securitylab ADVISORY

aiti ASSOCIAZIONE INDUSTRIE TICINESI

Benvenuti!

aiti
ASSOCIAZIONE INDUSTRIE TICINESI

Relatori

Siro Migliavacca

General Manager Security Lab Advisory

Francesca Colombo

Legal Counsel & Advisor Security Lab Advisory

Alessandro Carniato

e-Learning Instructional Designer - Security Lab

securitylab ADVISORY

aiti ASSOCIAZIONE INDUSTRIE TICINESI

Obiettivi del sistema di Cyber Security G&C

I principali obiettivi del sistema di **Governance & Compliance** della **Cyber Security** sono:

- «prevenire»; quindi, **ridurre il più possibile il livello di rischio**
- «accorgersi»; quindi, **saper rilevare tempestivamente** le minacce in corso e la possibilità di essere sotto-attacco
- «saper reagire»; quindi, **rispondere al meglio in caso di incidente**
- **garantire il rispetto delle normative, regolamenti, contratti** in materia di sicurezza dei dati e dei servizi informativi.

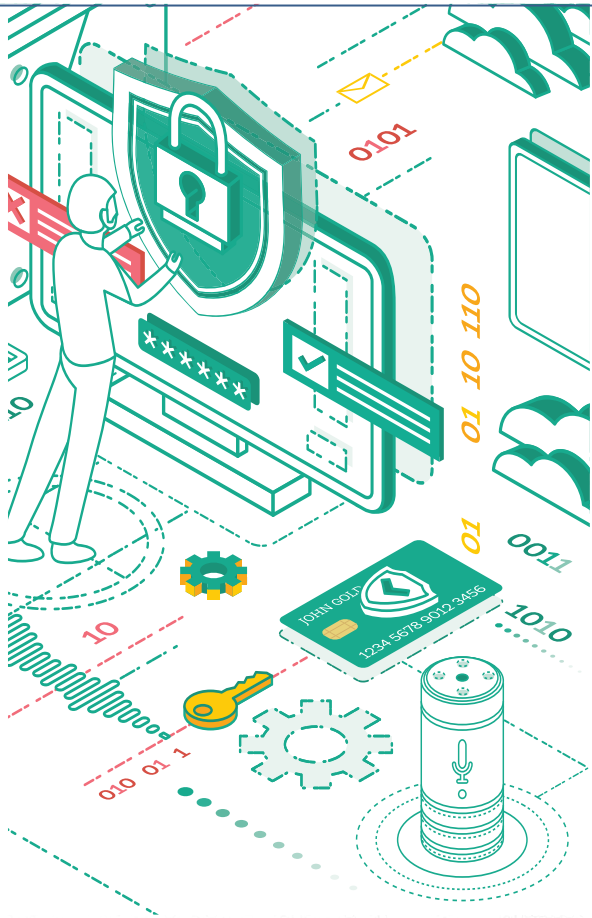
Obiettivi del webinar

Dare suggerimenti alle **Organizzazioni del Ticino** su come:

- predisporre / migliorare
- mantenere / far evolvere

il proprio **Sistema di**

Cyber Security Governance & Compliance



Contenuti del Webinar

- *Governance*: Elementi fondamentali della Governance della Cyber Security
- *Compliance*: Requisiti di Cyber Security richiesti da leggi e mercato
- *E-Learning* al servizio della Compliance: Esempi di Corsi interattivi LPD e GDPR
- *Percorso progettuale*: Costruire il proprio sistema di Cyber Security Governance
- *Domande e risposte*

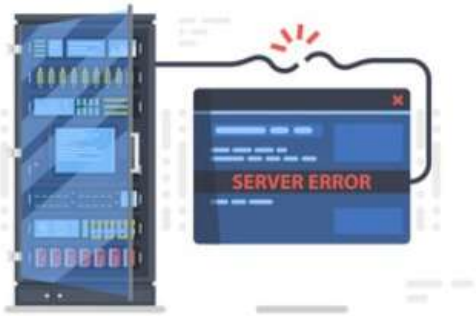
Contenuti del Webinar

- ***Governance*: Elementi fondamentali della Governance della Cyber Security**
  - Modelli di riferimento per la governance della cyber security
  - Metodologie di valutazione dei rischi cyber
  - Preparazione della risposta agli incidenti cyber
  - Evoluzione organizzativa dei servizi IT

Minacce alla Cyber Security

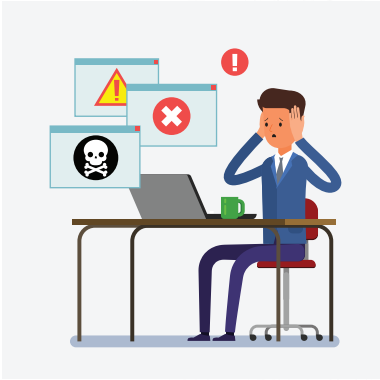
HACKING

FURTI, FRODI, ALTRI ILLECITI



MALFUNZIONAMENTO INFRASTRUTTURE / SOFTWARE

EVENTI AMBIENTALI



ERRORI UMANI

Ransomware attack 2020: Mattel e Campari

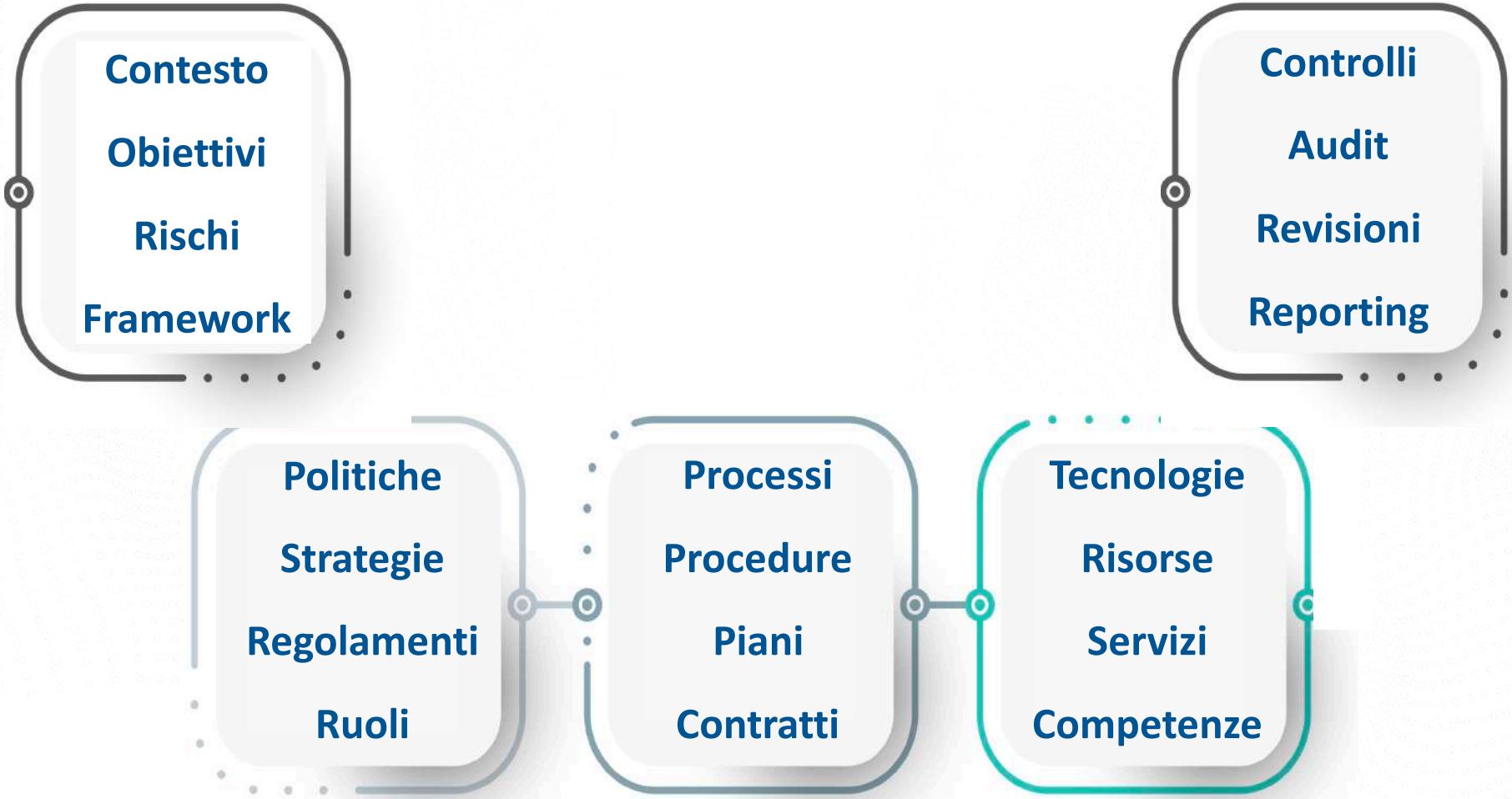
- Blocco di una parte dei sistemi/dati
- Nessuna esfiltrazione dati (indagine forense)

- Rilevazione dell'attacco
- Gestione della risposta
- Piani di disaster recovery (backup)

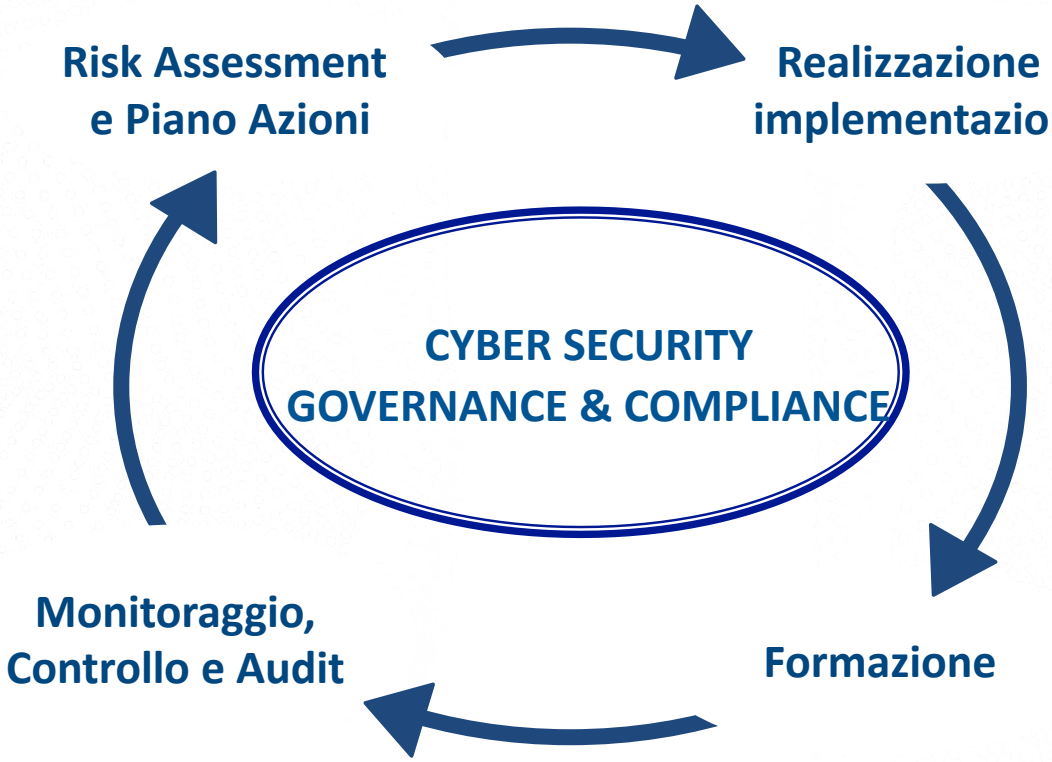
- Blocco di una parte dei sistemi/dati
- Esfiltrazione 2 TeraByte di dati confidenziali

