LA VALUTAZIONE DEI RISCHI INFORMATICI E LE MISURE DI SICUREZZA IN AZIENDA

LA CERTIFICAZIONE ISO 27001 COME STRUMENTO PER LA CONFORMITÀ LEGISLATIVA

EUGENIO RIZZI
PRODUCT DEVELOPER MANAGER ICT
BUREAU VERITAS ITALIA SPA

EUGENIO.RIZZI@IT.BUREAUVERITAS.COM

AGENDA

Introduzione

Informazioni e dati

Il nuovo Regolamento Europeo 2016/679 – le principali novità introdotte

La valutazione del Rischio e il suo trattamento

Il Sistema di Gestione per la Sicurezza delle Informazioni

La ISO/IEC 27001:2013 – Sintesi dei principali requisiti

I benefici della Certificazione ISO/IEC 27001:2013

INTRODUZIONE

- ✓ Con i sempre crescenti processi trasformazione digitale all'interno di aziende e organizzazioni, anche seguito della definizione del Regolamento (UE) 2016/679, la **Sicurezza delle Informazioni e dei Dati** ha assunto un'importanza cruciale, in termini di Gestione del Rischio:
  - Accessi non autorizzati; attacchi virus e pirateria informatica; perdite di dati o violazione di dati personali (**Data Breach**)

- ✓ L'implementazione di una **strategia per la gestione del rischio** compensa l'investimento, tecnologico ma anche **organizzativo**, necessario per la prevenzione, trattamento dei rischi e loro contenimento.

- ✓ **Certificazione ISO/IEC 27001:2013 – Sistema di Gestione per la Sicurezza delle Informazioni**

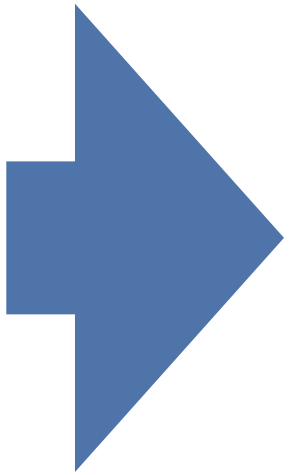
  È nell'interesse – non solo economico, ma anche istituzionale e di immagine – di ogni organizzazione dotarsi di un Sistema di Gestione per la Sicurezza delle Informazioni secondo la Norma ISO/IEC 27001:2013, con una certificazione da parte di un Ente Indipendente accreditato che ne attesti appropriatezza e conformità alla Norma stessa.

SCENARIO

Esigenze di conformità, l'evoluzione legislativa e l'aumento di incidenti hanno reso le Organizzazioni consapevoli della necessità di dotarsi di un approccio strutturato alla sicurezza delle informazioni

- Le Organizzazioni sono sempre più dipendenti dai loro asset informativi
- Gli utenti dell'informazione (interni ed esterni) ne chiedono sempre maggiore disponibilità
- Il numero di incidenti che minacciano la continuità dei servizi è in crescita

Una "breccia" di sicurezza può:



Distruggere l'immagine aziendale

Ridurre il valore del business

Compromettere futuri introiti

UN APPROCCIO

La resistenza culturale, che può nascere ed essere espressa dagli stakeholder/Users, in merito alla «limitazione d'accesso, profilazione e governo dei privilegi dell'accesso ai dati» **deve trasformarsi in una maggiore consapevolezza** della sicurezza e tutela del proprio operato, della propria professionalità (devo poter fare solo quello che serve per il mio lavoro).

«*Ogni utente e ogni applicazione deve avere il proprio personale e riservato codice di accesso ai sistemi informatici, il cui uso individuale sia garantito da appropriati controlli tecnologici di sicurezza*»

Le aziende non devono chiedersi **SE** saranno o meno obiettivo di un attacco informatico, ma **QUANDO** e attraverso **QUALI MODALITA' E CANALI**.

Le aziende sono già costantemente soggette ad attacchi più o meno gravi.

ALCUNI NUMERI (NUIX – “THE BLACK REPORT 2017”)

