UNIVERSITÀ DI PISA

DIPARTIMENTO DI INGEGNERIA DELL'ENERGIA DEI SISTEMI, DEL TERRITORIO E DELLE COSTRUZIONI

RELAZIONE PER IL CONSEGUIMENTO DELLA LAUREA MAGISTRALE IN INGEGNERIA GESTIONALE

Il processo di ICT Risk Management: gestione del Programma Strutturato di Sicurezza in Telecom Italia Information Technology

SINTESI

RELATORI

Prof. Antonella Martini
Dipartimento Dell'Energia, dei Sistemi, dei Trasporti e delle Costruzioni

Dott. Andrea Sassi
Team Manager in Demand and Management Group, Telecom Italia IT

Ing. Antonio Gentile
Consultant, CONSEL Consulting Academy

Ing. Leonardo Rescia
Consultant, CONSEL Consulting Academy

IL CANDIDATO

Silvia Mariotti

Sessione di Laurea del 19/02/2014
Anno Accademico 2013/2014

Il processo di ICT Risk Management: gestione del Programma Strutturato di Sicurezza in Telecom Italia Information Technology

Silvia Mariotti

SOMMARIO

Questo lavoro di tesi è il risultato di uno stage della durata di otto mesi, che si è svolto presso *Telecom Italia Information Technology*, sede di Roma, nel ruolo di "Junior Analyst" per conto di *ELIS Consulting Academy*. L'obiettivo della tesi è seguire la realizzazione di un progetto di sicurezza informatica, chiamato "Programma Strutturato di Sicurezza" (PSS), che coinvolge l'intera divisione dell'Information Technology del *Gruppo Telecom Italia* e, in particolare, la funzione Technical Security (IT.TS). Il PSS è nato all'inizio del 2013 in seguito a controlli effettuati all'interno dell'azienda che hanno rilevato la necessità di dedicare una maggior attenzione alla sicurezza informatica: sono state, infatti, riscontrate vulnerabilità ricorrenti nei sistemi IT tali da generare un elevato rischio potenziale, che potrebbe compromettere la sicurezza delle informazioni e dei servizi erogati da Telecom.

L'obiettivo del PSS è rendere il ciclo produttivo di TI.IT pienamente conforme al processo di ICT Risk Management, implementando una serie di attività che rendano trascurabile il rischio residuo dei sistemi IT (ovvero il rischio che permane in seguito all'adozione delle misure di sicurezza). In questo ambito, le principali attività svolte sono state:

- Individuazione del perimetro d'intervento, cioè dell'insieme di sistemi sui quali intervenire per sanare le vulnerabilità (fase di concezione);
- Definizione delle attività, mediante le quali sono stati realizzati gli interventi da porre in essere (fase di definizione);
- Analisi degli scostamenti, per l'individuazione delle criticità e la proposta di soluzioni a tali criticità (fase di analisi).

ABSTRACT

This thesis is the result of an internship period of eight months, which took place at the head office in Rome of *Telecom Italia Information Technology*, in the role of "Junior Analyst" on behalf of *ELIS Consulting Academy*. The thesis's aim is to follow the implementation of an information security project, called "Programma Strutturato di Sicurezza" (PSS), which involves the entire Information Technology division of *Gruppo Telecom Italia,* especially the Technical Security function (IT.TS). The PSS was born in early 2013 as a result of checks carried out within the company who have identified the need to devote greater attention to information security: indeed they were found recurring vulnerabilities in IT systems that would generate a high potential risk, which could compromise the security of the information and services provided by Telecom.

The PSS's goal is to make the production cycle of TI.IT fully compliant with the ICT Risk Management process, by implementing a series of activities that make negligible residual risk of the IT systems (ie the remaining risk after the security measures adoption). In this context, the main activities carried out were:

- Scope identification, that is the set of systems on which action to remedy the vulnerability (design phase);
- Activities definition, whereby were made the interventions to be implemented (development phase);
- Variances Analysis, for the identification of the critical issues and the proposed solutions to these problems (analysis phase).

1. CONTESTO E OBIETTIVI

Il presente lavoro di tesi è stato sviluppato nell'ambito del programma formativo "Junior Consulting" promosso da "ELIS - Consulting Academy" (http://consulting-academy.elis.org/). Il progetto a cui ho lavorato è stato commissionato dalla funzione Technical Security di Telecom Italia Information Technology (IT.TS), la funzione che si occupa di assicurare la protezione degli asset informativi, garantendo standard e livelli di sicurezza adeguati per le piattaforme tecnologiche attraverso la gestione del processo aziendale di ICT Risk Management. Le attività tipiche di IT.TS riguardano, quindi, l'ambito della sicurezza informatica e includono l'analisi delle vulnerabilità, del rischio, degli attacchi esterni e della successiva protezione sia dell'integrità hardware e software dei sistemi, sia dei dati in essi contenuti o scambiati nelle comunicazioni con gli utenti.