- Rilevazione dell'attacco
- Gestione della risposta
- Piani di disaster recovery (backup)

Sistema di Cyber Security Governance & Compliance

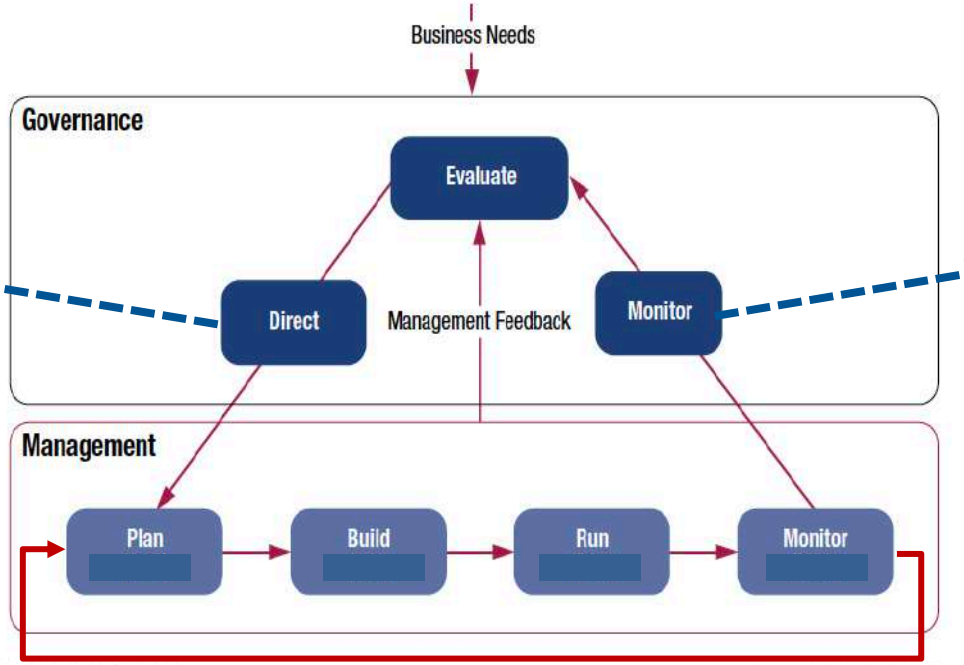


Cyber Security G&C process



- *Politiche*
- *Strategie*
- *Regolamenti*
- *Ruoli*
- *Processi*
- *Procedure*
- *Piani*
- *Contratti*
- *Tecnologie*
- *Risorse*
- *Servizi*
- *Competenze*

Governance & Management



- ✓ *Politiche*
- ✓ *Strategie*
- ✓ *Regolamenti*
- ✓ *Ruoli*

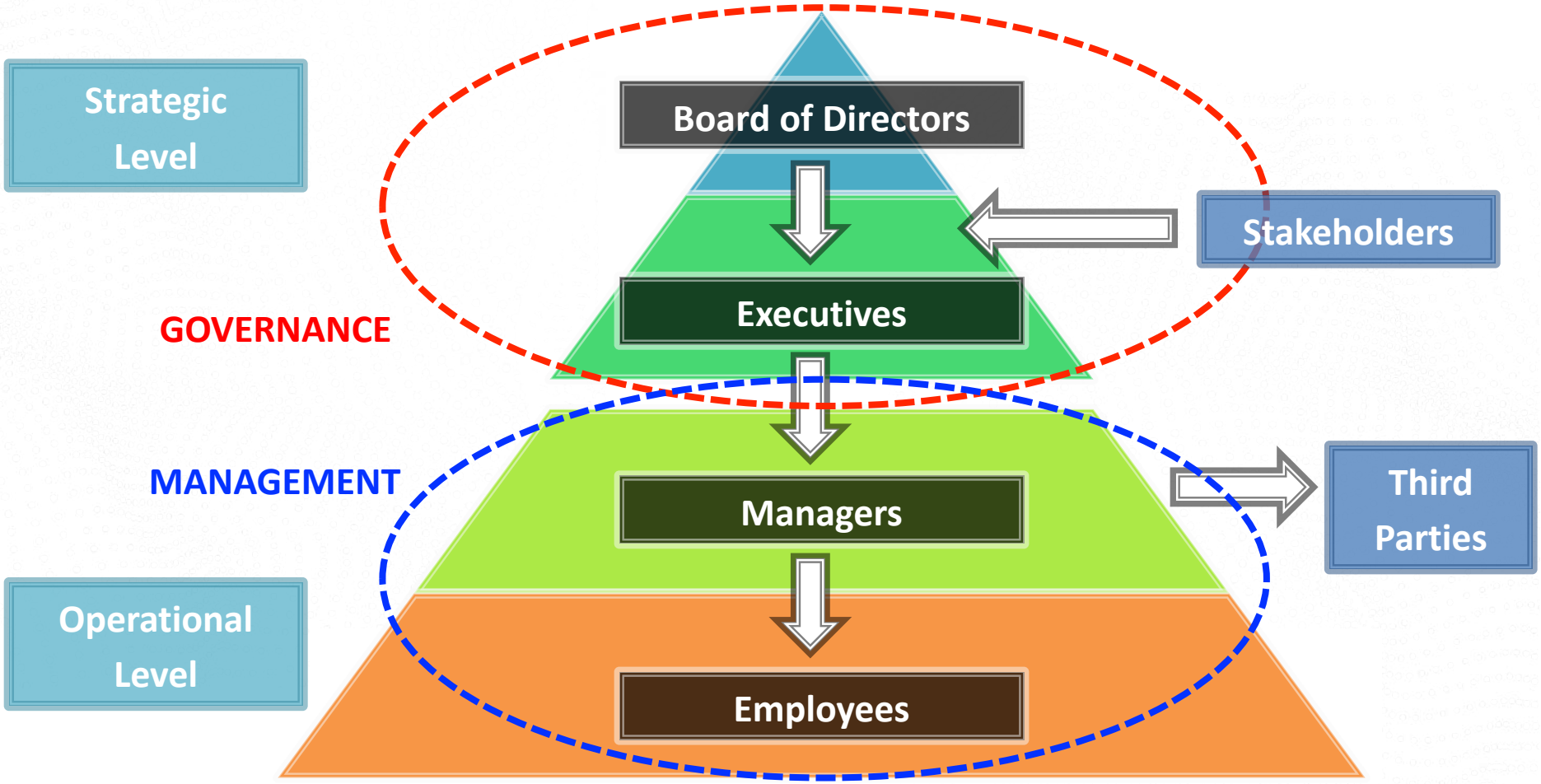
- ✓ *Controlli*
- ✓ *Audit*
- ✓ *Revisioni*
- ✓ *Reporting*

Processo ciclico di gestione della sicurezza a livello operativo

- ✓ *Processi*
- ✓ *Procedure*
- ✓ *Piani*
- ✓ *Contratti*
- ✓ *Tecnologie*
- ✓ *Risorse*
- ✓ *Servizi*
- ✓ *Competenze*

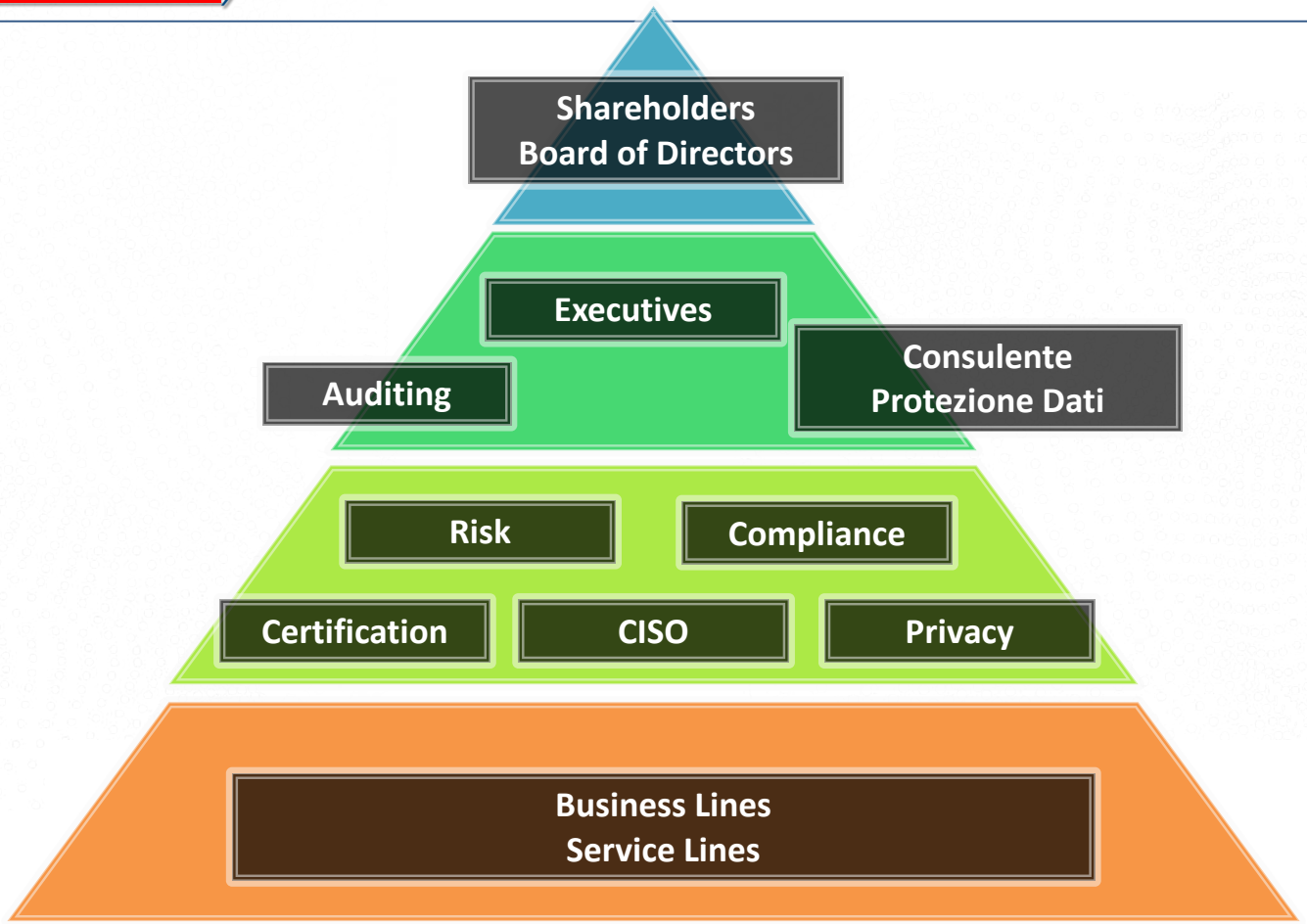
COBIT 5
Governance and Management Key Areas

