ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Gestire progetti di Ethical Hacking secondo le best practice di Project Management e Security Testing

Simone Onofri
Claudia Spagnuolo

Roma 25/02/2014

Relatori

Simone Onofri

simone.onofri@techub.it

Claudia Spagnuolo

claudia.spagnuolo@yahoo.it

Agenda

A. Introduzione al Project Management e ai Progetti di Security Testing

B. Esempio di un Progetto di Security Testing (fasi di pre-progetto, inizio, consegna, post-progetto)

C. Conclusioni

Agenda

Parte A - Introduzione al Project Management e ai Progetti di Security Testing

Cos'è un Progetto?

Il Progetto è un **organizzazione temporanea**,
che viene creata con lo scopo
di **consegnare uno o più**
prodotti specialistici.

*Esempi di prodotti di progetto: una applicazione **software**,*
*un **report** di valutazione delle vulnerabilità*

La definizione è liberamente ispirata a
PRINCE2®

Cos'è il Project Management?

E' un insieme di attività *strutturato* volto a **pianificare**, **delegare**, **monitorare** e **controllare** i vari aspetti del progetto per raggiungere

gli obiettivi stabiliti.

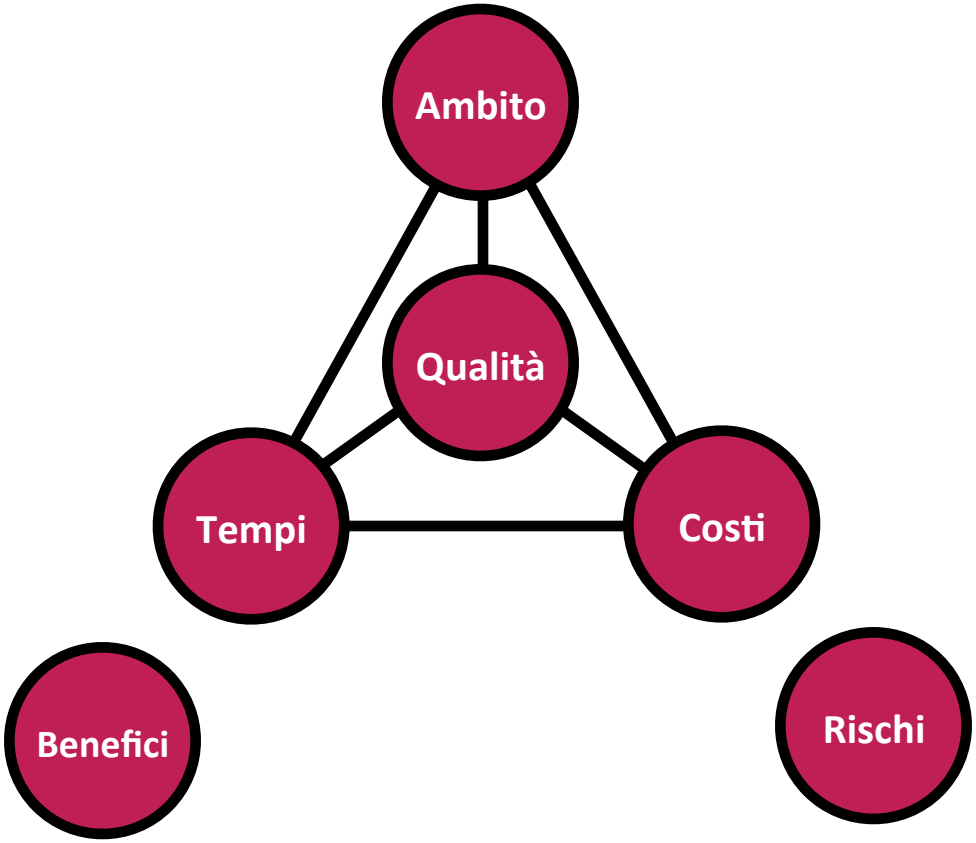
E' compito del responsabile di progetto tenere sotto controllo le sei variabili di progetto:

tempi, costi, ambito, qualità, rischio e benefici.

La definizione è liberamente ispirata a PRINCE2®

Variabili di progetto e performance

Mantenere le variabili di progetto all'interno delle tolleranze stabilite (p.e. qualità concordata) garantisce di conservare **elevati livelli di performance per progetto**



Valutazione della sicurezza delle informazioni

"**Determinare** quanto efficacemente un **sistema**, **applicazione** o più in generale un **servizio** **soddisfa** gli **obiettivi di sicurezza**"

La definizione è liberamente ispirata a al NIST SP800-115

Le best practices

Esistono molte Best Practices, buone
prassi consolidate dall'esperienza,
sia per il Security Testing
sia per il Project Management.
Ne vediamo alcune.

PRINCE2® (Projects in a Controlled Environment*), UK

PRINCE2® è un **metodo di gestione progetti** del governo inglese, standard *de-facto* basato sull'esperienza di migliaia di progetti. E' adattabile ad ogni ambito e si concentra sugli aspetti gestionali.

* Oggi PRINCE2® è un marchio registrato della AXELOS Limited.

OSSTMM è un manuale dell'ISECOM che descrive una **metodologia** per l'esecuzione di test di sicurezza in differenti ambiti. Prevede anche elementi relativi alla pianificazione e alle regole di ingaggio. Si utilizza di solito per i **Network Penetration Test** e i **Wireless Penetration Test**.