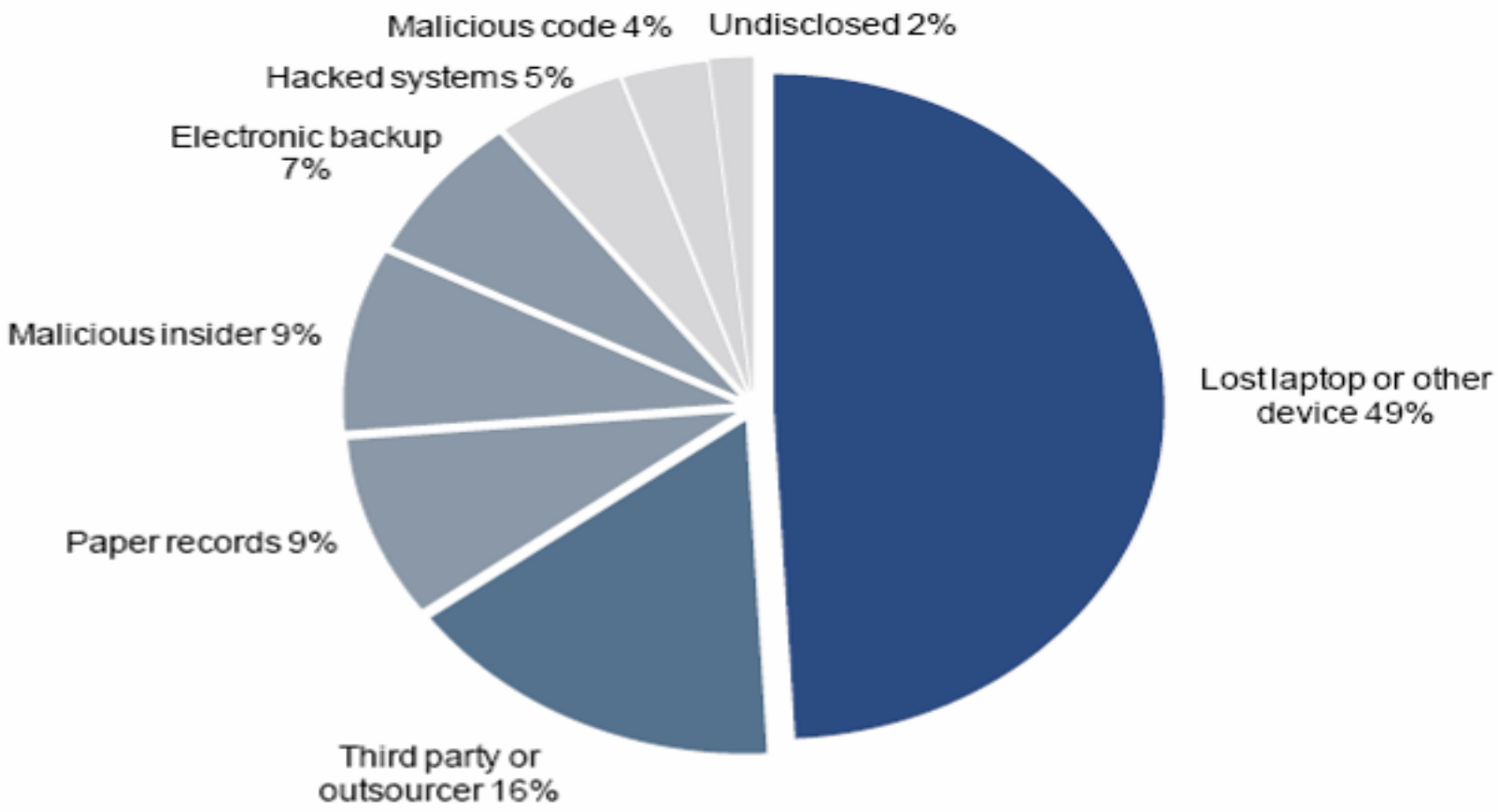
- L’81% degli hacker intervistati dichiarano che possono identificare le vulnerabilità e sottrarre i dati in meno di 12 ore
- L’84% usa tecniche di “social engineering” come parte della strategia di attacco (proviamo a fare in treno un Milano-Roma……)
- Il 52% ha ammesso che la consapevolezza (“awareness”) delle persone è la contromisura più efficace
- Il 100% degli hacker intervistati, esperti di penetration test e forensi concordano che una volta che si è riusciti ad accedere al dato/informazione, questo dato “*it’s gone… like gone gone*”

Timeline tipica di un attacco

MOTIVI DELLA PERDITA DI DATI

Laptop persi o rubati, ed altri dispositivi (es: pendrive) sono la maggiore fonte di perdita di informazioni.

(studio 2007: Il costo US della perdita dati – ricerca svolta da Ponemon Institute LLC)



TIPI DI DATI

- Progetti, dati economici, prodotti da brevettare, dati operativi
- Dati personali
  qualunque informazione relativa a persona fisica, identificata o identificabile
- Dati identificativi
  i dati personali che permettono l'identificazione diretta dell'interessato
- Dati giudiziari
- Ex «Dati Sensibili»
  i dati personali idonei a rivelare l'origine razziale ed etnica le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, dati personali idonei a rivelare lo stato di salute e la vita sessuale
- Dati relativi alla salute

  “I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute” (Art. 4.15, 9.1 e C.35 **GDPR**).