Responsabilità di Governance & Management



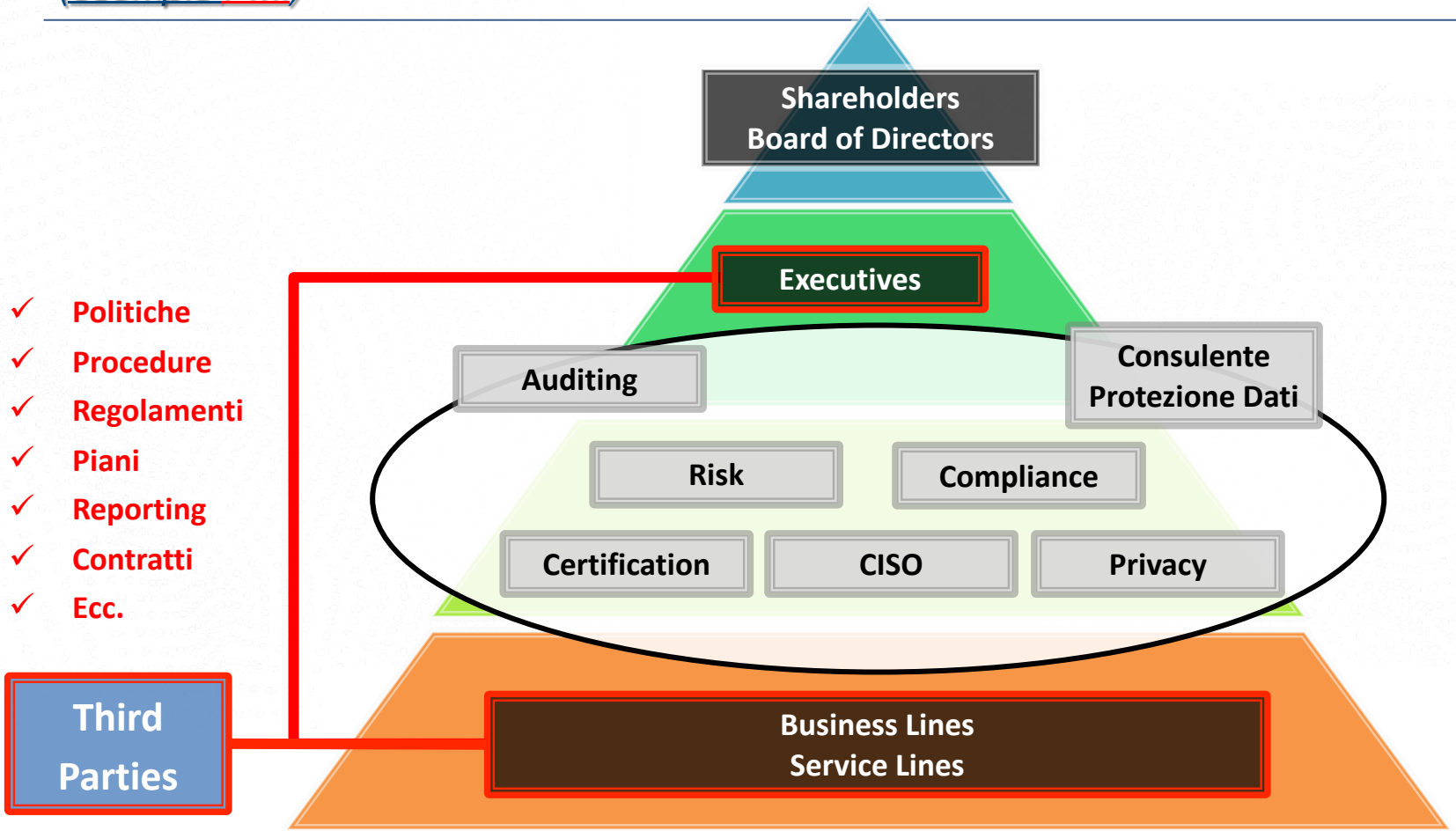
Ruoli del Sistema di Governance & Compliance

(esempio grande azienda)



Ruoli del Sistema di Governance & Compliance

(esempio PMI)



- ✓ Politiche
- ✓ Procedure
- ✓ Regolamenti
- ✓ Piani
- ✓ Reporting
- ✓ Contratti
- ✓ Ecc.

Chief information security officer (CISO) 1/2

CISO

Ha la responsabilità generale del sistema di Cyber Security.

Funge anche da funzione di «collegamento» tra la Direzione Aziendale (livello strategico) e i Responsabili delle linee di business e dei processi/servizi aziendali (livello operativo).

La responsabilità «ultima» del Sistema Sicurezza è comunque della funzione a cui il CISO riporta; ad esempio: CEO, COO, Membro del Board, Comitato Sicurezza Informazioni.

Comitato Sicurezza Informazioni

Qualora costituito, il Comitato garantisce la supervisione del Sistema Sicurezza e che le buone pratiche vengano applicate in modo efficace e coerente in tutta l'azienda.

Rappresenta il «Comitato di Direzione» della Cyber Security.

Chief information security officer (CISO) 1/2

Il CISO:

- Gestisce il sistema di Cyber Security
- Realizza la strategia di sicurezza delle informazioni (definita dalla Direzione)
- Definisce e gestisce il piano di trattamento dei rischi (in accordo con il CRO/CEO)
- Delega compiti di gestione operativa della sicurezza ai responsabili aziendali
- Valuta le questioni chiave con il supervisore diretto e/o con il Comitato.

- deve avere una conoscenza accurata della visione strategica aziendale
- deve essere capace di tradurre gli obiettivi aziendali in requisiti di sicurezza delle informazioni
- deve avere buone doti comunicative e saper costruire relazioni efficaci con i leader aziendali.

Contenuti del Webinar

- ***Governance*: Elementi fondamentali della Governance della Cyber Security**
  - Modelli di riferimento per la governance della cyber security
  - Metodologie di valutazione dei rischi cyber
  - Preparazione della risposta agli incidenti cyber
  - Evoluzione organizzativa dei servizi IT

Obiettivi della gestione dei Rischi di CyberSecurity

Il principale obiettivo della **Cyber Security Governance&Compliance** è:

- **aumentare «il più possibile» il livello di sicurezza e, quindi, ridurre «il più possibile» il livello di rischio**

Cosa significa «ridurre il livello del rischio di sicurezza il più possibile»?

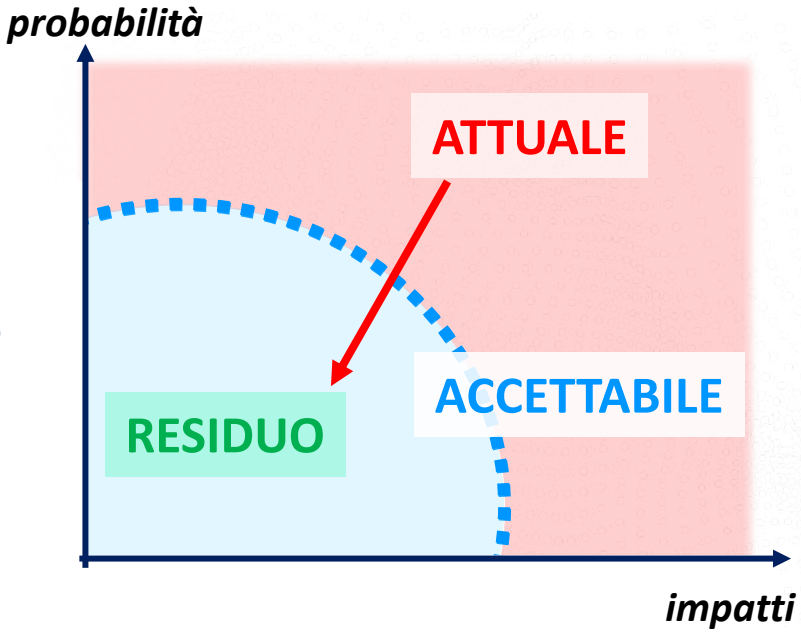
Poiché il Rischio non si può eliminare del tutto, bisogna mantenere nel tempo un livello di rischio «il più basso possibile» in coerenza con:

- la convenienza/opportunità per l'Organizzazione di investire in CyberSecurity
- la capacità di spesa/investimento in CyberSecurity da parte dell'Organizzazione.

La «Governance» deve definire il «Rischio Massimo Accettabile»

Cosa bisogna fare

1) Identificare i rischi
2) Valutare il livello di «**Rischio Attuale**»
3) Definire il valore del «**Rischio Massimo Accettabile**»
4) Investire nel sistema di Cyber Security Governance & Compliance in modo che il «Rischio Attuale» venga ridotto ad un valore di «**Rischio Residuo**» che sia inferiore al «Rischio Accettabile»
   (considerando le conseguenze di ogni intervento sul business e sull'operatività).



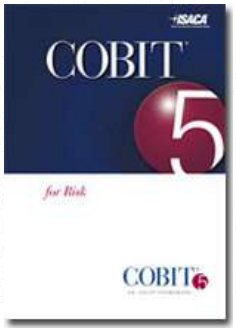
E, poiché il contesto e l'organizzazione cambiano nel tempo, questo processo deve essere ripetuto ciclicamente.