Nel mese di marzo del 2013 è stato lanciato il "Programma Strutturato di Sicurezza" (PSS), in risposta alle vulnerabilità rilevate dalla funzione aziendale "Direzione Audit", la quale ha il compito di effettuare audit periodici per individuare le principali criticità relative alla sicurezza. In questo ambito, PSS si pone gli obiettivi di rendere il ciclo produttivo di TI.IT pienamente conforme al processo di ICT Risk Management di Telecom Italia, interamente ripensato nel 2012 ma non ancora adottato dall'intera organizzazione.

Il programma prevede la realizzazione di una serie di attività che eliminino le vulnerabilità rilevate e garantiscano che gli aspetti di sicurezza siano tenuti in considerazione sin dalle prime fasi del ciclo di sviluppo del software. Il team di cui ho fatto parte (composto da altre due laureande) ha affiancato il PM di Technical Security nella pianificazione del PSS, svolgendo le funzioni di Project Management Office (PMO). Per raggiungere l`obiettivo di cui sopra, sono state progettate ed implementate tre tipologie di misure:

- Misure Organizzative
- Misure Tecniche
- Misure di Awareness

Si è reso, anzitutto, necessario definire le misure organizzative con cui gestire il PSS, attribuendone le relative responsabilità, in modo da individuare il quadro di riferimento nel quale poter circoscrivere l'ambito di intervento. Una volta definito l'ambito, sono state progettate le misure tecniche, ovvero tutto l'insieme di attività specifiche che risultavano necessarie per la messa in sicurezza dei sistemi IT. Tali attività sono state suddivise in quattro aree di intervento Patching, Hardening, Sviluppo Sicuro del Codice e Gestione delle Credenziali. Parallelamente, si è deciso di pianificare le misure di awareness per sensibilizzare tutti gli attori coinvolti sull'importanza di manutenere nel tempo la "cultura della sicurezza", ottenendo così una maggiore collaborazione nell'applicazione e nel rispetto dei requisiti di sicurezza. All'interno di questo contesto, l'obiettivo specifico del lavoro di tesi è stato quello di supportare la pianificazione, la messa in campo e il monitoraggio di queste tre misure.

2. METODOLOGIA

Il lavoro si è articolato in tre fasi principali, riportate nel Gantt di Figura 1, ed è stato organizzato secondo le tecniche e gli strumenti del Project Management, in merito ai quali ho seguito un corso di formazione di 32 ore, "Project Management- Preparazione alla certificazione CAPM (Certified Associate in Project Management)", organizzato da Consel- Consorzio Elis.

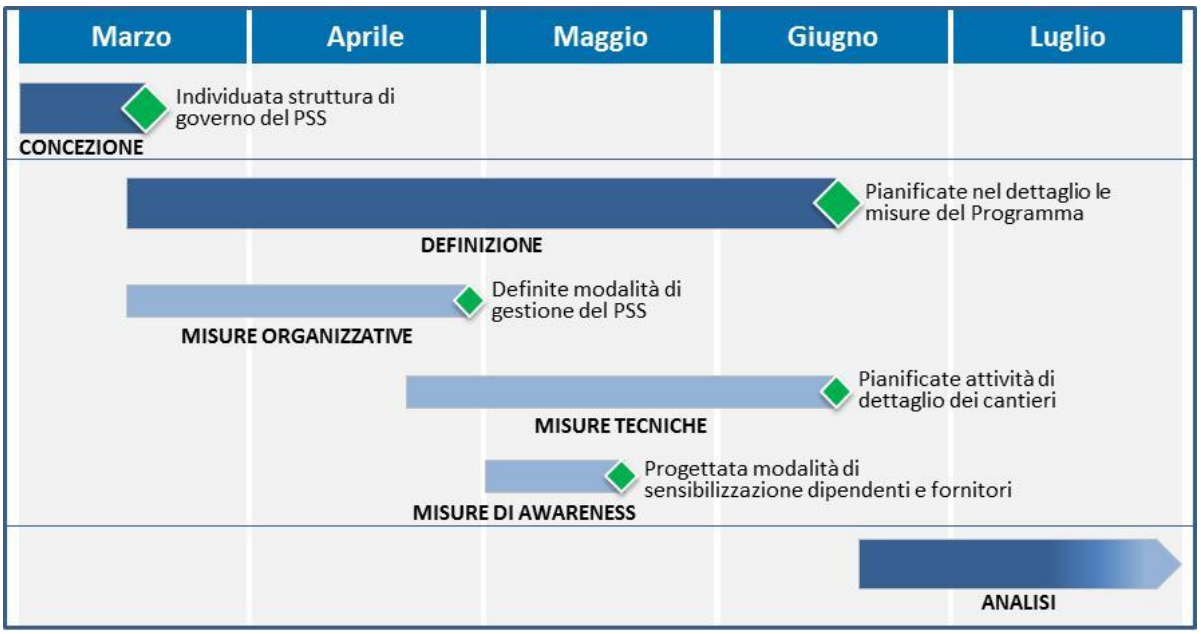

Figura 1 - Gantt delle fasi del PSS

A. Concezione

All'inizio del progetto, è stato necessario avviare una fase in cui venisse definita la struttura del PSS in modo da poter gestire la complessità del lavoro. Per questo sono state svolte le seguenti attività:

- individuazione e definizione delle tre misure, Organizzative, Tecniche e di Awareness, da porre in essere per raggiungere gli obiettivi del PSS;
- riconoscimento delle responsabilità e dei ruoli delle funzioni coinvolte nel PSS;
- identificazione di regole con le quali scegliere i sistemi su cui effettuare le azioni (perimetro teorico d'intervento);
- scelta dell'approccio da adottare.