BUREAU VERITAS

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO – SINTESI

L'assemblea plenaria del Parlamento Europeo, dopo un iter legislativo durato 4 anni, in aprile 2016 ha approvato il Regolamento Europeo per il trattamento dei dati personali, che mira a garantire maggiori opportunità e tutele per cittadini e imprese ed a superare la normativa adottata quando i trattamenti di dati venivano effettuati prevalentemente su supporti cartacei

Il Regolamento si applica solo ai dati relativi alle persone fisiche. Non si applica alle persone giuridiche

Sanzioni (Maggio 2018)

- Sono previste sanzioni fino a 20 milioni di euro o fino al 4% del fatturato annuale mondiale di un'Organizzazione

Consenso

- Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale **manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile**, che i dati personali che lo riguardano siano oggetto di trattamento

Notificazione di eventuali violazioni (data breach) all'authority e agli interessati

- In caso di violazione dei dati personali in grado di provocare danni fisici, materiali o immateriali alle persone fisiche (perdita del controllo dei dati personali) il titolare del trattamento deve notificare la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza

BUREAU VERITAS

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO – SINTESI

Con la ***Privacy by Design*** il titolare mette in atto misure tecniche e organizzative adeguate, fin dalla fase della progettazione (es.: pseudonimizzazione) volte ad attuare in modo efficace i principi di protezione dei dati

Le misure devono tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, (come anche dei rischi del trattamento aventi probabilità e gravità diverse per diritti e libertà delle persone fisiche)

La ***Privacy by Default***, invece, prevede che la protezione del dato diventi l'impostazione predefinita per ogni trattamento assicurando che siano **trattati solo i dati personali necessari per ogni specifica finalità del trattamento** (l'obbligo vale per quantità dei dati personali raccolti, portata del trattamento, periodo di conservazione e accessibilità) e non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica

I Registri delle attività di trattamento devono essere tenuti in forma scritta (anche elettronica) dal titolare e, ove sia presente, dal responsabile, al fine di dimostrare la conformità al Regolamento; tale obbligo sussiste per le imprese o le organizzazioni:

- con più di 250 dipendenti;
- che effettuino un trattamento che presenta rischi per diritti e libertà dell'interessato, non sia occasionale e includa categorie particolari di dati sensibili

BUREAU VERITAS

LA SICUREZZA DELLE INFORMAZIONI E DEI DATI

- In passato l'importanza della Sicurezza delle Informazioni era riconosciuta limitatamente alla protezione dei dati contabili e finanziari.
- Oggi, la globalizzazione dei mercati e il libero commercio hanno aumentato la sensibilità rispetto alla Sicurezza delle Informazioni, anche da parte delle legislazioni nazionali.
- Particolari stimoli alla gestione delle Informazioni come "beni da proteggere" sono derivati, inoltre, da fattori quali la responsabilità legale (**Privacy, D.Lgs. 231/01**), la salvaguardia dell'immagine e, non ultimo, lo sviluppo delle tecnologie informatiche.
- Il numero di virus, attacchi e intrusioni cui si deve far fronte quotidianamente testimonia l'importanza di salvaguardare anche le Informazioni gestite dai propri Sistemi Informativi.

BUREAU VERITAS

L’INFORMAZIONE COME “ASSET”

L’Informazione:

‘’Un asset che, come altri importanti asset aziendali, è essenziale per il business di un’Organizzazione e di conseguenza deve essere adeguatamente protetto’’

Definizione di “Asset”:

“qualunque entità abbia valore per una Organizzazione”

INFORMATION SECURITY NON VUOLE DIRE SOLO “IT SECURITY”

L’Informazione deve essere protetta lungo tutto il suo ciclo di vita:

- Creazione
- Archiviazione
- Elaborazione
- Distribuzione

L’Informazione deve essere protetta indipendentemente dal suo formato o media

Bisogna proteggere anche il “contenitore dell’informazione”: infrastrutture tecnologiche, infrastrutture… non solo IT

- Documenti cartacei (sulla scrivania, nel cestino, vicino alla fotocopiatrice)
- Comunicazioni verbali
- Conversazioni in luoghi pubblici
- Persone

BUREAU VERITAS

INFORMATION SECURITY

Information Security

"Mantenimento della riservatezza, integrità e disponibilità dell'informazione; in aggiunta, altre caratteristiche possono essere incluse, quali autenticità, non-ripudio ed affidabilità"

Riservatezza: Assicurare che l'Informazione sia accessibile solo a coloro che sono autorizzati. *Sez. 01 della ISO/IEC 27001*

Integrità: Salvaguardare l'accuratezza e la completezza dell'informazione e dei metodi di processo. *Sez. 01 della ISO/IEC 27001*

Disponibilità: Assicurare che gli utenti autorizzati abbiano accesso all'informazione e relativi asset quando richiesto. *Sez. 01 della ISO/IEC 27001*

INFORMATION SECURITY MANAGEMENT SYSTEM

Information Security Management System (ISMS)

La parte del Sistema di Gestione aziendale, basata su un approccio di rischio, volta a definire, implementare, gestire, monitorare, riesaminare, mantenere e migliorare l'information security

- E' un processo **gestionale** e non un processo tecnologico
- E' il frutto di una decisione strategica dell'organizzazione
  - Progettazione ed implementazione
    - Esigenze ed obiettivi
    - Requisiti di sicurezza
    - Processi coinvolti
    - Dimensioni e struttura dell'organizzazione
  - Commisurata alle "esigenze"

ISO/IEC 27001

Due norme strettamente correlate

- ISO/IEC 27001 è la norma che definisce i requisiti di un Sistema di Gestione per l'Information Security (ISMS).
- ISO/IEC 27002 (ex ISO/IEC 17799:2005 e 27001:2007) è la linea guida e può essere considerata come il catalogo delle buone prassi da seguire con riferimento alla norma.