Metodologie di gestione del Rischio *(esempi)*

ERM-COSO

Enterprise Risk Management

International Organization for Standardization
ISO 31000
Risk-Management



Information Security Risk Management

ISO 27005

Processo di gestione del Rischio di Information Security

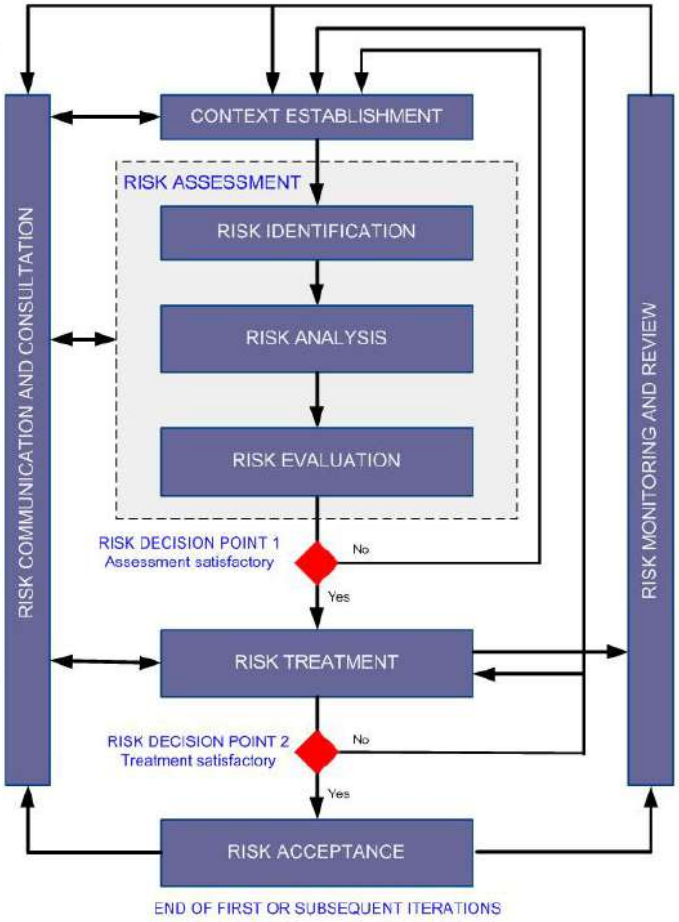


Illustration of an information security risk management process

(ISO 27005)

Valutazione «qualitativa» del Rischio

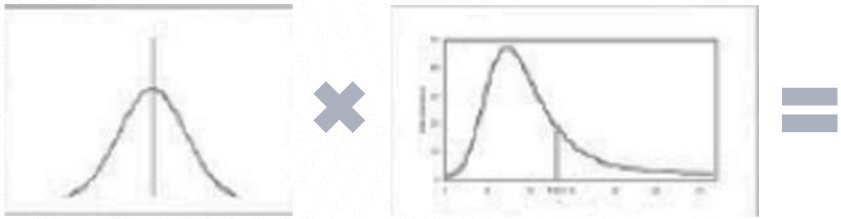
IMPATTO	MOLTO BASSO	BASSO	MEDIO	ALTO	MOLTO ALTO
MOLTO ALTO	5	10	15	20	25
ALTO	4	8	12	16	20
MEDIO	3	6	9	12	15
BASSO	2	4	6	8	10
MOLTO BASSO	1	2	3	4	5

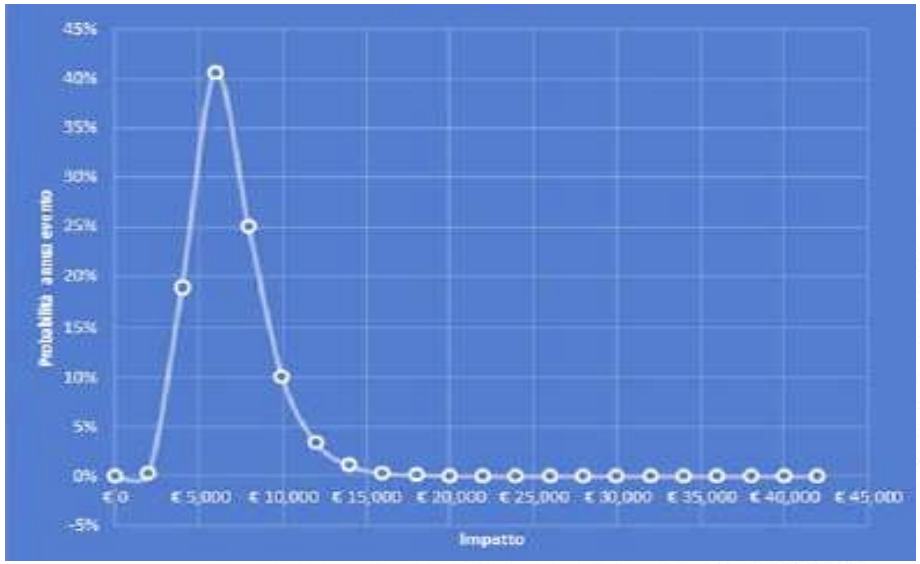
PROBABILITÀ

Valutazione quantitativa/probabilistica del Rischio

Rischio = "Frequenza probabile con cui si verifica una potenziale perdita futura"

PROBABILITÀ × **IMPATTO** = **RISCHIO**





Open FAIR™ Foundation

FAIR INSTITUTE

Factor Analysis of Information Risk

Contenuti del Webinar

- ***Governance*: Elementi fondamentali della Governance della Cyber Security**
  - Modelli di riferimento per la governance della cyber security
  - Metodologie di valutazione dei rischi cyber
  - Preparazione della risposta agli incidenti cyber
  - Evoluzione organizzativa dei servizi IT

Reagire in caso di Incidente

DETECT

- Tecnologie per la rilevazione degli attacchi e la loro analisi
- Processo di monitoring and detection

RESPOND

- Policy, processi e procedura di escalation per la Gestione Incidenti (specifici per Cyber Incident Response)
- Procedura Data Breach Notification
- Crisis Management Plan
- Competenze specialistiche (Cyber Team, DPO, ecc.)

RECOVER

- Strategie di Recovery
- Business Continuity Plan
- Disaster Recovery Plan

Aspetti principali della Governance dell'Incidente 1/2

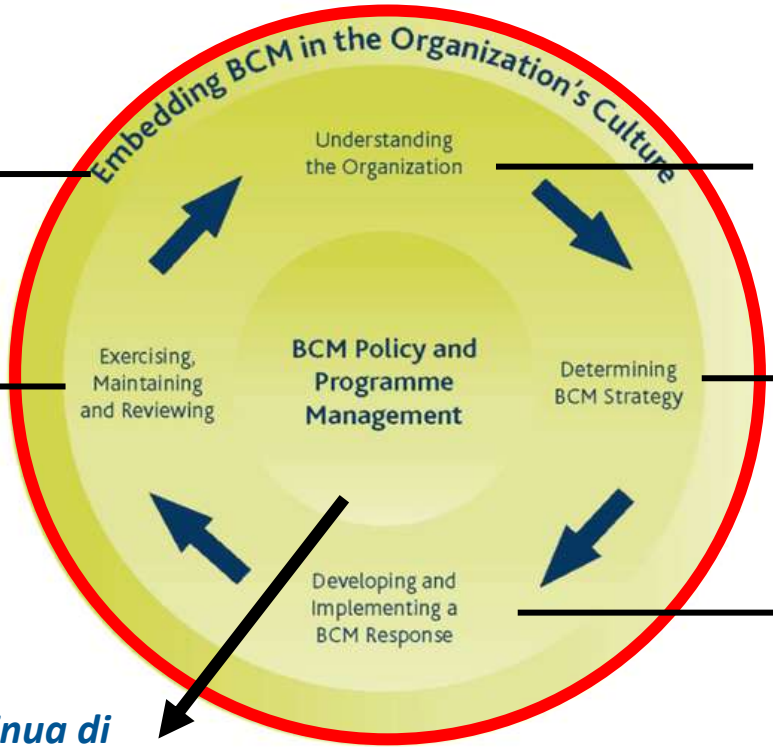
- Rispetto degli SLA contrattualizzati
- Classificazione, registrazione e database delle soluzioni/workaround
- Per diversi scenari di incidente/crisi, diversa gestione (e processo di escalation)
- Conservazione log, informazioni e prove
- Piano delle comunicazioni in emergenza
- Team specialistici di pronto intervento

Aspetti principali della Governance dell'Incidente 1/2

- Formazione delle persone coinvolte nella gestione degli incidenti/crisi
- Periodiche attività di test e simulazione per gravi incidenti/crisi
- Definizione dei tempi RTO e RPO per i processi/servizi aziendali critici
- Definizione delle strategie di recovery
- Definizione del processo di aggiornamento, manutenzione e controllo dei Piani di Crisis Management, Business Continuity, Disaster Recovery.

Gestione della Business Continuity

ISO 22301 Business Continuity Management



Attività periodiche (di solito annuali)

Formazione

Esercitazione

BIA / RISK

Strategie

BCP

Aggiornamento continuo

Attività continua di aggiornamento e Governance

(ISO 22301)

Contenuti del Webinar

- ***Governance*: Elementi fondamentali della Governance della Cyber Security**
  - Modelli di riferimento per la governance della cyber security
  - Metodologie di valutazione dei rischi cyber
  - Preparazione della risposta agli incidenti cyber
  - Evoluzione organizzativa dei servizi IT

Centralità dell'Area IT

La **principale area aziendale impegnata «in prima linea»** nelle attività operative rivolte alla gestione della Cyber Security è senz'altro l'**Area Informatica**.

- **Tecnologie e sistemi di sicurezza informatica**
- **Gestione dei processi/servizi IT**
- **Governo e controllo dei fornitori IT**

È opportuno che i processi di gestione dell'IT vengano rivisitati, al fine di tener conto, non solo degli aspetti funzionali e di performance dei servizi IT, ma anche degli aspetti di sicurezza che i processi/servizi IT sono in grado di garantire (riservatezza, integrità, disponibilità).

Revisione dei Processi IT in ottica di Sicurezza 1/2

I processi IT devono essere ottimizzati dal punto di vista della sicurezza.

Quante volte troviamo nelle aziende che:

ACCESSI AI SISTEMI

- vecchi accessi non vengono eliminati
- i privilegi sono assegnati con poca attenzione senza applicare il principio del need to know
- vengono utilizzate utenze di gruppo e non nominali, anche se potrebbe farsi diversamente

SVILUPPO SOFTWARE

- in fase di progettazione non sono considerati i requisiti di sicurezza
- non viene verificato il codice sviluppato / i test non sono completi
- non viene valutato e controllato attentamente e periodicamente l'open source

VULNERABILITÀ/PATCH

- non vengono svolti vulnerability assessment con la necessaria periodicità
- il processo di gestione delle patch non è regolamentato e strutturato
- non viene posta sufficiente attenzione nell'analisi e test delle patch

Revisione dei Processi IT in ottica di Sicurezza 2/2

I processi IT devono essere ottimizzati dal punto di vista della sicurezza.

