Qualification Program in Information Security Management according to ISO/IEC 27002

Cesare Gallotti

Milano, 23 gennaio 2009

Agenda

- Presentazione
- Le norme della serie ISO/IEC 27000
- La sicurezza delle informazioni secondo le ISO/IEC 2700x
- Le certificazioni professionali ISO/IEC 2700x

Presentazione

Cesare Gallotti

- Da 10 anni mi occupo di consulenza e di auditing nell'ambito dell'Information Technology
- Dal 1999 al 2008 dipendente Securteam, Intesis e DNV
- Consulente e Project Manager per la realizzazione di Sistemi di Gestione per la Sicurezza delle Informazioni (Risk Assessment, definizione dei processi, ...) e di adeguamento alle normative vigenti presso aziende di varie dimensioni e settori.
- Lead Auditor ISO/IEC 27001:2005 (CEPAS)
- Progettista e docente per corsi ISO/IEC 27001 accreditati CEPAS
- Relatore presso Master della Bocconi in ambito Sicurezza delle Informazioni

Le norme della serie ISO/IEC 27000

Standard verificabili vs. linee guida

- Standard verificabile: uno standard con specifiche rispetto alle quali può essere condotto un audit da parte di personale indipendente
  - > La ISO/IEC 27001 è uno standard verificabile: tutti i suoi requisiti devono essere messi in opera per dichiarare la propria conformità allo standard.
- Linee guida: manuali o raccolte di best practices disponibili per una loro selezione al fine di raggiungere un certo obiettivo
  - > La ISO/IEC 27002 (ex ISO/IEC 17799) è una "linee guida" e per questo possono presentare più approcci da seguire per la realizzazione dell'ISMS, anche tra loro non completamente coerenti
  - > Per questo motivo, non è corretto dichiarare una conformità rispetto a queste linee guida.

ISO/IEC 27001 vs. ISO/IEC 27002

- La ISO/IEC 27001 presenta i *requisiti* (usa il verbo "shall") o *specifiche* di un ISMS affinché possa essere certificato.
- La ISO/IEC 27002 è una *linea guida* (*Code of practice,* usa il verbo "should") che riporta gli stessi controlli di sicurezza (Annex A) della 27001 e li approfondisce. È una sorta di manuale o di linea guida che presenta delle *best practices*, selezionabili e applicabili dalle aziende.

Cronologia

Linee guida (ISO/IEC 27002)

1995: BS 7799

BS 7799-1:1999

↓

ISO/IEC 17799:2000

ISO/IEC 17799:2005

↓

ISO 27002:2005 (del 200\7)

Requisiti (ISO/IEC 27001)