In Tabella 1 si riportano le modalità con cui sono state attuate le attività di questa fase.

Attività	Modalità di attuazione
Individuazione e definizione delle tre misure	Analisi delle vulnerabilità e dei progetti IT passati (ad es. studio relazione interna su Crash Program)
Riconoscimento dei ruoli e delle responsabilità	Individuazione degli attori aventi le competenze necessarie (studio matrice RACI di Technical Security)
Identificazione del perimetro teorico d'intervento	Identificazione di regole per effettuare la scelta dei sistemi su cui intervenire (analisi criticità dei sistemi IT)
Scelta dell'approccio	Analisi della letteratura

Tabella 1 - Attività fase di concezione

B. Definizione

Dopo aver formalizzato la struttura del PSS, sono state progettate nel dettaglio le tre misure individuate in precedenza:

- **Misure Organizzative:** sono state definite le modalità di gestione delle attività del PSS al fine di facilitare e migliorare l'esecuzione delle attività stesse. Per far questo sono stati revisionati i processi oggetto del Programma, seguendo l'approccio precedentemente stabilito (PDCA). È stato, inoltre, circoscritto il perimetro teorico grazie all'identificazione di "regole di esclusione", definendo in questo modo il perimetro effettivo d'intervento.

- **Misure Tecniche:** in quest'ambito l'attenzione è stata rivolta alle quattro aree di intervento, chiamate "cantieri", ovvero Patching, Hardening, Sviluppo Sicuro del Codice e Gestione delle Credenziali. Per ciascuna di queste, sono state svolte le attività di pianificazione operativa, riportate in Tabella 2, con le relative modalità di attuazione.

Attività	Modalità di attuazione
Definire gli obiettivi	Stima delle percentuali di completamento
Definire i ruoli e le interfacce organizzative	Riunioni aziendali coi responsabili per costruire la matrice di responsabilità
Individuare le attività	Colloqui e riunioni con il gruppo operativo e con i Focal Point delle unità operative
Stimare i tempi di esecuzione delle attività	Interviste e colloqui con il gruppo operativo per stabilire i tempi
Stimare la capacità produttiva	Raccolta ed elaborazione dei dati in un documento Excel da inviare al Demand per la verifica
Definire il budget	Raccolta, elaborazione degli effort e calcolo dei costi tramite il software Microsoft Excel
Sviluppare la schedulazione	Raccolta dei dati e realizzazione del diagramma di Gantt con il software Microsoft Project
Definire un sistema di monitoraggio	Raccolta e centralizzazione delle informazioni e dei KPI da inserire nel database (definizione di Macro classi)
Pianificazione della reportistica	Periodiche riunioni con il team operativo per la preparazione di slide contenenti gli aggiornamenti

Tabella 2 - Attività di pianificazione operativa

- **Misure di Awareness:** parallelamente alla pianificazione delle misure Tecniche, è stato necessario progettare le modalità di condivisione della "cultura della sicurezza" in due direzioni:
  - **Verso i dipendenti**, data la necessità di accrescere il livello di consapevolezza del personale sulle politiche di sicurezza aziendali. La sicurezza deve diventare aspetto centrale della cultura organizzativa, affinché le azioni del PSS non siano vanificate da errori umani, una volta che il Programma sarà concluso.
  - **Verso i fornitori** dei software, data l'assenza di clausole contrattuali omogenee che richiamino gli sviluppatori esterni al rispetto delle politiche di sicurezza di Telecom Italia.

C. Analisi

Nell'ultima fase è stata monitorata l'implementazione delle misure tecniche tramite la formulazione di previsioni, in modo da evidenziare con continuità gli eventuali scostamenti rilevanti dal piano. In Tabella 3 si riportano le principali attività, con le relative modalità di attuazione.

Attività	Modalità di attuazione
Analisi degli scostamenti	Verifica degli scostamenti dalla baseline e dai Gantt per aggiornare le previsioni su costi e tempi
Analisi delle criticità	Evidenza delle criticità tramite analisi su tempi e costi ed elaborazioni di possibili soluzioni
Monitoraggio target e KPI	Monitoraggio tramite grafici Excel del raggiungimento dei target e analisi dei principali KPI dei quattro processi

Tabella 3 - Attività fase di analisi

Il Programma Strutturato di Sicurezza ha **durata triennale** ed è stata pianificata una quarta fase di chiusura per la fine del 2015, che prevede l'entrata a regime delle attività, il rilascio delle risorse impegnate nel progetto, la valutazione del grado di raggiungimento degli obiettivi e l'analisi critica delle attività svolte, al fine di accumulare in modo organico l'esperienza acquisita. Le attività specifiche sotto la mia responsabilità hanno riguardato le aree di Patching e di Hardening e possono essere riassunte in: individuazione del perimetro teorico di intervento (fase A), pianificazione operativa delle attività (fase B) e analisi degli scostamenti (fase C).