Quante volte troviamo nelle aziende che:

BACKUP

- non si fanno prove di restore
- non ci sono copie remote
- non vengono crittografate le copie, seppure con dati altamente critici e sensibili

LOG

- non vengono raccolti e controllati i log delle attività critiche
- i log non sono sufficientemente protetti
- non vengono rispettati i requisiti temporali di conservazione dei log

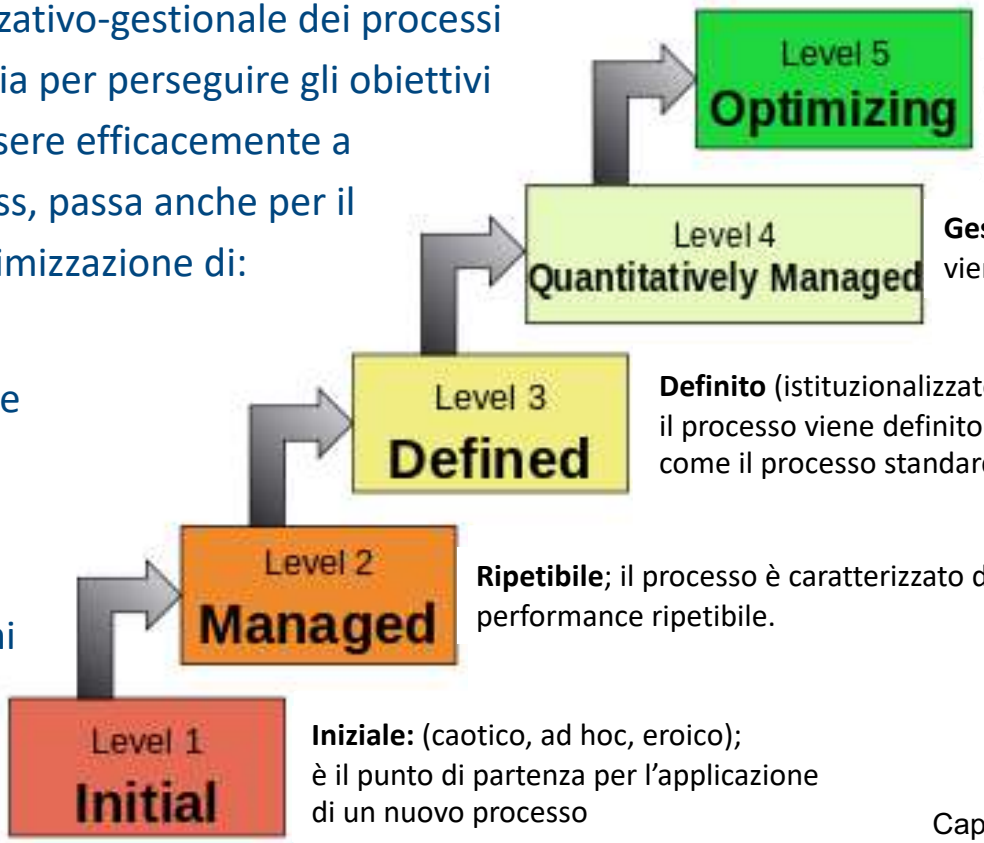
MOBILE

- non vengono seguite regole stringenti sul download del software
- contengono dati personali, oltre a quelli aziendali
- non sono protetti adeguatamente

«Salto» di maturità dei Processi/Servizi IT

L'evoluzione organizzativo-gestionale dei processi e servizi IT, necessaria per perseguire gli obiettivi di «sicurezza» ed essere efficacemente a supporto del business, passa anche per il miglioramento e ottimizzazione di:

- politiche, regole e linee guida
- attività, ruoli e responsabilità
- indicatori e azioni di controllo.



Ottimizzato (miglioramento del processo); la gestione del processo include una deliberata ottimizzazione e miglioramento

Gestito (quantificato); il processo viene gestito e misurato

Definito (istituzionalizzato); il processo viene definito e confermato come il processo standard aziendale

Ripetibile; il processo è caratterizzato dalla performance ripetibile.

Iniziale: (caotico, ad hoc, eroico); è il punto di partenza per l'applicazione di un nuovo processo

CMMI
Capability Maturity Model Integration

INTERVALLO

Riprenderemo fra 5 minuti, grazie!

Contenuti del Webinar

- *Governance*: Elementi fondamentali della Governance della Cyber Security
- *Compliance*: Requisiti di Cyber Security richiesti da leggi e mercato
- *E-Learning* al servizio della Compliance: Esempi di Corsi interattivi LPD e GDPR
- *Percorso progettuale*: Costruire il proprio sistema di CyberSecurity Management
- *Domande e risposte*

Accountability in senso sostanziale!

Compliance Integrata 1/2

Compliance integrata 2/2

L'ambito di interesse della **SECURITY COMPLIANCE** riguarda il controllo del rispetto di tutto il «Corpo Normativo» in materia di information security:

- **normative vigenti in materia di information security** (leggi, regolamenti di settore, ecc.)
- **condizioni contrattuali stipulate con le terze parti in materia di information security** (clienti e fornitori)

Controllo del Corpo Normativo

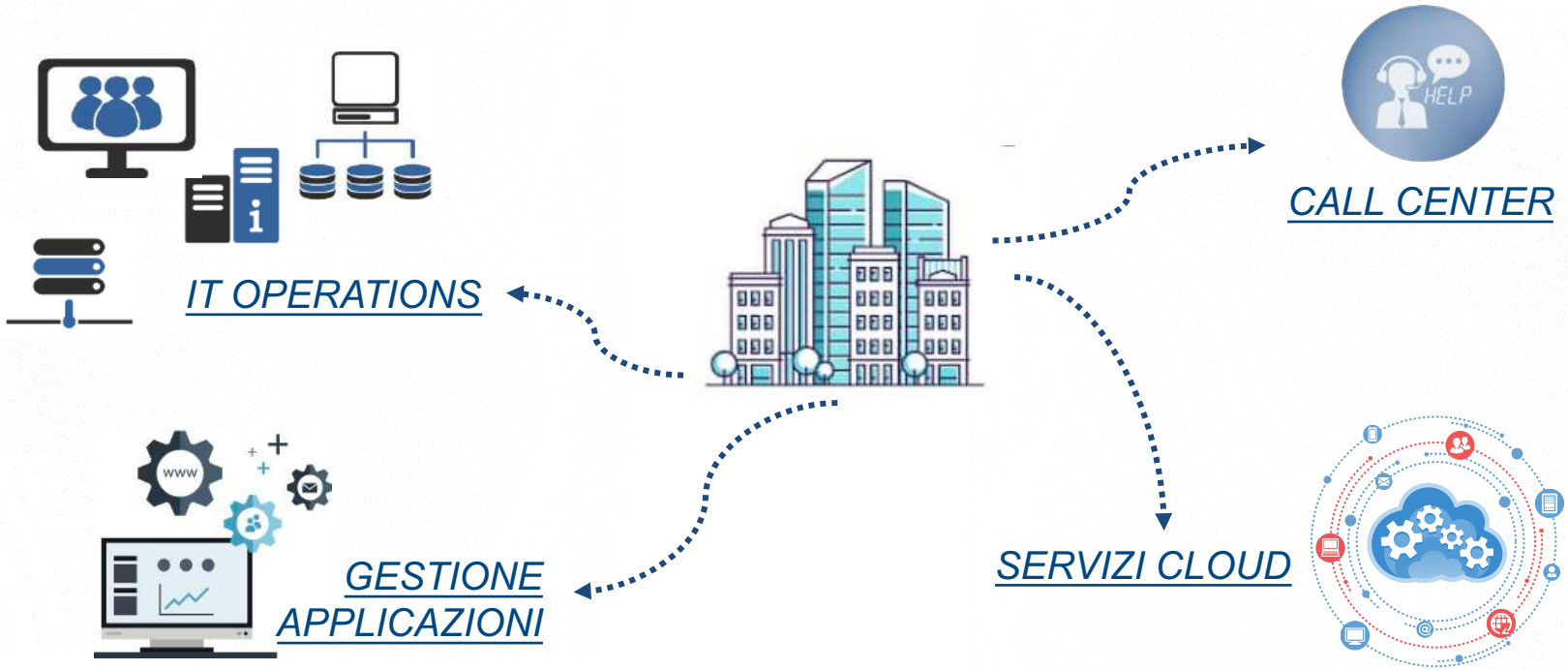
LEGAL INVENTORY ⟹ **TRADURRE IL REQUISITO NORMATIVO in SCHEMI** utili per identificare nuovi adempimenti, procedure, ruoli, ecc.

Per ciascuna norma sarà necessario individuare:

- obblighi e divieti imposti dal nuovo provvedimento
- tutte le abrogazioni e le modifiche di altri provvedimenti, indicando anche l'impatto operativo di questi interventi
- il campo di applicazione, in modo da agevolare la valutazione di applicabilità
- la descrizione del singolo adempimento e le modalità per adempiere
- i soggetti obbligati (ruoli e responsabilità)
- le scadenze
- la periodicità dell'adempimento
- le sanzioni e gli organi deputati al controllo

Controllo delle condizioni contrattuali 1/3

Tipologie di outsourcing (IT)



Controllo delle condizioni contrattuali 2/3

Facciamo un esempio....