BS 7799-2:1998

BS 7799-2:1999

BS 7799-2:2002

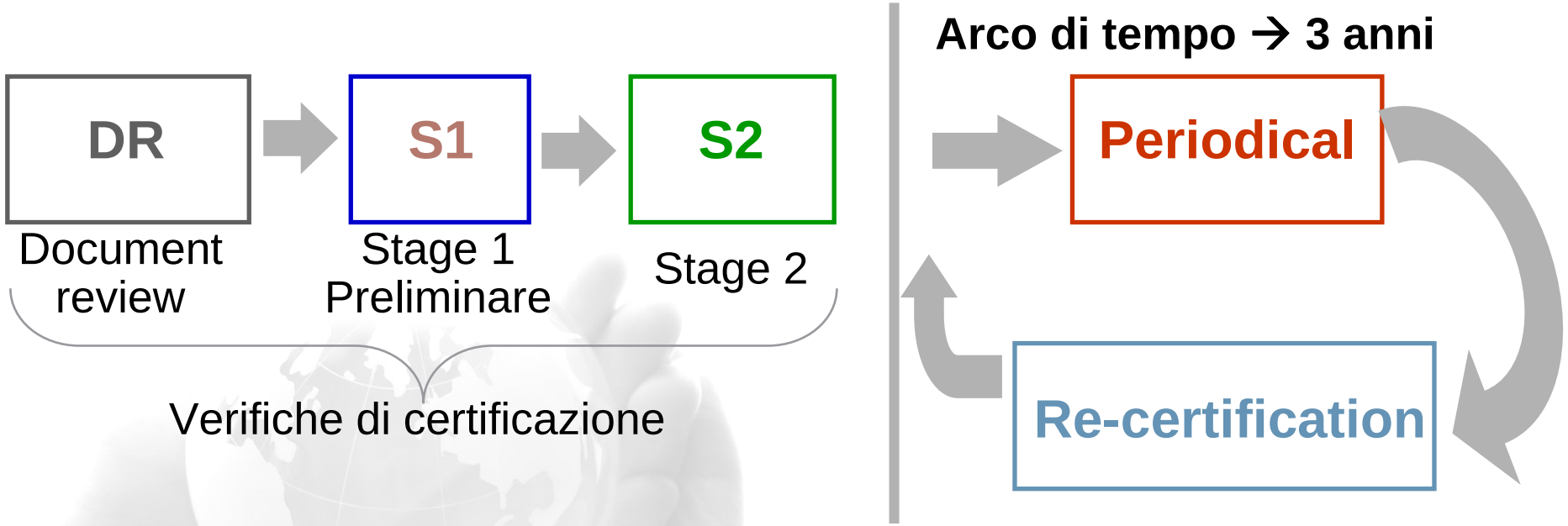
↓

ISO/IEC 27001:2005

Altre norme correlate

- La norma ISO/IEC 27001 è orientata alla certificazione, per questo, deve essere correlata alle norme che regolano gli audit e le certificazioni, in particolare a:
  - ISO/IEC 19011 ("Linee guida per gli audit")
  - ISO/IEC 27006 ("Requirements for bodies providing audit and certification of information security management systems")
- Altre norme sono state sviluppate:
  - ISO/IEC 27005: Information security risk management
- Altre norme sono in corso di sviluppo:
  - ISO/IEC 27000: Overview and vocabulary
  - ISO/IEC 27003: Information security management system implementation guidance
  - ISO/IEC 27004: Measurement
  - ...

L’iter di certificazione



- Un certificato dura generalmente 3 anni.
- Verifiche periodiche sono necessarie (almeno una all’anno) per dare confidenza del mantenimento della conformità ai requisiti.
- La ISO/IEC 27006:2007 richiede che le verifiche “di certificazione” vengano condotte in almeno due stages.

La sicurezza delle informazioni secondo le ISO/IEC 2700x

Information Security

- Le ISO/IEC 27001 e 27002 trattano degli Information Security Management Systems (ISMS)
- Le *informazioni* sono dati significativi (ossia che hanno significato per qualcuno). Le informazioni non sono riconducibili ai soli sistemi IT
- Per *sicurezza delle informazioni* si intende l'attività volta a definire, conseguire e mantenere le seguenti proprietà delle informazioni:
  - riservatezza
  - integrità
  - disponbilità
- Un Sistema di Gestione della Sicurezza delle Informazioni (ISMS o SGSI) è un insieme di elementi tra loro correlati e interagenti per stabilire politiche e obiettivi e per conseguire tali obiettivi con riferimento alla gestione della sicurezza delle informazioni

Importante

- La sicurezza si garantisce attraverso processi organizzativi e prodotti adeguati.
  - > Buoni processi organizzativi portano a scegliere ed usare prodotti adeguati.
  - > Non è vero l'inverso.