3. RISULTATI

3.1 Risultati fase di Concezione

Come precedentemente riportato, il PSS costituisce il piano di riposta alle problematiche emerse dagli audit effettuati, le quali possono essere sintetizzate in tre macro-categorie:

- vulnerabilità dei sistemi informatici da imputare a errori generati in fase di sviluppo del software;
- efficacia parziale dei processi di sicurezza previsti sui sistemi informatici poiché non ripetuti con la giusta frequenza;
- Predicibilità e mancato aggiornamento delle password di alcuni sistemi.

Per eliminare tali vulnerabilità e rendere il ciclo produttivo di TI.IT pienamente conforme al processo di ICT Risk Management è stata necessario individuare tre tipologie di misure: **organizzative, tecniche e di awareness**, riportate nella Figura 2 e che saranno oggetto specifico della fase di definizione.

Figura 2 - Articolazione delle misure del PSS

In seguito, le responsabilità sono state affidate per competenze, assegnando un Project Manager ad ogni cantiere ed un Program Manager a supervisione dell'intero Programma. La struttura di governo del PSS ha affiancato la struttura permanente, di tipo gerarchico-funzionale, di Telecom Italia IT e le attività sono state svolte in parallelo rispetto a quelle tipiche delle diverse unità coinvolte (già a partire dalla fase di concezione, è stato indispensabile coinvolgere, oltre a Technical Security, le funzioni Infrastructure, Demand & Assurance Management, Application Development & Management, Operating Governance e Architecture). In Figura 3 si riporta la Struttura di governo del PSS che è stata definita.

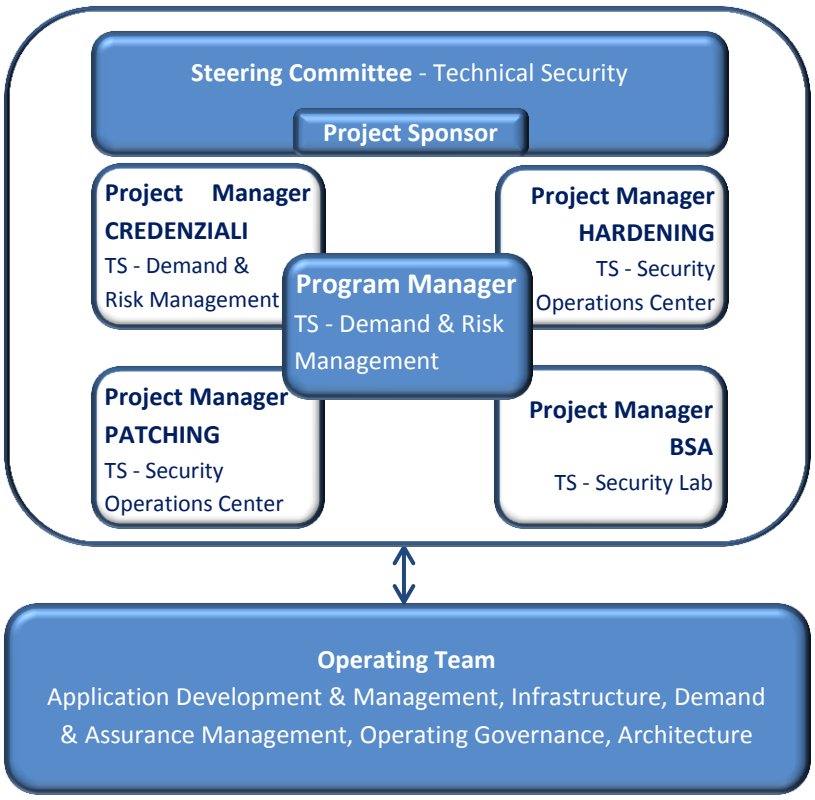

Figura 3 - Struttura di governo del PSS

Uno degli output principali della fase di concezione è stato il "perimetro", cioè l'insieme di sistemi sui quali implementare le azioni previste per i diversi progetti. È stato prima definito un perimetro teorico, dal quale, nella fase successiva, sono stati esclusi i sistemi che non potevano essere oggetto di interventi a causa di vincoli di diversa natura. Il perimetro teorico è stato identificato prendendo in considerazione tutte le applicazioni sulle quali Telecom Italia IT ha responsabilità diretta nel sanare le non conformità riscontrate da Audit, avendo almeno un ruolo in qualità di:

- **Ingegneria:** area che progetta il sistema sulla base dei requisiti provenienti dalla funzione Demand, la quale si occupa di raccogliere i bisogni dei clienti per trasformarli in requisiti funzionali. Le specifiche della progettazione vengono poi inviate alla Software Factory;
- **Software Factory:** area che sviluppa e implementa il codice delle applicazioni, che poi viene inviato alla Gestione Applicativa;
- **Gestione Applicativa**: area che gestisce la fase di esercizio, monitorando il corretto funzionamento del sistema una volta che è stato attivato;
- **Control Room**: area che controlla i server che ospitano le applicazioni.