Gestione fornitori servizi informatici

Mantenimento livello di sicurezza delle informazioni e servizi

- *LPD (Art. 8)*
- *GDPR (Art. 28)*
- *ISO27001 (A.15)*
- *Regolamenti di settore*

PROCEDURA di selezione, valutazione, gestione, controllo del fornitore

Controllo delle condizioni contrattuali 3/3

CONTROLLO DELLE CONDIZIONI CONTRATTUALI CON TERZE PARTI

Per quanto riguarda le esternalizzazioni rilevanti dal punto di vista della sicurezza (segnatamente in ambito informatico), l'impresa e il fornitore di servizi fissano contrattualmente requisiti in materia di sicurezza. ***L'impresa deve sorvegliarne il rispetto****.*

CONTRATTI
Servizi, Requisiti,
SLA e Penali

- *Livelli minimi disponibilità*
- *Procedura change management*
- *Modalità e frequenza Backup*
- *Formazione collaboratori*
- *Procedura gestione emergenze*
- *BCP / DRP*
- *Exit Plan*
- *Audit e Reporting*

Titolare e Responsabile del trattamento 1/2

TITOLARE DEL TRATTAMENTO
Definisce scopo e mezzi del trattamento

RESPONSABILE DEL TRATTAMENTO
Tratta dati per conto del Titolare

Titolare e Responsabile del trattamento 2/2

Contratto di affidamento del trattamento al Responsabile

- Il Titolare può affidare il trattamento ad un Responsabile del trattamento **attraverso un contratto/accordo**.
- È di solito un **addendum al Contratto di Servizi**.
- Il Titolare deve assicurare che il Responsabile del trattamento sia in grado di **garantire la sicurezza dei dati.**

- Descrizione del trattamento
- Finalità e modalità
- Tipo di dati personali
- Categorie di interessati
- Durata del trattamento
- Obblighi e diritti del Titolare
- Obblighi e diritti del Responsabile

Principali obblighi: Protezione e Sicurezza dei Dati (Artt. 7 e 8)

la legge richiede di

ADOTTARE I PROVVEDIMENTI TECNICI E ORGANIZZATIVI NECESSARI

- **GARANTIRE LA CONFORMITÀ ALLE DISPOSIZIONI SULLA PROTEZIONE DEI DATI**

- **GARANTIRE LA SICUREZZA DEI DATI / EVITARE VIOLAZIONI DELLA SICUREZZA DEI DATI**

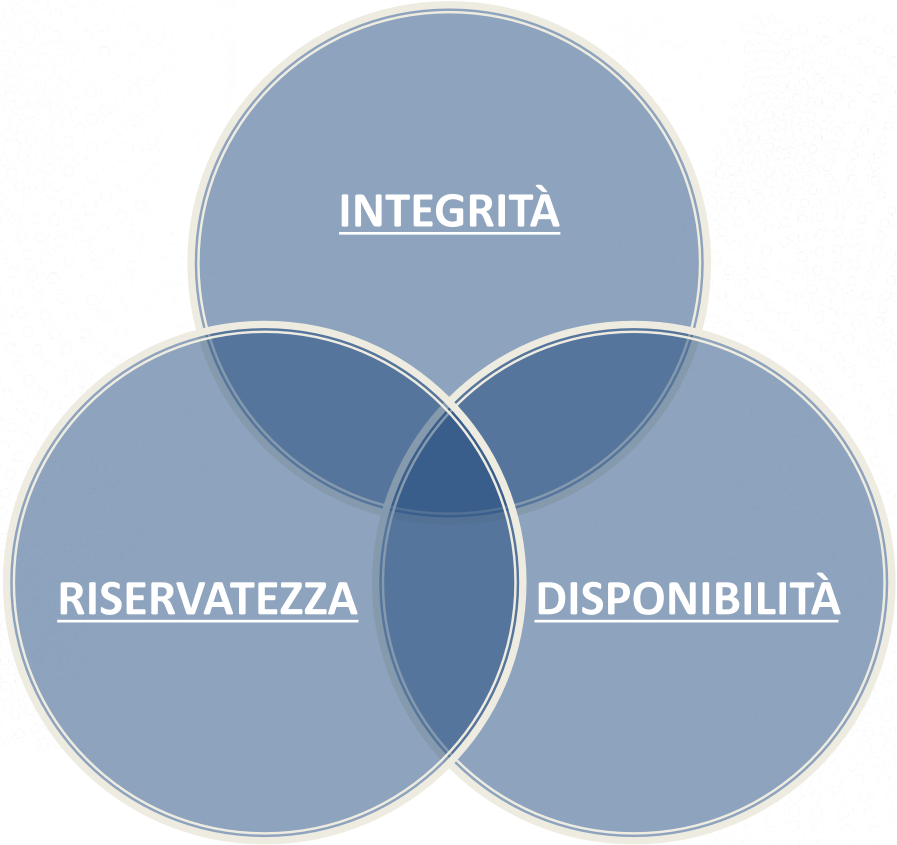
Garantire la conformità alle disposizioni sulla protezione dei dati rispetto ai principi

- I dati personali **devono essere trattati in modo LECITO**: con questo concetto s'intende che l'elaborazione deve avere un *fondamento giuridico* valido: consenso della persona interessata; un interesse preponderante (privato o pubblico) oppure dalla legge medesima
- Il trattamento deve essere conforme ai principi della **buona fede** e della **proporzionalità**
- I dati personali **sono distrutti o resi anonimi appena non sono più necessari per lo scopo** del trattamento.
- I dati personali possono essere raccolti soltanto per uno **scopo determinato e riconoscibile** per la persona interessata ⟹ **INFORMATIVA**
- Chi tratta dati personali deve accertarsi che **siano esatti** ⟹ l'onere di garantire l'aggiornamento delle informazioni raccolte ricade su chi tratta i dati personali, ossia l'organizzazione.

Garantire la conformità alle disposizioni sulla protezione dei dati rispetto ai diritti riconosciuti agli interessati

- DIRITTO DI ACCESSO
- DIRITTO DI FARSI CONSEGNARE I DATI O DI ESIGERNE LA TRASMISSIONE A TERZI
- DIRITTO DI RETTIFICA, CANCELLAZIONE O DISTRUZIONE, DIVIETO DI TRATTAMENTO O DI COMUNICAZIONE A TERZI

Garantire la sicurezza dei dati / evitare violazioni della sicurezza dei dati



Artt. 7 e 8: Provvedimenti tecnici e organizzativi

ART. 7.

1) Il titolare del trattamento è tenuto ad adottare i **provvedimenti tecnici e organizzativi necessari** affinché il trattamento dei dati personali **sia conforme alle disposizioni sulla protezione dei dati**, in particolare ai principi di cui all'articolo 6. **li adotta sin dalla progettazione**.

2) I **provvedimenti tecnici e organizzativi devono essere adeguati** in particolare **allo stato della tecnica**, **al tipo** e **all'entità del trattamento** dei dati personali come pure **ai rischi derivanti dal trattamento** per la personalità o i diritti fondamentali delle persone interessate.

3) Il titolare del trattamento è tenuto a garantire, **mediante appropriate impostazioni predefinite**, che il trattamento di dati personali **sia circoscritto al minimo indispensabile per lo scopo perseguito**, salvo che la persona interessata disponga altrimenti.

ART. 8

1) Il titolare e il responsabile del trattamento garantiscono, mediante appropriati provvedimenti tecnici e organizzativi, **che la sicurezza dei dati personali sia adeguata al rischio**.

2) I provvedimenti devono **permettere di evitare violazioni della sicurezza dei dati**.

3) Il Consiglio federale emana disposizioni sui **requisiti minimi in materia di sicurezza dei dati**.

PRIVACY BY DESIGN

BEST PRACTICE

PROPORZIONALITÀ

RISCHIO

PRIVACY BY DEFAULT

MINIMIZZAZIONE

REQUISITI MINIMI

Novità normative sulla protezione dei dati personali (LPD e GDPR)

- **05.2010:** l'UFG avvia l'iter di revisione della Legge federale del 19.06.1992 sulla protezione dei dati;
- **25.09.2020:** approvazione nuova LPD con 141 voti favorevoli, 54 contrari e 1 astensione;
- **Seconda metà 2022:** probabile entrata in vigore della Legge.

Valutazione d'impatto sulla protezione dei dati (art. 22)

*Il **Titolare** del trattamento **effettua previamente** una valutazione d'impatto sulla protezione dei dati quando il trattamento **può comportare** un **rischio elevato** per la personalità o i diritti fondamentali della persona interessata*

(es.: trattamento su grande scala di dati personali degni di particolare protezione).

Consultazione dell'IFPDT (art. 23)

*Il **Titolare** del trattamento **chiede previamente il parere dell'IFPDT** se dalla valutazione d'impatto sulla protezione dei dati emerge che, **nonostante i provvedimenti previsti dal Titolare**, il trattamento previsto comporta un rischio elevato per la personalità o i diritti fondamentali della persona interessata.*

*Il **Titolare privato** del trattamento **può rinunciare a consultare l'IFPDT** se ha consultato il **Consulente per la protezione dei dati**.*

La valutazione d'impatto sulla protezione dei dati contiene:

- una descrizione del trattamento previsto
- una valutazione dei rischi per la personalità o per i diritti fondamentali della persona interessata
- nonché i provvedimenti a loro tutela.

Notifica di violazioni della sicurezza dei dati (art. 24)

Il **Titolare** del trattamento **notifica quanto prima all'IFPDT** ogni violazione della sicurezza dei dati **che comporta verosimilmente un rischio elevato** per la personalità o i diritti fondamentali della persona interessata.

«Violazione»

qualsiasi incidente di sicurezza dei dati (riservatezza, integrità, disponibilità) in seguito al quale, in modo accidentale o illecito, i dati personali vengono persi, cancellati, distrutti, modificati, oppure divulgati o resi accessibili a persone non autorizzate.

Esempi di «Violazione»

- ✓ *perdita o furto di un hard disk contenente dati personali*
- ✓ *diffusione di dati via mail a persone non autorizzate a trattarli*
- ✓ *alterazione dei dati in seguito ad un attacco informatico o ad un errore software*
- ✓ *indisponibilità dei dati a causa di un malfunzionamento dei sistemi o di un attacco informatico.*

Notifica di violazioni della sicurezza dei dati (art. 24)

Il **Responsabile** del trattamento **informa quanto prima il Titolare** del trattamento su **ogni violazione** della sicurezza dei dati.

RESPONSABILE TRATTAMENTO

informa

TITOLARE TRATTAMENTO

informa

PERSONA INTERESSATA

Il **Titolare** del trattamento **informa la persona interessata** sulla violazione della sicurezza dei dati, **se ciò è necessario per proteggere la persona interessata o se lo esige l'IFPDT**.

Il consulente per la protezione dei dati (art. 10)

CHI si occupa di «data protection» per un'organizzazione deve essere dotato di **competenze multidisciplinari**:

- competenze informatiche
- conoscenza del funzionamento dei processi aziendali
- conoscenza specialistica della normativa
- determinate qualità personali

Le sanzioni (artt. 60, 61, 62, 63, 64)

Sono quattro i casi che Legge Federale sulla Protezione dei Dati considera come violazione e che possono comportare **una multa il cui valore può raggiungere i 250.000 CHF a seguito di una querela di parte**:

- *una violazione degli obblighi di informare, di concedere l'accesso e di collaborare*
- *una violazione degli obblighi di diligenza*
- *una violazione dell'obbligo del segreto;*
- *una inosservanza di una decisione intimata dall'Autorità di Controllo.*

Attenzione... sino ad ora abbiamo parlato di procedimenti **contro le persone fisiche**, quindi contro il proprietario dell'azienda, il management, i dirigenti, i membri degli organi preposti alla gestione, contro i soggetti che svolgono attività d'affari o di servizio per terze persone, i quali possono essere responsabili delle violazioni di cui abbiamo parlato o per dolo o per colpa, anche quando omette di impedire che la violazione sia commessa da un subordinato, da un mandatario

l'art. 64 «**Infrazioni commesse nell'azienda**» ci dice che alle infrazioni commesse dall'azienda si applicano gli artt. 6 e 7 della Legge federale sul diritto penale amministrativo (DPA) del 22.03.1974

Le sanzioni (artt. 60, 61, 62, 63, 64)

Se la multa applicabile non supera i 50 000 franchi e se la determinazione delle persone punibili secondo l'articolo 6 DPA esige provvedimenti d'inchiesta sproporzionati all'entità della pena, l'autorità può prescindere da un procedimento contro dette persone e, in loro vece, condannare al pagamento della multa **l'azienda** (art. 7 DPA)

AZIENDA o MANAGEMENT

NESSUNO… è IMMUNE

DA RESPONSABILITÀ!!