ISO/IEC 27001

Specifica i requisiti per definire, implementare, gestire, monitorare, riesaminare, mantenere e migliorare un ISMS documentato

Sviluppato per:

- Assicurare un adeguato insieme di controlli di sicurezza per proteggere gli asset informativi
- Dare fiducia a clienti e parti interessate

BUREAU VERITAS

ISO/IEC 27002:2013 (ISO/IEC 27002:2007)

- Uno schema di riferimento per costruire un sistema di gestione basato sul rischio che possa ricevere una certificazione indipendente
- Una linea guida che promuove l'adozione di un sistema di gestione per l'Information Security personalizzabile, misurabile e ripetibile
- Definisce 114 controlli di sicurezza strutturati in 14 capitoli
- Fornisce guida sulle best practice per la gestione
- Definisce un set di obiettivi di controllo e di controlli
- Suggerisce indicazioni per l'implementazione

BUREAU VERITAS

ISO/IEC 27001 VERSIONE 2013

- **Due grandi influenze sulla revisione**
- **Il primo - Allineamento con l'allegato SL alla Parte 1 delle direttive ISO / IEC**

  a) ISO ha stabilito che tutti i nuovi sistemi e le revisioni su norme sui sistemi di gestione devono essere conformi alla struttura di alto livello e identico testo di base di cui all'allegato SL alla Parte 1 delle direttive ISO / IEC

  b) Per garantire che i requisiti del sistema di gestione che non sono disciplinano specifiche sono formulate in maniera identica in tutti gli standard del sistema di gestione

  c) Vantaggi organizzazioni che operano sistemi di gestione integrati (es. ISO 9001 e ISO 27001)

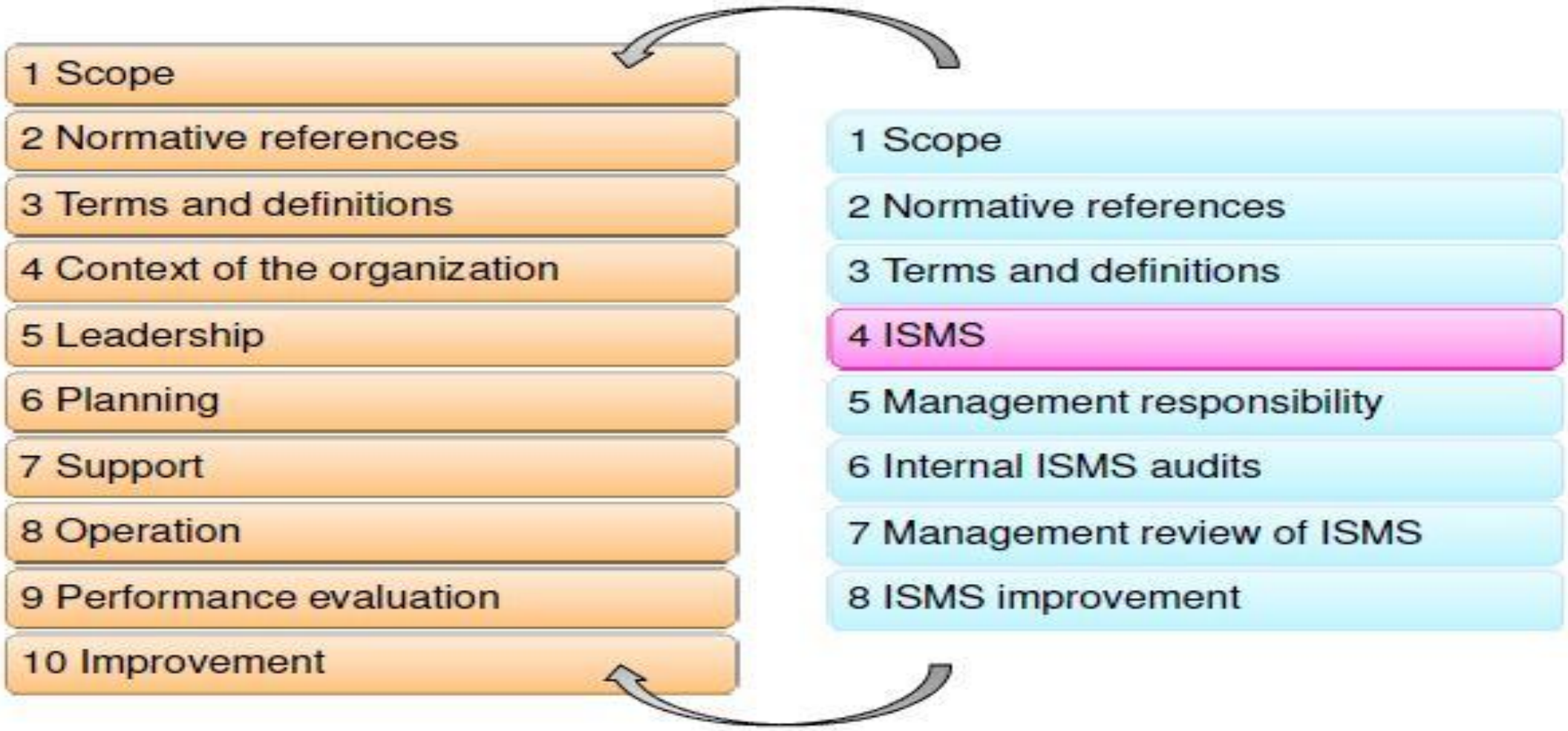
- **La seconda - Allineamento con ISO 31000 (Risk Management)**