Chi dovrebbe realizzare un ISMS

Chi deve garantire sicurezza a potenziali clienti

Chi vuole confrontare le proprie soluzioni gestionali con altri

Chi vuole avere un approccio coerente alla gestione della icurezza

Chi vuole dimostrare la propria capacità di garantire un adeguato livello di sicurezza

Chi vuole avere una valutazione di parte terza

Chi vuole igliorare i propri servizi nei confronti dei clienti

Le principali finalità di un ISMS

- Seguire un approccio sistematico
- Ridurre gli incidenti e/o i reclami
- Migliorare le condizioni assicurative
- Ridurre eventuali danni di immagine a seguito di incidenti
- Disporre di una struttura per il miglioramento continuo
- Dare confidenza all'interno e all'esterno dell'organizzazione
- Migliorare la conoscenza e l'importanza dei problemi di sicurezza delle informazioni a livello della Direzione
- Accrescere le competenze
- Fornire una base sulla quale sostenere gli stimoli creativi e le spinte all'innovazione.

Struttura delle norme ISO/IEC 27001 e 27002

- La norma ISO/IEC 27001 è suddivisa in 3 parti:
  - Introduzione e definizioni (capitoli 0-3)
  - Requisiti di sistema (capitoli 4-8)
  - Controlli di sicurezza (Annex A; capitoli da A.5 a A.15; non esistono capitoli A.1-A.4)
- La norma ISO/IEC 27002 è suddivisa in 3 parti:
  - Introduzione alla sicurezza delle informazioni (capitoli 0-3)
  - Risk assessment (capitolo 4)
  - Controlli di sicurezza (capitoli 5-15)

Come sono descritti i controlli

- I 133 controlli della ISO/IEC 27001 e ISO/IEC 27002 sono suddivisi in:
  - capitoli, che suddividono i controlli in 11 categorie
  - obiettivi di controllo, che raggruppano i controlli a seconda di ciò che si vuole conseguire.
- I controlli sono descritti da una specifica dichiarazione (non più di 4 righe) che soddisfa l'obiettivo di controllo.
- La ISO/IEC 27002 accompagna la dichiarazione con:
  - *Implementation Guidance*: informazioni più dettagliate sulle possibili modalità con cui realizzare il controllo
  - *Other information*: eventuali ulteriori considerazioni, riferimenti ad altri standard o richiami a possibili aspetti legali.