INTERVALLO

Riprenderemo fra 5 minuti, grazie!

Contenuti del Webinar

- *Governance*: Elementi fondamentali della Governance della Cyber Security
- *Compliance*: Requisiti di Cyber Security richiesti da leggi e mercato
- *E-Learning* al servizio della Compliance: Esempi di Corsi interattivi LPD e GDPR
- *Percorso progettuale*: Costruire il proprio sistema di CyberSecurity Management
- *Domande e risposte*

Contenuti del Webinar

- ***Compliance:* Requisiti di Cyber Security richiesti da leggi e mercato**
  - Novità normative sulla protezione dei dati personali (LPD e GDPR)
  - Standard e best practice di Cyber Security riconosciuti dal mercato
  - Certificazione del sistema di Cyber Security

Standard and Framework

COBIT 2019

Information Security Management ISO 27001 Certified

International Organization for Standardization ISO 22301

ITIL® 4

ITIL® è un marchio registrato di AXELOS Limited il cui uso è consentito solamente previa autorizzazione di AXELOS Limited

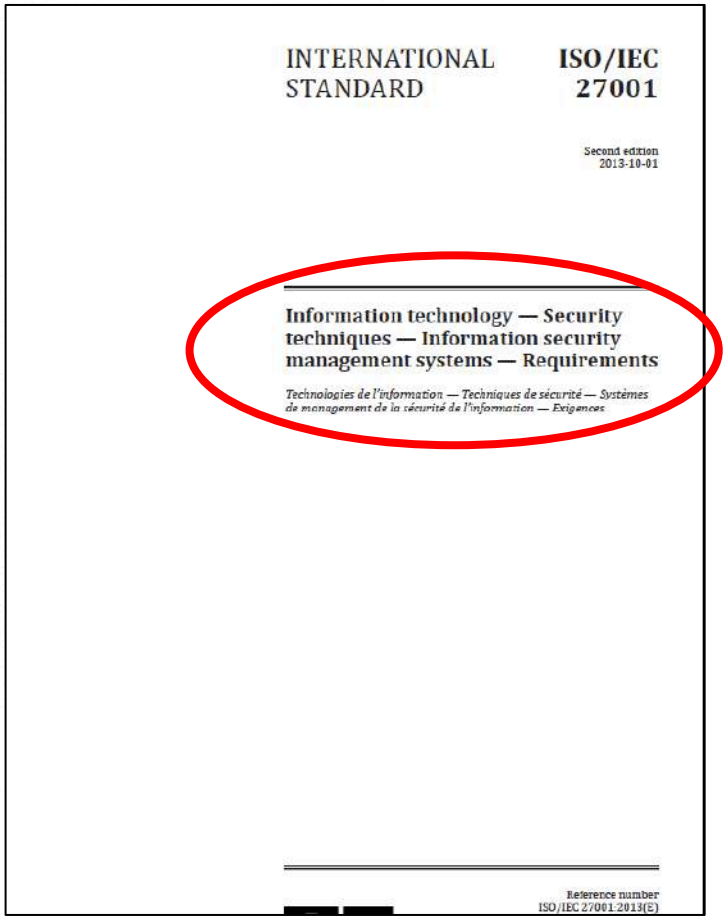
IDENTIFY PROTECT DETECT RESPOND RECOVER NIST CSF

enisa European Network and Information Security Agency

Contenuti del Webinar

- ***Compliance:* Requisiti di Cyber Security richiesti da leggi e mercato**
  - Novità normative sulla protezione dei dati personali (LPD e GDPR)
  - Standard e best practice di Cyber Security riconosciuti dal mercato
  - Certificazione del sistema di Cyber Security

ISO 27001: ISMS Requirements & IS Controls



INTERNATIONAL STANDARD

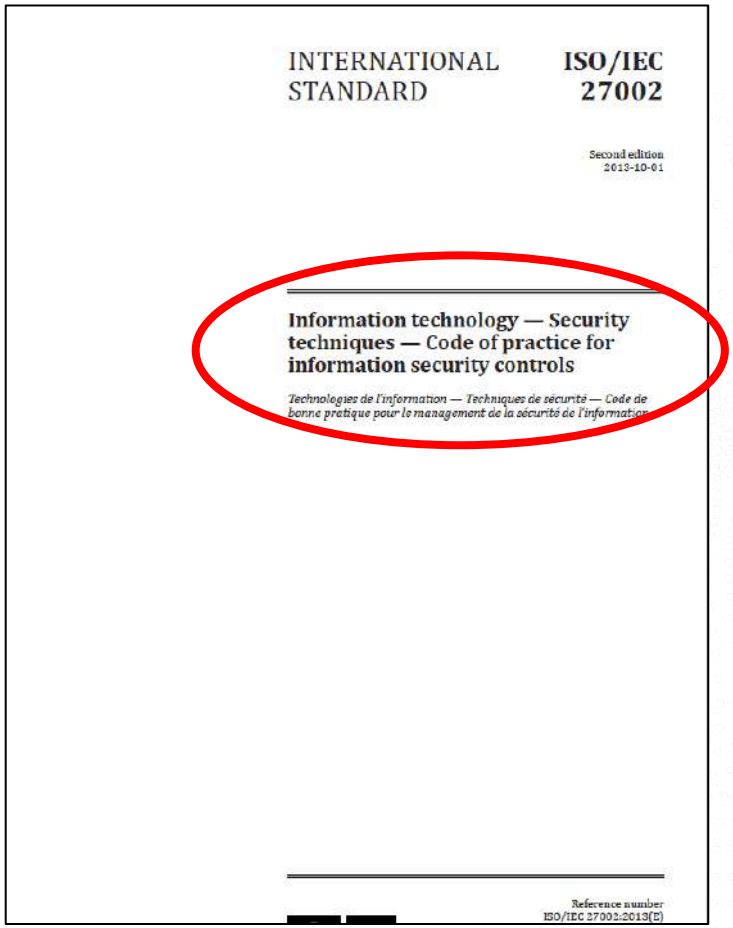
ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)



INTERNATIONAL STANDARD

ISO/IEC 27002

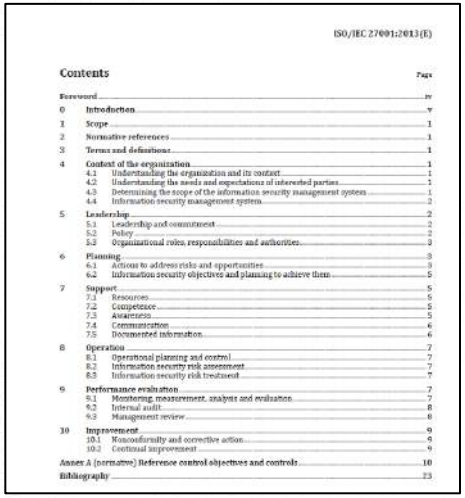
Second edition
2013-10-01

Information technology — Security techniques — Code of practice for information security controls

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

Reference number
ISO/IEC 27002:2013(E)

ISO 27001: Information Security Management Process



ISO/IEC 27001:2013(E)