  a) principi di valutazione del rischio di ISO 27001 allineate alle indicazioni fornite nella ISO 31000

  b) Vantaggi per organizzazioni che operano con sistemi di gestione integrati in quanto metodologia di valutazione del rischio stesso può essere utilizzato in vari standard

BUREAU VERITAS

DALL'ANNEX SL ALLA NUOVA ISO 27001:2013



LO STANDARD ISO/IEC 31000:2010

Gestione del rischio - Principi e linee guida:

- *“Tutte le attività dell’organizzazione comportano dei rischi”*

Fornisce principi e linee guida generali per la per la gestione del rischio in senso ampio e non esclusivamente di origine IT

Promuove la realizzazione di una struttura interna per la gestione dei rischi

Richiamata dalla 27001 per la *definizione del contesto* dell’Organizzazione:

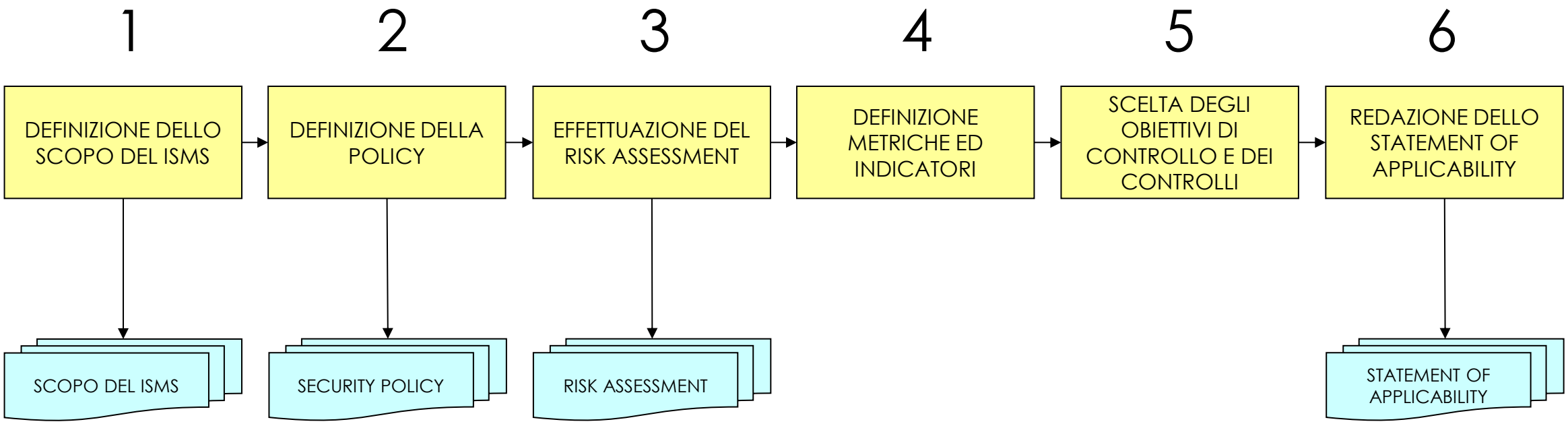
4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009[5].

FLUSSO DI PROCESSO PER L'INFORMATION SECURITY



IL RISK MANAGEMENT

Il rischio di un “incidente di information security” è funzione della probabilità che si manifesti una minaccia e del danno da essa causato

R = f (P,D)

Analisi dei rischi (metodologia)

Clause 6.1.2 Information Security risk assessment

- si allinea con i principi e le linee guida a ISO 31000
- identificazione dei beni, delle minacce e delle vulnerabilità non sono un pre-requisito per l'identificazione del rischio , ampliando così la scelta dei metodi di valutazione del rischio che l'Organizzazione può utilizzare
- Oltre a " criteri di accettazione del rischio " le Organizzazioni devono definire anche " i criteri per l'esecuzione di valutazione dei rischi per la sicurezza delle informazioni« (metodologia)
- La clausola si riferisce a "proprietari di rischio " piuttosto che " i proprietari di attività » , come nella versione precedente della norma
- **Proprietari del rischio**: titolari nella fase di approvazione piano di trattamento dei rischi e rischi residui

IL RISK ASSESSMENT

L’analisi iniziale dei rischi deve essere sviluppata considerando:

- le attuali condizioni del sistema
- la situazione a seguito dell’adozione delle contromisure ipotizzate

Il risultato della differenza è il “rischio residuo”, che la Direzione deve valutare ed accettare, per implementare l’ISMS

Il Risk Assessment è un processo iterativo, come previsto dal ciclo di Deming.