Alle applicazioni così individuate (circa 2.400) è stato poi associato un ordine di priorità, sulla base di due parametri:

- **Rischio RID** (Riservatezza, Integrità e Disponibilità dei dati trattati): valuta gli impatti di business derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate;
- **Criticità di Business**: valuta l'importanza che un sistema riveste per il funzionamento dei processi aziendali da esso supportati e la compliance dei dati trattati.

In questo modo, sono state identificate quattro zone, ognuna caratterizzata da una priorità di intervento, rappresentate in Figura 4:

Criticità di Business	Criticità RID		
	C1	C2	C3
Mission Critical	8	44	44
Altissima	46	58	62
Alta	143	148	104
Media	140	81	57
Bassa	505	82	174
n.d.	660	7	41
Totale	1502	420	482

Red Zone, composta dalle 482 applicazioni più critiche dal punto di vista della sicurezza;

Yellow Zone, composta da applicazioni caratterizzate da elevata criticità di business;

Green Zone, composta da applicazioni con medio-bassa criticità di business;

Black Zone, composta da applicazioni per le quali non è ancora stata identificata la criticità di business.

Figura 4 - Individuazione delle quattro zone del perimetro teorico

Il PSS ha l'**obiettivo** prioritario di intervenire sulle applicazioni maggiormente esposte a rischio, cioè quelle della Red Zone. Dopo aver trattato questi sistemi, sarà valutata la modalità sostenibile per estendere, anche parzialmente, le azioni dei cantieri alle restanti zone. L'approccio adottato per la pianificazione, realizzazione e monitoraggio delle attività del PSS, segue il ciclo di Deming (Plan Do Check Act), in Figura 5, in modo da garantire non solo la risoluzione delle criticità riscontrate ma anche l'adozione di processi che da nuovi devono diventare routinari, andando a caratterizzare la cultura organizzativa. In questo modo, sarà possibile evitare l'insorgere delle problematiche che attualmente caratterizzano i sistemi e sono all'origine di continue ripianificazioni e di interventi correttivi.

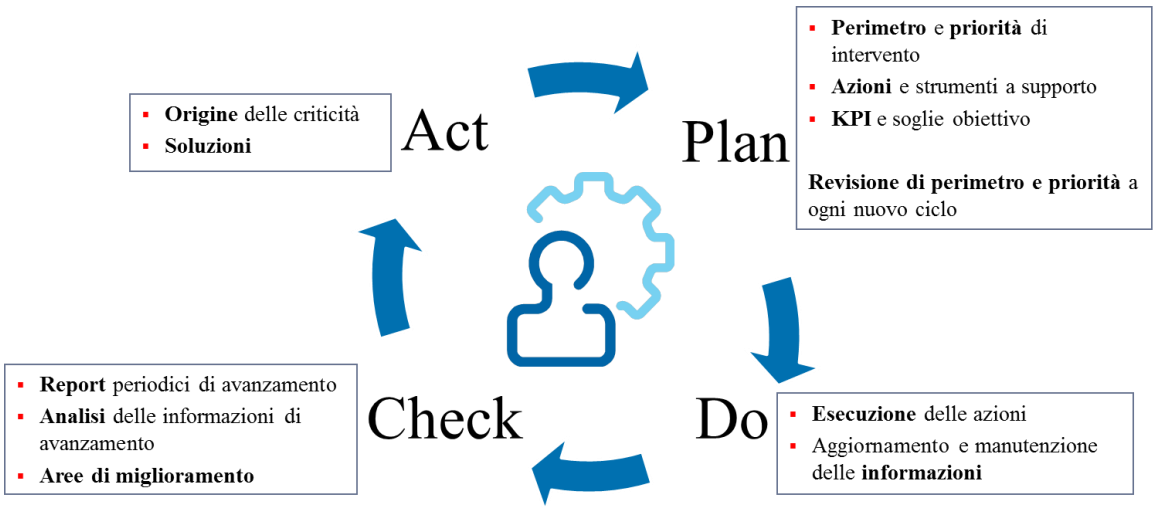

Figura 5 - Schema dell'approccio PDCA adottato

3.2 Risultati fase di Definizione

La fase di definizione è stata quella su cui il lavoro del Project Management Office si è concentrato maggiormente, a livello di misure organizzative, misure tecniche e misure di awareness.