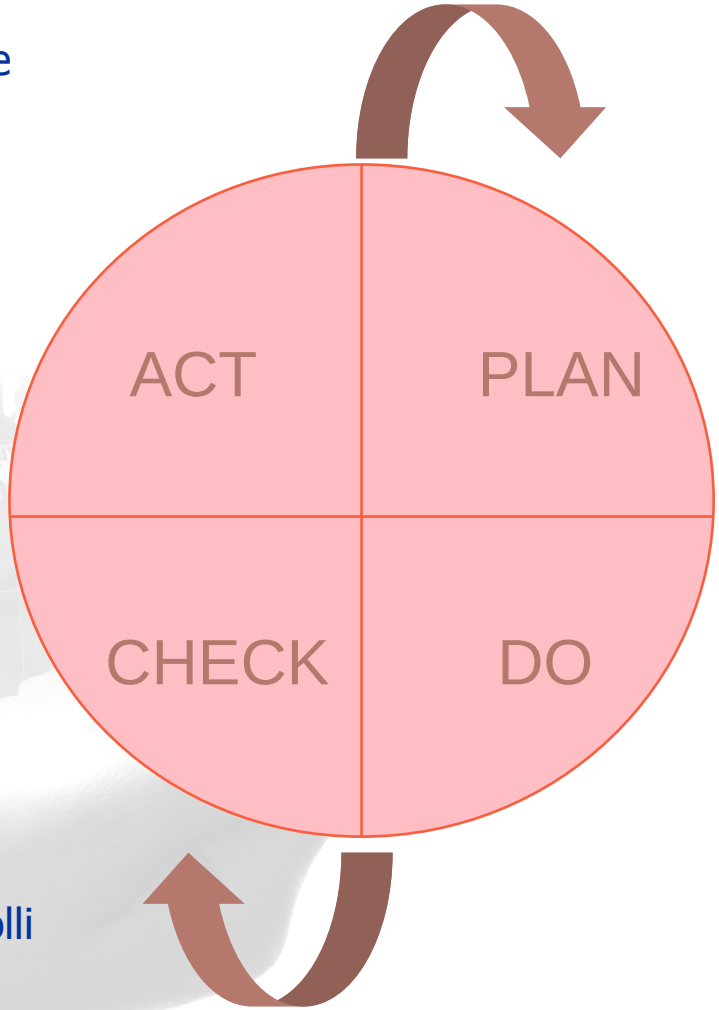
I requisiti di sistema

Azioni preventive

Azioni correttive

Manutenzione

Miglioramento



Politiche dell'ISMS

Campo di applicazione dell' ISMS

Risk Assessment

Trattamento del rischio

Allocare le risorse

Redigere la documentazione

Realizzare le misure di:

- Sicurezza del Personale
- Sicurezza fisica
- Gestione comunicazioni,
- Controllo accessi
- Sviluppo e manutenzione
- Continuità del business