CONFORMITÀ ALLA ISO/IEC 27001

Tutti i punti di norma nella ISO/IEC 27001 sono obbligatori (Sez.4-10)

- Il Piano di trattamento del rischio è basato sul Risk assessment
- La documentazione supporta diversi requisiti
- Lo “Statement of Applicability” giustifica l’adozione dei “controlli” e segue e dà indicazione in merito a questi documenti ed argomenti:
  - L’Annex A fornisce una lista dei “controlli” obbligatori (al netto delle esclusioni giustificate)
  - L’escludibilità sui punti di controllo è ammessa ma deve essere fornita una valida motivazione per l’esclusione di un controllo
  - I controlli individuati devono essere documentati
  - Sostituisce a tutti gli effetti il Manuale Qualità della 9001 (non obbligatorio secondo la 27001).

La certificazione richiede che tutti i requisiti siano implementati

BUREAU VERITAS

4 CONTESTO DELL'ORGANIZZAZIONE

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 ritenuti "impliciti"):

- Contesto interno ed esterno
- Interfacce ed interdipendenze tra l'Organizzazione ed altre organizzazioni

Attuazione del ISMS ("*establish, implement, maintain and continually improve…*")

5 LEADERSHIP

Introdotta la “Leadership” al posto del “Impegno della Direzione”:

- Assicurare le risorse necessarie
- Integrare ISMS nell’Organizzazione
- Supportare il personale interno
- Definire gli obiettivi

Definizione della politica di sicurezza delle informazioni

- Deve contenere gli obiettivi
- Sia comunicata e resa disponibile
- Promuova il miglioramento continuo

Definire ruoli e responsabilità

Informazioni documentate:

- Information security policy

6 PIANIFICAZIONE

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

Identificazione, analisi, valutazione e trattamento del rischio sono nel planning perché contribuiscono alla pianificazione del sistema di gestione per la sicurezza delle informazioni

Si chiede di identificare i “risk owner", (“*person or entity with the accountability and authority to manage a risk*”)

7 SUPPORTO

Riguarda le risorse, le risorse umane, la comunicazione e le informazioni documentate.

Maggiore rilievo alla preparazione ed 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” ma non cambiano le modalità di gestione dei documenti

8 ATTIVITÀ OPERATIVE

Si richiama il punto 6 per la pianificazione, implementazione e controllo dei processi necessari al raggiungimento degli obiettivi di sicurezza (6.1 e 6.2)

Si richiama il punto 6 *(ensure, apply)* per l'attuazione *(perform)*

Riferimenti al controllo dei cambiamenti *(changes)* ed ai processi in outsourcing

Trattamento del rischio *(implement)*

9 VALUTAZIONE DELLE PRESTAZIONI

La valutazione delle performance specifica ora maggiori elementi, riferendosi ai controlli ed ai processi *(what, how, when, who)*

Introdotta la richiesta di valutare il raggiungimento degli obiettivi di sicurezza nel riesame di Direzione

10 MIGLIORAMENTO

Non Conformità e azioni correttive

Miglioramento continuo

Eliminate le azioni preventive (da vedere come caso particolare di trattamento dei rischi)

INFORMAZIONI DOCUMENTATE

Clause	Documented information
4.3	Scopo del ISMS
5.2	Information security policy
6.1.2	Processo di “Information security risk assessment”
6.1.3	Processo di “Information security risk treatment”
6.2	Statement of Applicability (SOA)
7.5.1 b)	Informazioni documentate sono stabilite dall’Organizzazione come necessarie per l’efficacia del ISMS
8.1	Pianificazione e controllo operativo
8.2	Risultati of the information security risk assessments
8.3	Risultati of the information security risk treatment

BUREAU VERITAS

INFORMAZIONI DOCUMENTATE

Clause	Documented information
9.1	Evidenza del risultato del monitoraggio e delle musrazioni (metriche)
9.2 g)	Evidenza della pianificazione degli audit e dell'esecuzione dello stesso
9.3	Evidenza dei risultati del riesame della direzione
10.1 f)	Evidenza delle cause della NC e delle azioni prese.
10.1 g)	Evidenza dei risultati delle AC.