3.2.1 Misure organizzative

Le misure organizzative adottate sono state rivolte principalmente su due fronti:

- **Revisione dei processi** di Patching, Hardening, Business Software Assurance e Gestione delle Credenziali, per conformarsi al nuovo macro-processo di ICT Risk Management, innovato nel 2012. Gli obiettivi per cui sono stati revisionati i quattro processi sono:
  - prevenire i problemi alla fonte, evitando di dover implementare onerose azioni correttive ex post;
  - ridefinire i ruoli all'interno delle diverse fasi del processo, così da responsabilizzare gli attori coinvolti nei diversi stadi del ciclo di sviluppo del software.
- **Definizione e revisione periodica del perimetro di intervento**. Si è provveduto a individuare l'effettivo numero di sistemi da trattare, a partire dal perimetro teorico costituito dalle 482 applicazioni della Red Zone. L'attività è risultata particolarmente critica, dal momento che le informazioni sui sistemi sono in costante aggiornamento e risiedono su cataloghi diversi, non sempre allineati tra loro. Data la continua evoluzione dei sistemi e in accordo con l'approccio PDCA, sono state pianificate due milestone (all'inizio del 2014 e all'inizio del 2015) per revisionare il perimetro di intervento alla luce delle modifiche sui cataloghi.
  Per definire il perimetro di intervento sono state adottate alcune regole di esclusione che saranno applicate anche in occasione delle due revisioni:
  - **Responsabilità delle azioni**: dal perimetro target sono escluse le applicazioni per cui Telecom Italia Information Technology non riveste il ruolo di responsabile;
  - **Vincoli tecnologici**: dal perimetro target sono esclusi i sistemi su cui non è possibile effettuare le azioni a causa di problemi tecnici di varia natura;
  - **Impatti di intervento**: dal perimetro target sono escluse le applicazioni su cui devono essere implementate azioni per cui la valutazione costi/benefici risulta particolarmente sfavorevole (ad esempio applicazioni in dismissione).

3.2.2 Misure tecniche

In questo ambito, la fase di definizione ha riguardato le quattro aree di intervento pensate per rispondere alle criticità tecniche rilevate da Audit sui sistemi informatici:

Patching: L'obiettivo del Patching è ridurre i bug di sicurezza che vengono generati a ogni aggiornamento del software a causa di errori di scrittura del codice sorgente e malfunzionamenti. Il processo è effettuato installando sui server file eseguibili chiamati patch (letteralmente "pezze"), creati per risolvere gli specifici errori di programmazione. La prassi di Telecom Italia prevede che il processo di patching sia effettuato almeno una volta all'anno, ma dalle rilevazioni di Audit è emerso che questa frequenza spesso non viene rispettata, esponendo i sistemi a potenziali attacchi esterni;

Hardening: L'obiettivo dell'hardening è minimizzare il numero di servizi aperti su un dato server, attraverso una sua idonea configurazione, in modo da ridurre il rischio connesso ad un attacco esterno. Il processo inizia con la selezione e la compilazione di Checklist, ovvero configurazioni specifiche che, se applicate correttamente, garantiscono la sicurezza del sistema in esame. Una volta identificate le Checklist idonee, le configurazioni indicate vengono implementate sul sistema. Audit ha rilevato un elevato numero di vulnerabilità dovute alla mancata o errata compilazione delle Checklist di hardening;

Gestione delle credenziali: L'obiettivo è rendere le credenziali di accesso (username e password) conformi alle policy di sicurezza aziendale, in modo da evitare l'accesso di entità non autorizzate sui sistemi. Audit ha rilevato la presenza di password predicibili, banali o non cifrate, che espongono i sistemi ad un elevato rischio di attacchi esterni;

Sviluppo sicuro del codice (Business Software Assurance): L'obiettivo è rilevare ed eliminare le vulnerabilità che si generano in fase di scrittura del codice sorgente, servendosi del supporto di uno strumento automatico. Tale strumento è già utilizzato all'interno di Telecom Italia IT in fase di controllo finale del codice ma, data la numerosità degli errori originati durante lo sviluppo del software, risulta opportuno utilizzare lo strumento a monte del processo di scrittura, in modo da prevenire l'insorgere delle vulnerabilità senza doverle correggerle ex post.

Per ogni cantiere, sono state svolte attività di pianificazione necessarie al conseguimento degli obiettivi, in un ottica PDCA. In particolare il team si è occupato delle attività riportate in Tabella 4.