Contents

1. Context analysis & ISMS perimeter definition

2. Actual Controls analysis & Risk Assessment

3. Policy, Organization and Resources

ISO 27001:2013 INFORMATION SECURITY MANAGEMENT PROCESS

4. Strategies definition and Action Planning

5. ISMS & Controls implementation

6. Training

7. Monitoring of Objectives/Indicators and Compliance

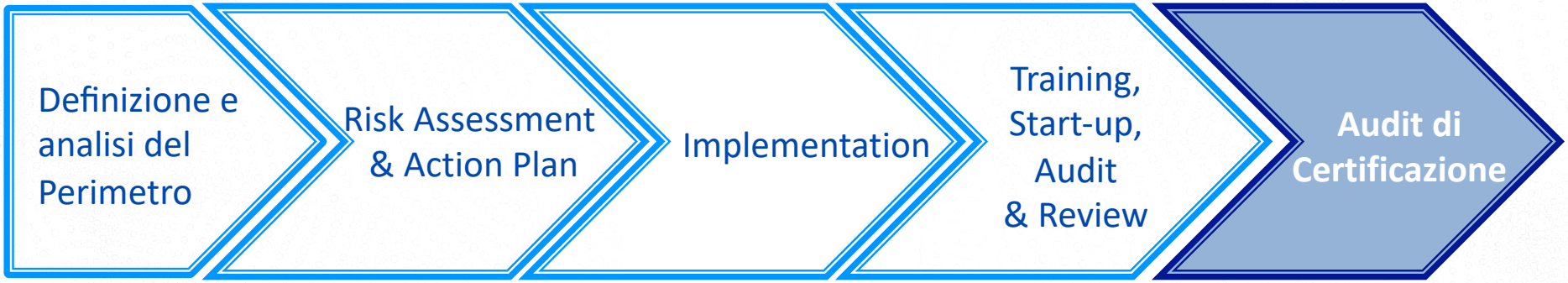
8. Audit & Reporting

9. ISMS Continual improvement

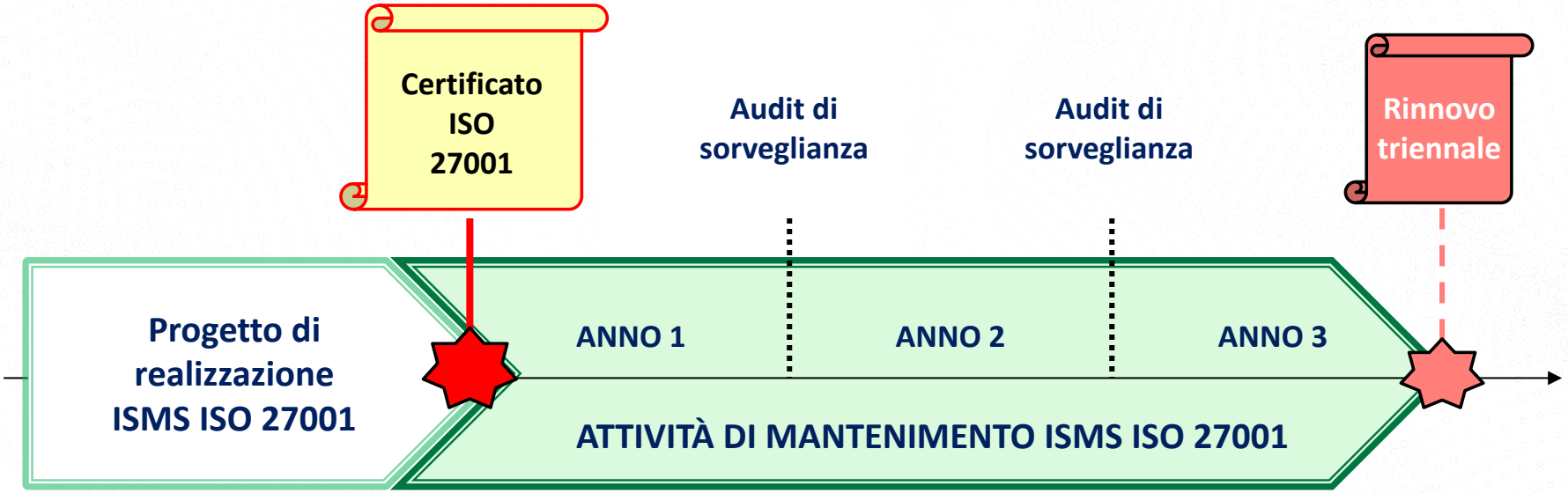
ISO 27001: Technological/Organizational Controls

- Asset management
- Cryptographic
- Secure IT Development and Maintenance
- Secure Network and Information Transfer
- Secure IT Operations
- Logging and monitoring
- Backup Management
- Technical vulnerability management
- Logical Access Control
- Mobile devices and teleworking
- Protection from cyber attack
- Physical Asset Security
- Incident Management
- IT Continuity
- Secure Supplier Relationships
- Secure People Behaviours

Progetto per la Certificazione ISO 27001



Ciclicità annuale dell'Audit dell'Ente di Certificazione



Certificato ISO 27001

- Garanzia per gli Azionisti e altri Stakeholders
- Riconosciuto dal Mercato in tutto il mondo
- Suggerito da Normative e Regolamenti di Settore
- Apprezzato da Revisori e Autorità di Controllo
- Favorisce la responsabilizzazione interna
- Supporta il miglioramento continuo

Contenuti del Webinar

- *Governance*: Elementi fondamentali della Governance della Cyber Security
- *Compliance*: Requisiti di Cyber Security richiesti da leggi e mercato
- *E-Learning* al servizio della Compliance: Esempi di Corsi interattivi LPD e GDPR
- *Percorso progettuale*: Costruire il proprio sistema di CyberSecurity Governance
- *Domande e risposte*

Sistema di Cyber Security G&C «fatto su misura»

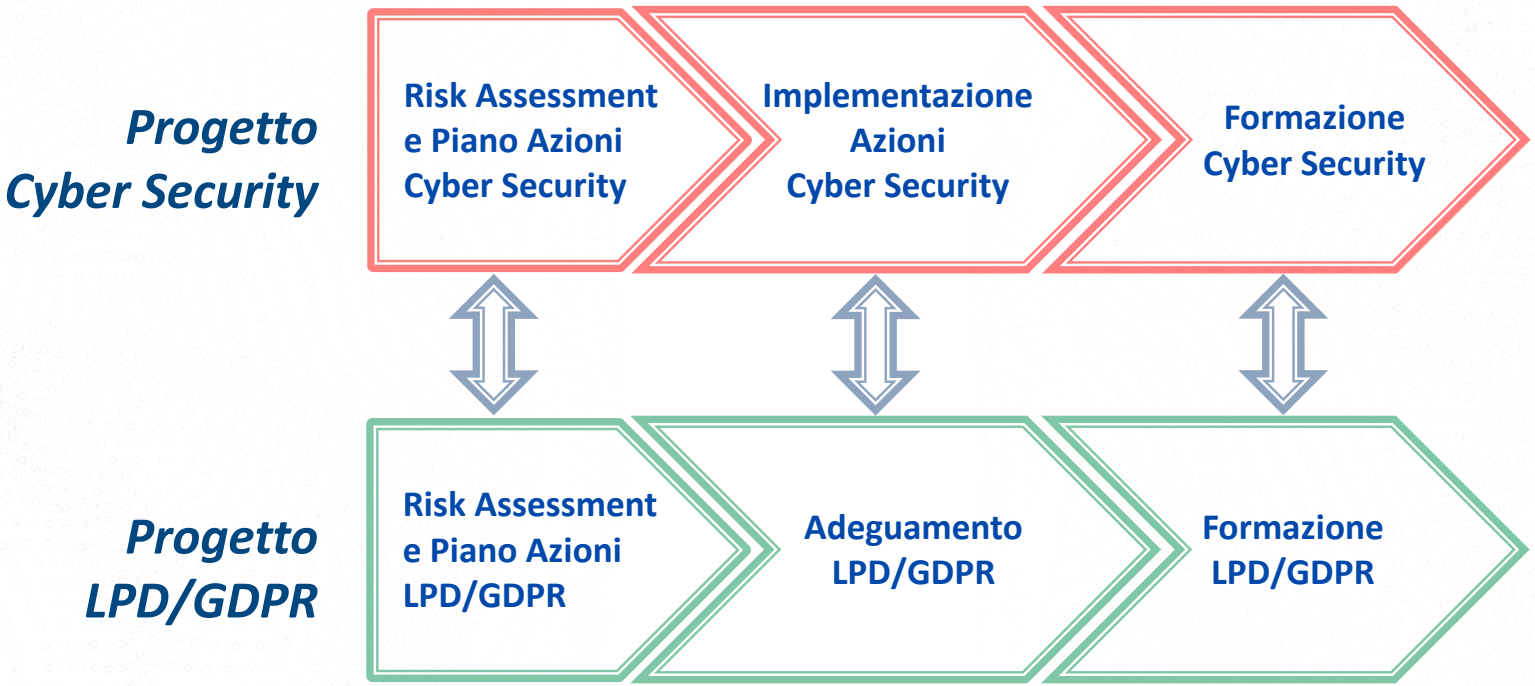
Il **percorso di sviluppo** del proprio sistema di **Cyber Security Governance & Compliance deve essere inquadrato nel percorso aziendale più ampio** di:

- gestione dei rischi operativi aziendali
- adeguamento ai nuovi requisiti normativi (LPD/GDPR) e regolamentari di settore
- evoluzione organizzativo-gestionale («*salto manageriale*»)

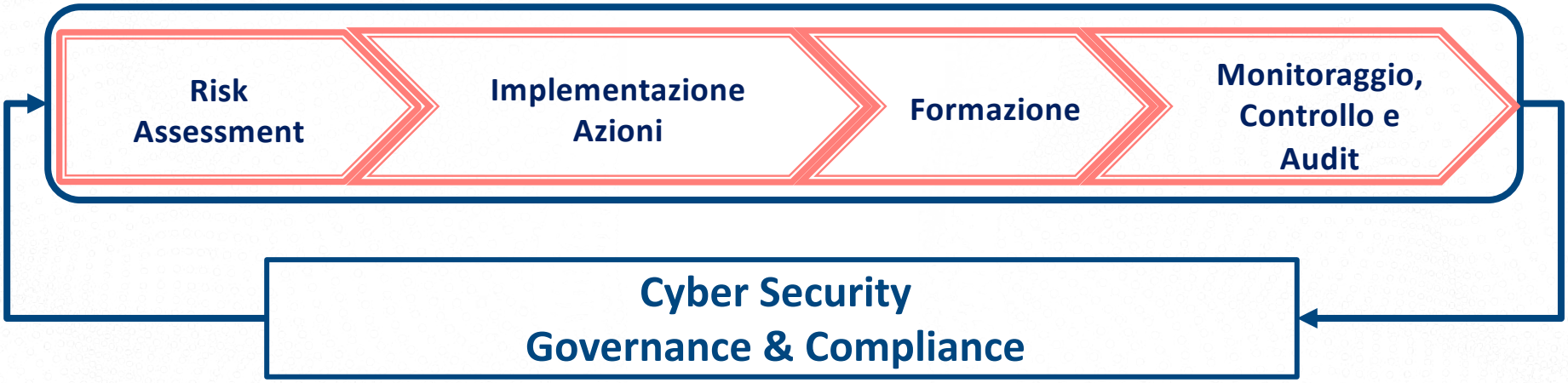
che **l'azienda ha necessità/opportunità di intraprendere a fronte di**:

- *novità normative e regolamentari*
- *aumento delle problematiche e minacce alla sicurezza*
- *crescita esponenziale della quantità/sensibilità dei dati scambiati*
- *evoluzione tecnologica e crescente pervasività delle tecnologie*
- *obiettivi e piani strategici di business*
- *richieste del mercato (es. Certificazione ISO 27001).*

Progetto 2021: Cyber Security Governance & Compliance



Cyber Security Governance & Compliance



RUOLI DI COORDINAMENTO E CONTROLLO

- SECURITY MANAGER (CISO)
- CONSULENTE PROTEZIONE DATI (LPD)

Conclusioni

- La **Cybersecurity è fondamentale per tutte le Organizzazioni** e lo sarà sempre più con l'evoluzione delle tecnologie digitali.

- Le **nuove normative ed il mercato** richiedono maggiori garanzie di sicurezza e richiedono di utilizzare le metodologie e gli standard di riferimento.

- Diverse sono le **metodologie e gli standard** per le varie tematiche e ambiti di applicazione: è importante scegliere quelli più adeguati all'organizzazione.

- Il **Certificato ISO 27001** è, ad oggi, lo standard riconosciuto in tutto il mondo per la costruzione del sistema di Information Security Governance.

- La **Direzione Aziendale** rappresenta il "Garante" della Cyber Security e della Privacy e ne risponde verso la proprietà, il mercato e le leggi.

Contenuti del Webinar

- *Governance*: Elementi fondamentali della Governance della Cyber Security
- *Compliance*: Requisiti di Cyber Security richiesti da leggi e mercato
- *E-Learning* al servizio della Compliance: Esempi di Corsi interattivi LPD e GDPR
- *Percorso progettuale*: Costruire il proprio sistema di CyberSecurity Management
- *Domande e risposte*

Grazie per l'attenzione!

siro.migliavacca@sec-lab.com

francesca.colombo@sec-lab.com

alessandro.carniato@sec-lab.com

www.sec-lab.com

www.elearningatelier.ch