuni vincoli terminologici.

Si prevede che i lavori termineranno verso luglio 2022.

Conclusioni

Cosa fare se si ha già un SGSI?

- Rimappare i controlli esistenti con la nuova ISO/IEC 27002
- Pianificare il prossimo risk assessment utilizzando i nuovi controlli

Cosa fare se si ha già un PIMS o una certificazione 27018?

- Rimappare i controlli dell'Annex A della ISO/IEC 27001 inerente

Da quando conviene utilizzare la nuova ISO/IEC 27002?

- Dipende da che tempi ha il vostro SGSI, se il rinnovo è dopo novembre conviene iniziare da subito con la nuova norma

Question time

UNI
UN MONDO FATTO BENE

UNITRAIN
Conoscere e applicare gli standard

Number 27002

twenty-seven thousand and two (twenty-seven thousand and second) **(X)(X)(V)MMII**

..--- --... ----- ----- ..---

Mathematics

The divisors: 1, 2, 23, 46, 587, 1174, 13501, 27002
Number of divisors: 8 **It's not a prime number.**
Sum of divisors: 42336

27002
27002

Languages

Spanish	veintisiete mil dos
German	siebenundzwanzigtausendzwei
French	vingt-sept mille deux
Portuguese	vinte e sete mil e dois
Chinese	二万七千零二

Informatics

Binary	110100101111010
Ternary	1101001002
Octal	64572
Hexadecimal	697A
BASE64	MjcwMDI=

Classical numerology

27002 = 2+7+0+0+2 = 1+1 = **2**

UNITRAIN

Conoscere e applicare gli standard

– Via Sannio, 2 – 20137 Milano

02 70024379 - 228 formazione@uni.com www.uni.com