ESEMPI DI POLICY / PROCEDURE OPERATIVE

Gestione della Security Policy

Uso accettabile degli asset

Identificazione e manipolazione di informazioni

Job description relative alla Information Security

Gestione delle procedure operative

Gestione di media rimovibili

Scambio di informazioni

Monitoraggio dell’uso dei sistemi

Politica di controllo degli accessi

Registrazione degli utenti

Scrivania pulita

Accesso a sistemi operativi

Crittografia

Installazione di software in sistemi operativi

Change Control-Change management

Redazione e gestione dei piani di continuità aziendale

Identificazione della legislazione applicabile

ESEMPI DI EVENTUALI PROCEDURE AGGIUNTIVE

Gestione dei backup

Verifica dello stato della sicurezza

Business Continuity

Incident Handling

Disaster Recovery

Antivirus

Network Security

Configurazione dei firewall

Information Security su media non elettronici

ISO/IEC 27001:2013 ANNEX A

- Riepiloga i controlli per contrastare il rischio
- Ristrutturazione in clauses (aree), control categories (obiettivi) e controls (controlli)
- Passaggio da 133 controlli a 114 aggregando diversi controlli tecnici
- Aggiunta di controlli su *sviluppo sicuro, testing, supply chain e project management*
- Revisione della terminologia e adattamento alle nuove tecnologie

LA STRUTTURA DELL'ANNEX A

Clause: definisce il controllo di sicurezza (area)

Control category: categoria principale contenente e **Control objective:** cosa si vuole raggiungere

Control : definisce il controllo nello specifico ("*measure that is modifying risk*")

A.5	POLITICA PER LA SICUREZZA DELL'INFORMAZIONE
A.5.1	ORIENTAMENTO DELLA DIREZIONE PER LA SICUREZZA DELL'INFORMAZIONE [Obiettivo: fornire gli orientamenti della Direzione e il necessario supporto per la sicurezza delle informazioni in accordo ai requisiti per le attivita' svolte e le leggi e i regolamenti rilevanti]
A.5.1.1	Il documento sulla politica e'approvato dalla Direzione, pubblicato, comunicato a tutto il personale e alle parti esterne interessate?
A.5.1.2	Il documento sulla politica e' oggetto di revisione ad intervalli pianificati o in caso di cambiamenti significativi per assicurare che sia appropriato, adeguato ed efficace?

BUREAU VERITAS

GLI AMBITI DI CONTROLLO ISO 27001 (ANNEX A)

A.5 – POLITICA PER LA SICUREZZA DELL'INFORMAZIONE
A.6 - ORGANIZZAZIONE DELLA SICUREZZA DELL'INFORMAZIONE
A.7 - RISORSE UMANE E SICUREZZA DELL' INFORMAZIONE
A.8 – GESTIONE DEGLI ASSET
A.9 - CONTROLLO DEGLI ACCESSI
A.10 - CRITTOGRAFIA
A.11 – SICUREZZA DELL' INFORMAZIONE FISICA E AMBIENTALE
A.12 – SICUREZZA DELLE OPERAZIONI
A.13 – SICUREZZA DELLE COMUNICAZIONI
A.14 - ACQUISTO, SVILUPPO E MANUTENZIONE DEI SISTEMI
A.15 – RAPPORTI CON I FORNITORI
A.16 - GESTIONE DEGLI INCIDENTI DI SICUREZZA DELL'INFORMAZIONE
A.17 - ASPETTI DI SICUREZZA DELL'INFORMAZIONE SULLA GESTIONE DELLA CONTINUITA' AZIENDALE
A.18 – CONFORMITA'

BUREAU VERITAS

I VANTAGGI NELL'ADOZIONE DI UN SISTEMA DI GESTIONE CERTIFICATO ISO/IEC 27001:2013

- ✓ **Strumento a supporto** per l'organizzazione e controllo delle attività e dei processi di trattamento dei dati
- ✓ Sviluppo di un **approccio razionale alla Sicurezza delle Informazioni**, tramite un'attenzione focalizzata alle vulnerabilità ed alla prevenzione degli incidenti (Data Breach)
- ✓ **Misurabilità dell'efficacia**: relazione tra i controlli selezionati e i risultati del processo di valutazione e di trattamento del rischio
- ✓ Valorizzazione e **protezione degli asset informativi** (Dati), in termini di *confidenzialità, integrità* e *disponibilità*
- ✓ Aumento della **consapevolezza dei rischi** e delle contromisure adottate o da adottare, anche tramite verifiche di Gap Analysis
- ✓ **Responsabilizzazione e formazione delle Risorse Umane**, anche tramite servizi di traininng specifici sulla Sicurezza delle Informazioni

BUREAU VERITAS

I SERVIZI INTEGRATIVI A COMPLEMENTO DELLA CERTIFICAZIONE ISO/IEC 27001:2013

- ✓ **Audit di Gap Analysis**

  per preparare al meglio si Sistema di Gestione per la Sicurezza delle Informazioni, è possibile eseguire una visita propedeutica di Gap Analysis per misurare il livello di implementazione del sistema rispetto ai requisiti richiesti dalla Norma di riferimento.

  E' una simulazione della visita di certificazione al fine di abbassare il rischio di fallimento del processo di certificazione iniziale.