Definire gli obiettivi	Per ogni sotto-progetto sono stati determinati dei valori target, espressi come percentuali di completamento delle attività, da raggiungere alla fine di ogni anno. Tali target costituiscono la base per il monitoraggio degli avanzamenti, in termini di tempi e risorse stanziate
Definire i ruoli e le interfacce organizzative	Ciascun Project Manager ha costituito il proprio team di lavoro e definito la matrice delle responsabilità, identificando i collaboratori interni o esterni a Telecom. Anche all'interno del PMO, ogni team member è stata assegnata a uno specifico progetto (nel mio caso, quello relativo al Patching & Hardening) per aiutare la raccolta e l'elaborazione delle informazioni provenienti dai diversi cantieri. Inoltre sono stati designati i Focal Point per ciascuna funzione coinvolta nel Programma, i quali sono stati incaricati di interfacciarsi con i referenti operativi
Individuare le attività	Sono state identificate le attività di dettaglio necessarie per il raggiungimento degli obiettivi. Per avere una visione di insieme degli obiettivi e dei deliverable associati ai diversi progetti, le attività sono state organizzate nella Work Breakdown Structure.
Stimare i tempi di esecuzione delle attività	Per la stima è stata di fondamentale importanza la collaborazione con le funzioni incaricate di intervenire a livello operativo sui sistemi (Demand, Ingegnerie, Control Room, Gestione Applicativa)
Stimare la capacità produttiva	Collaborando con le Ingegnerie, si è andati a stimare la capacità produttiva necessaria per il completamento di tutte le azioni. Quindi, è stata confrontata tale capacità produttiva (teorica) con quella effettivamente disponibile all'interno delle unità operative
Definire il budget	In funzione degli effort disponibili, è stato definito il budget da allocare alle attività. È stata stimata la baseline per i tre anni di svolgimento del PSS, utilizzata nella successiva fase di analisi per controllare gli scostamenti dal pianificato.
Sviluppare la schedulazione	Le attività di dettaglio sono state declinate sui tre anni di svolgimento del PSS e sono stati definiti i diagrammi di Gantt di ciascun progetto
Definire un sistema di monitoraggio	Per controllare con continuità e dare evidenza ad Audit dell'esecuzione delle attività dei progetti, è stato progettato un tool di monitoraggio, gestito da Technical Security ma accessibile dai responsabili delle funzioni coinvolte nel PSS. Il monitoraggio ha interessato, da un lato, i tempi e i costi del Programma, dall'altro, l'effettiva esecuzione delle azioni pianificate e i KPI dei processi
Pianificazione della reportistica	Per allineare i diversi cantieri durante le fasi di definizione e realizzazione, si è deciso di programmare per ogni settimana un SAL interno alla funzione Technical Security. Si è optato per un orizzonte settimanale a causa della complessa articolazione del PSS e del numero di soggetti interessati allo svolgimento delle attività. I report di avanzamento commentati ai SAL sono stati condivisi con Audit in incontri pianificati con cadenza mensile

Tabella 4 - Attività di pianificazione di dettaglio dei cantieri del PSS

3.2.3 Misure di awareness

Per condividere e diffondere la "cultura della sicurezza" **verso i dipendenti**, sono state pianificate le seguenti attività:

- **Comunicazione** formale (via email) delle "golden rules" della sicurezza, un elenco di regole che dovrebbero essere osservate dai dipendenti coinvolti nelle attività di Telecom Italia IT;
- **Formazione**: definizione di percorsi formativi rivolti al personale interno, costituiti da corsi in aula e online riguardanti il processo di Risk Management e gli strumenti a supporto della sicurezza dei sistemi aziendali. In particolare, è stato realizzato un modulo formativo

dedicato al rispetto delle password policy aziendali da inserire in tutti i corsi di formazione in aula, a prescindere dallo specifico contesto formativo.

- **Informazione continua**: realizzazione di un'area dedicata al processo di ICT Risk Management sulla Intranet aziendale, da mettere in evidenza con periodicità definita;

Per quanto riguarda la sensibilizzazione **dei fornitori**, sono state pianificate attività di:

- richiamo formale alla stretta osservanza delle policy di sicurezza rivolto a tutti i fornitori di TI.IT;
- revisione degli schemi contrattuali in essere al fine di indirizzare correttamente il processo di Risk Management.

3.3 Risultati fase di Analisi

Le attività pianificate sono state avviate nella seconda metà del 2013. In questa fase, è stato determinante monitorare la loro esecuzione dal punto di vista dei costi e dei tempi, al fine di individuare le criticità e i vincoli che si presentavano e implementare opportune azioni correttive.

3.3.1 Analisi degli scostamenti di tempo e di costo

Nei primi mesi di svolgimento del PSS, si sono presentate due principali **problematiche**:

- **Ritardo nella definizione del perimetro di intervento**, a causa delle difficoltà riscontrate nel reperire informazioni esaurienti relative ai sistemi. Queste difficoltà sono da ricondurre a due aspetti principali:
  - Informazioni contenute in cataloghi diversi, non sempre allineati tra loro, né costantemente aggiornati;
  - Scarsa collaborazione dei referenti operativi delle funzioni esterne a Technical Security impegnate sul Programma Strutturato di Sicurezza. Le azioni del PSS sono state viste, in certi casi, come di ostacolo alle altre attività operative e talvolta le informazioni sono pervenute ai Project Manager con mesi di ritardo, nonostante i ripetuti richiami formali.

  Soluzione: data la necessità di avviare quanto prima le attività dei diversi progetti, si è deciso di modificare l'approccio (basato su una logica di priorità) con cui selezionare le applicazioni da trattare. Infatti, non è stato possibile definire nei tempi previsti un ordine di priorità di intervento per i sistemi della Red Zone. Pertanto, si è stabilito di trattare quanto prima un insieme di applicazioni (chiamato "package") per le quali le unità operative avevano fornito i dati necessari in tempi rapidi.