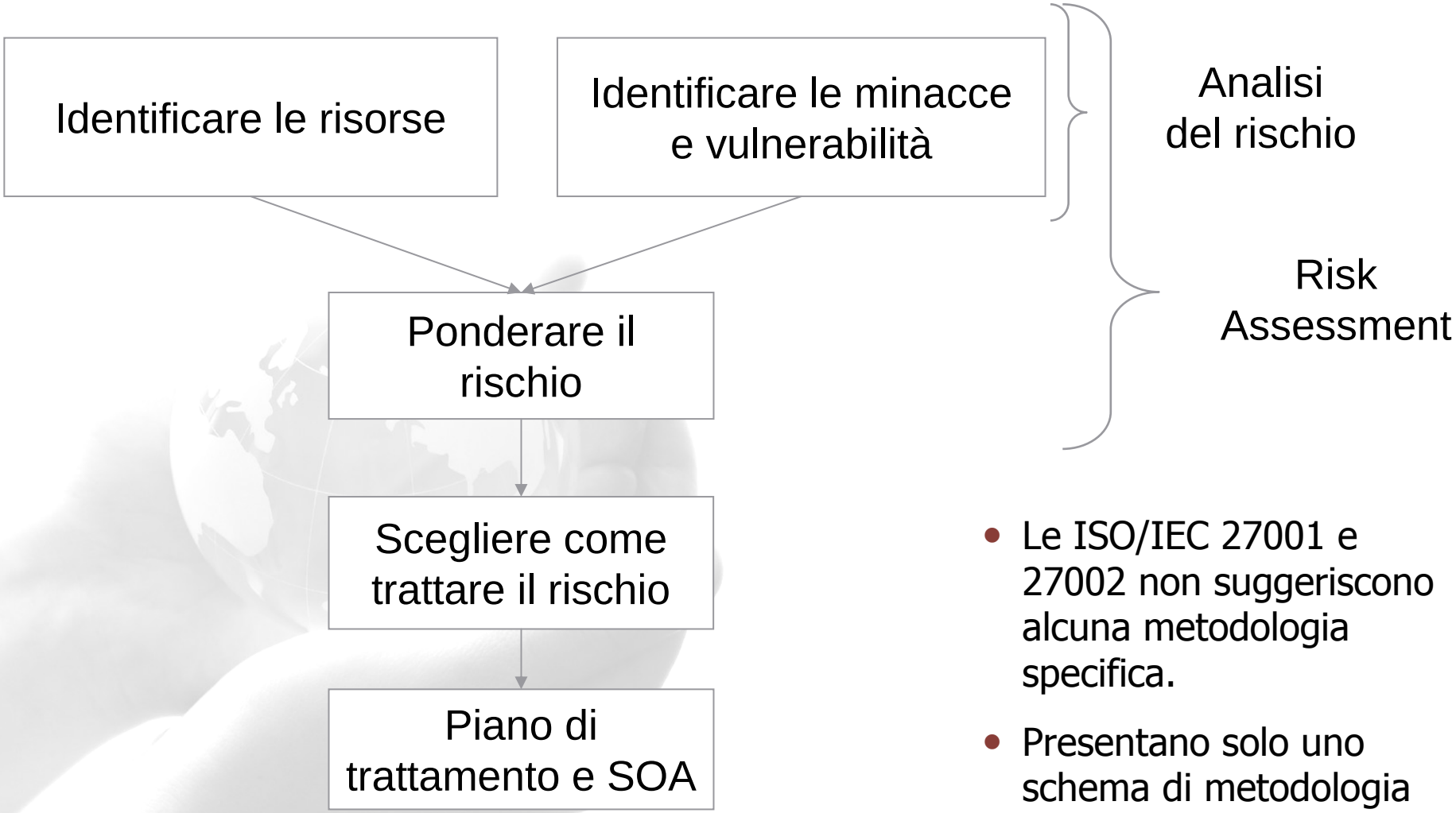
Controlli tecnici

Audit

Riesame Direzione

Analisi misure di efficacia dei controlli

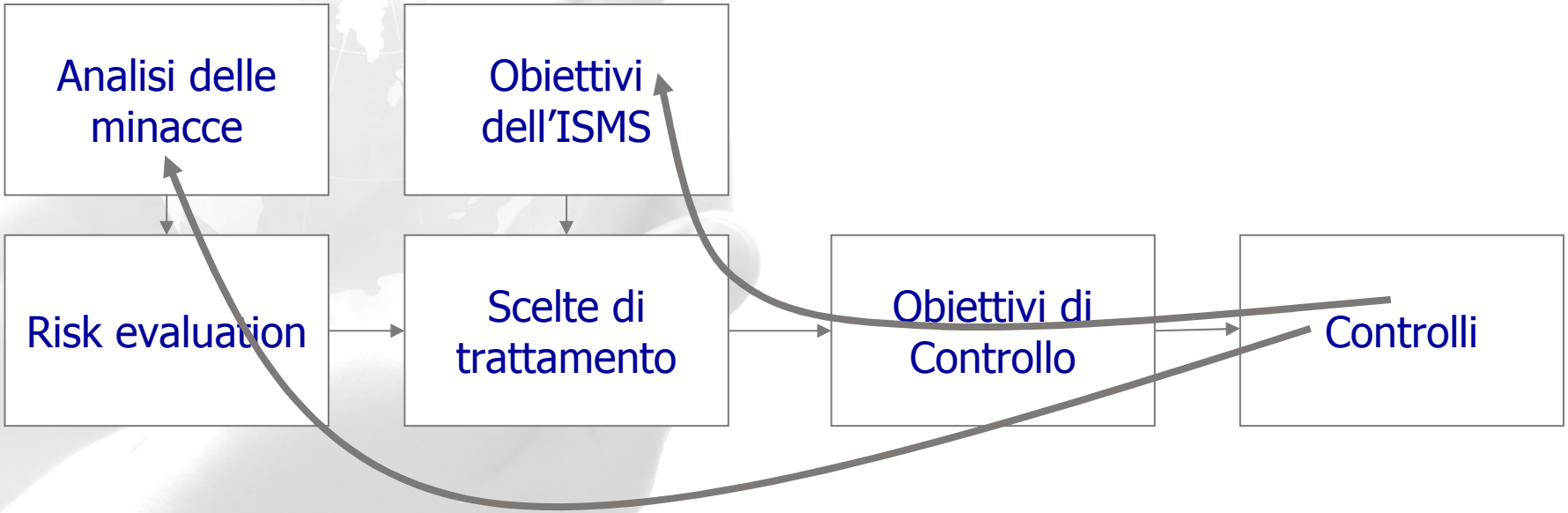
Schematicamente: analisi del rischio



- Le ISO/IEC 27001 e 27002 non suggeriscono alcuna metodologia specifica.
- Presentano solo uno schema di metodologia

Valutazione del rischio

- Alle diverse minacce vanno correlati i controlli scelti per contrastarle.
- A fronte della valutazione del rischio "iniziale" è logico aspettarsi una presunta valutazione del rischio a seguito della messa in opera dei controlli scelti.