- ✓ **Training specifico sulla norma e/o per la qualifica dei Valutatori Interni del Sistema di Gestione**

  La competenza delle risorse dedicate al monitoraggio del Sistema di Gestione risulta fondamentale per mantenere ai più alti livelli la sua efficacia, tramite Auditor Interni qualificati a seguito di un corso specifico di 16 ore, con esame finale e Certificato di competenza.

  Anche la consapevolezza di tutto il personale coinvolto è uno degli aspetti più importanti contenuto nella Norma di riferimento: aumentare questa consapevolezza tramite training informativo specifico è quindi di primaria importanza.

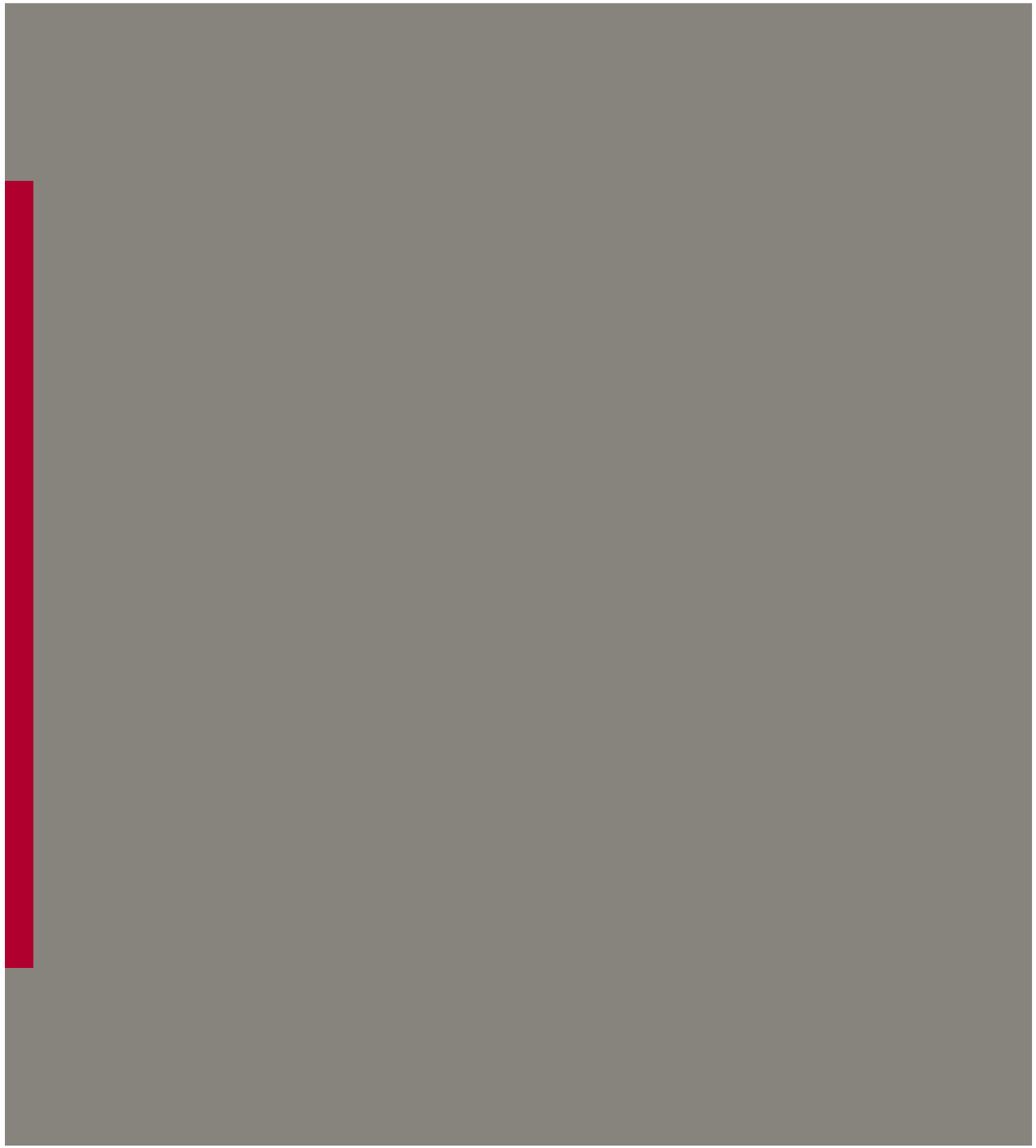
- ✓ **Audit sui Fornitori e Partner (Audit di II Parte)**

  Infine, quando nella nostra catena di fornitura sono presenti partner/fornitori critici per garantire la sicurezza delle nostre informazioni trasmesse a loro, è sempre possibile effettuare degli audit specifici su queste organizzazioni per valutare il grado di conformità alle politiche di sicurezza che gli chiediamo di rispettare (Audit di II Parte)

BUREAU VERITAS

Grazie

Domande?



Move Forward with Confidence