- **Informazioni sui diversi progetti disallineate**, data la complessità dell'ambiente multi-project e l'elevato numero di interdipendenze presenti. I soggetti impegnati sul PSS (i quattro Project Manager con i rispettivi team di lavoro) hanno manifestato la necessità di accedere in maniera più diretta alle informazioni degli altri cantieri e di standardizzare la documentazione associata. Uno dei compiti principali del PMO è stato rivolto in questa direzione, anche al fine di fornire informazioni di tipo aggregato su tutto il PSS.

  Soluzione: per rispondere a questa criticità, si è pensato di estendere le funzioni del sistema di monitoraggio, identificato nella fase di definizione, in modo da utilizzarlo anche come strumento di reporting. Il tool progettato è diventato una base di dati a cui i Project Manager possono accedere a tutte le informazioni sui progetti del PSS e aggiornare i dati relativi al proprio cantiere. Interrogando il database, è inoltre possibile disporre di viste aggregate su tutto il Programma, al fine di effettuare analisi su tempi, costi e stato dei sistemi oggetto degli interventi di sicurezza.

In seguito all'analisi dei costi, è stato possibile calcolare il costo unitario di ciascuna tipologia di interventi, dividendo i costi effettivi per il numero di attività realizzate. Da questo calcolo è derivata un'importante considerazione: su tutti i cantieri le stime iniziali erano state sovradimensionate rispetto al costo reale. Pertanto, i responsabili dei team di progetto, in accordo con lo Steering Committee, hanno deciso di **tagliare il budget del 2014 del 30%**.

3.3.2 Monitoraggio dei target e dei KPI

A partire dal mese di settembre è stato costantemente monitorato il numero di interventi realizzati sui cantieri, allo scopo di controllare l'effettivo raggiungimento degli obiettivi di fine anno. Per disporre di una visione più esaustiva sui risultati raggiunti dal PSS e sulla diffusione dei nuovi quattro processi, è stato monitorato l'andamento dei relativi indicatori di prestazione (efficienza, non conformità, incidenza dei vincoli). Si è ritenuto, infatti, che la buona riuscita del Programma non fosse influenzata esclusivamente dal raggiungimento dei target, ma anche dall'efficacia e dall'efficienza dei nuovi processi, la cui diffusione nell'organizzazione rientrava tra le responsabilità dei team di progetto.

4. CONCLUSIONI E SVILUPPI FUTURI

Al termine del 2013 è stata realizzata una valutazione dell'andamento generale del PSS. L'implementazione di una due attività relative alle **misure organizzative** (ovvero la definizione del perimetro d'intervento) non è stata conclusa in tempo, ritardando l'avvio dell'esecuzione degli interventi previsti dalle **misure tecniche**. Il problema è stato risolto grazie alla definizione della logica "di package" che, insieme alla centralizzazione delle informazioni in un DB condiviso, ha garantito il raggiungimento degli obiettivi target su tre delle quattro aree. Il cantiere di Hardening ha incontrato maggiori difficoltà, dettate dalla complessità della tipologia delle sue azioni, e pertanto è stata prevista una rimodulazione del suo target per il 2014. Le **misure di awareness** hanno contribuito alla sensibilizzazione dell'importanza della cultura della sicurezza verso i dipendenti ed i fornitori di software.

In ultima analisi, si evidenziano i benefici che il team di progetto, in veste di PMO, ha apportato alla pianificazione e all'implementazione di successo del Programma:

- Sostegno alla fase di definizione del perimetro d'intervento, grazie alla raccolta, analisi ed elaborazione dei dati e delle informazioni provenienti dai quattro progetti;
- Miglioramento della comunicazione e maggiore trasparenza dei dati scambiati tra i team operativi e il Program Manager, grazie alla centralizzazione delle informazioni in un unico strumento condiviso;
- Monitoraggio dello schedule delle attività con il quale sono state evidenziate, analizzate e prontamente risolte le criticità, senza compromettere il raggiungimento dei target;
- Monitoraggio del consumo di risorse e del rispetto dei costi stimati, mediante il quale è stato evidenziato un sovradimensionamento del budget;
- Miglioramento del reporting verso il management di alto livello sullo status del PSS, grazie alla definizione di una reportistica standard e condivisa.

A partire dal 2016, terminato il raggio di azione del Programma Strutturato di Sicurezza, si prevede di estendere le azioni alle applicazioni appartenenti alle altre zone (Yellow, Green e Black) e di convogliare tutte le informazioni in un unico catalogo IT, al fine di bonificare tutti i sistemi dell'azienda. Inoltre sono previsti ulteriori corsi di formazione per far sì che questo Programma non rimanga circoscritto nell'ambito delle funzioni coinvolte, ma si possa diffondere a tutti i livelli organizzativi, applicando concretamente le *best practice* del processo di ICT Risk Management.