Controlli di sicurezza

5. Security policy
6. Organization of information security
7. Asset management
8. Human resources security
9. Physical and environmental security
10. Communications and operations management
11. Access control
12. Information systems acquisition, development and maintenance
13. Information security incident management
14. Business continuity management
15. Compliance

Le certificazioni professionali ISO/IEC 2700x

Il programma di qualifica ISMS

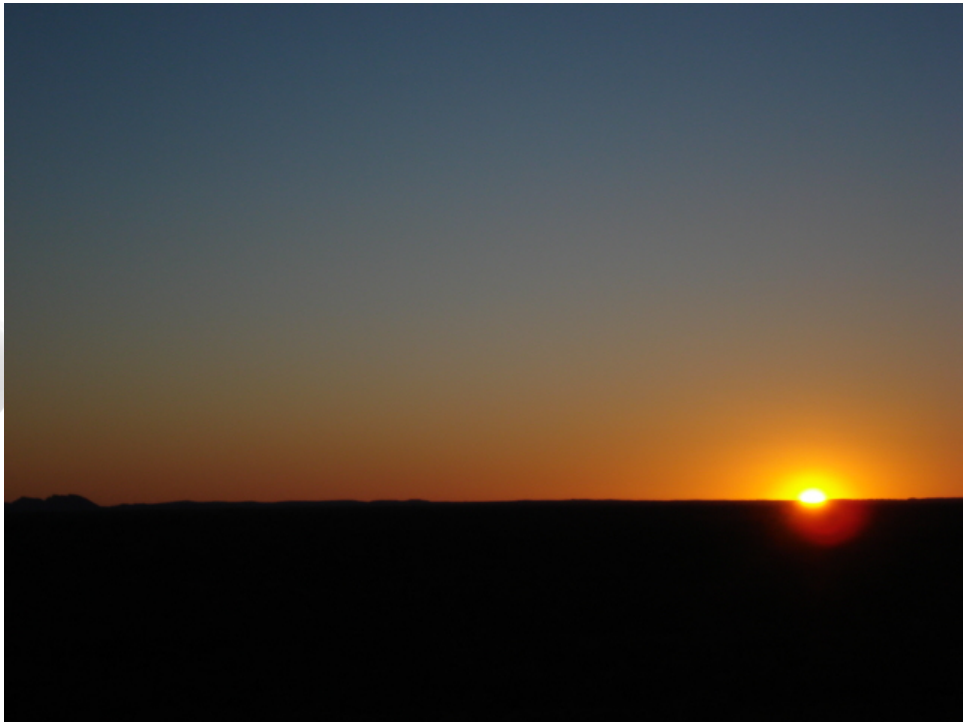
- Gli esami Exin sono denominati:

  Information Security based on ISO/IEC 27002

- Sono previsti e disponibili due tipologie di esami:
  - Information Security Foundation based on ISO/IEC 27002
  - Information Security Management Advanced based on ISO/IEC 27002
- L'esame Foundation è propedeutico per poter sostenere l'esame Advanced
- Non vengono trattati i capitoli "tecnici" della ISO/IEC 27002: 9-12

Considerazioni sugli schemi di certificazione ISMS

- Il programma di EXIN:
  - > non è orientato all'auditing
  - > può essere affrontato da persone con diversi gradi di competenza e permette la partecipazione ai corsi anche a professionisti con poca esperienza in materia
  - > richiede che i corsi di preparazione siano focalizzati su come realizzare e mantenere un ISMS



Domande?

- Cesare Gallotti
  - > www.cesaregallotti.it