OWASP (Open Web Application Security Project), USA

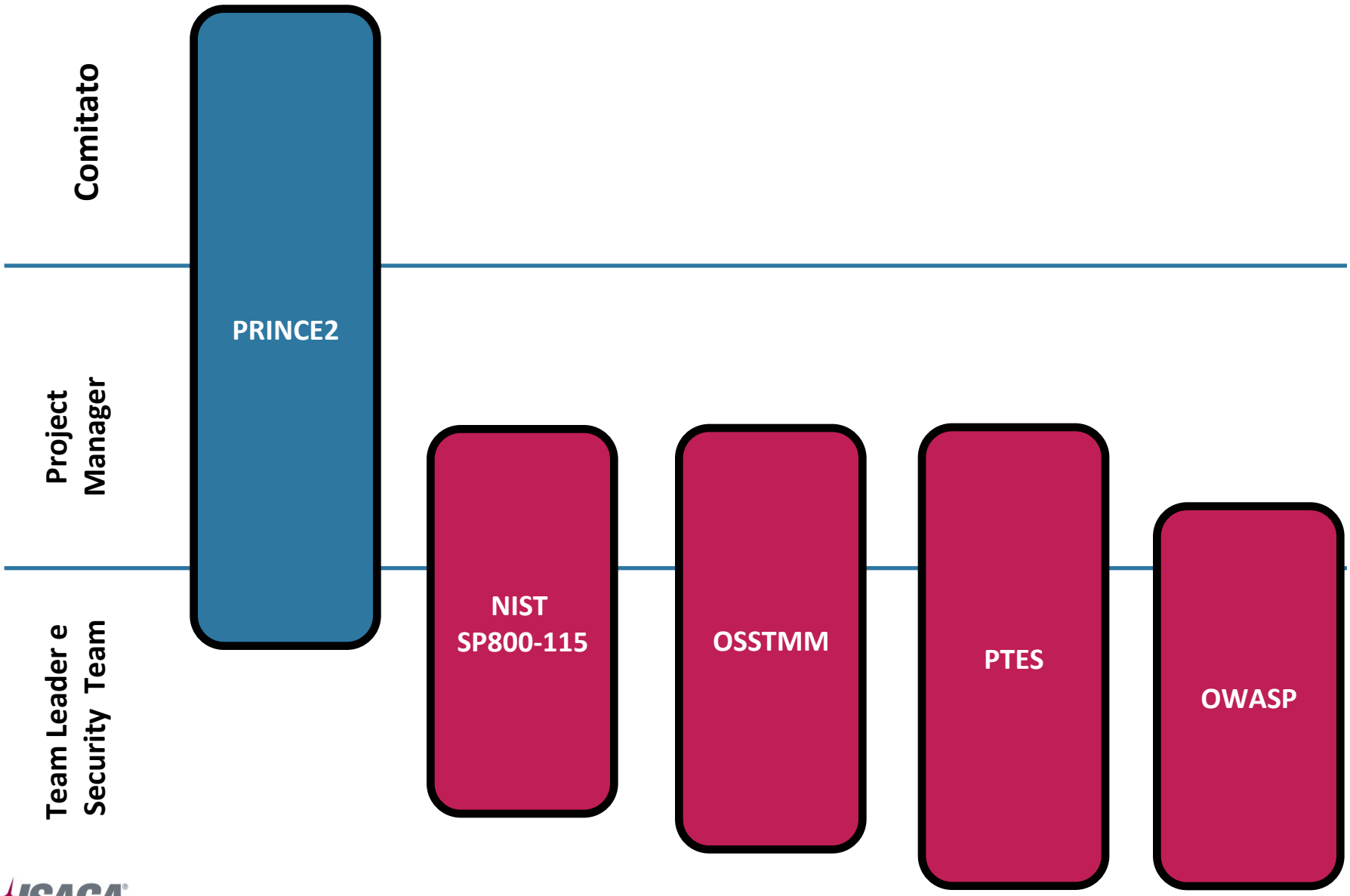
OWASP è un'organizzazione indipendente dedicata alla creazione e alla diffusione di una "cultura della sicurezza delle applicazioni web". Ha redatto la **Testing Guide**, una guida per la valutazione della sicurezza delle Applicazioni Web. Si utilizza di solito per i **Web Application Penetration Test**.

Il **NIST** è un istituto del Ministero del commercio americano che si occupa di standard e tecnologie.
La **SP 800-115** del NIST descrive le raccomandazioni per il Testing e l'Assessment per la Sicurezza delle Informazioni. Si utilizza di solito per i **Vulnerability Assessment** e per stabilire un **Programma** dei Test.

Il **PTES** è uno standard de-facto per l'esecuzione di Penetration Test scritto da un gruppo di professionisti. Si occupa sia della pianificazione che degli aspetti tecnici. Si utilizza di solito per i **Network Penetration Test** e **Wireless Penetration Test**.

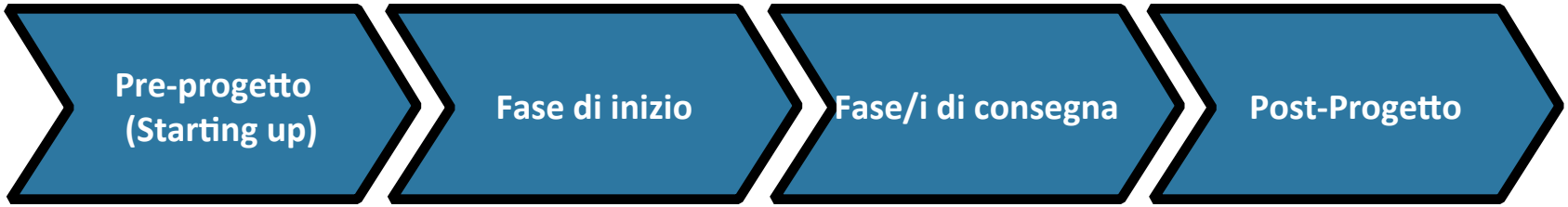
Possiamo integrare
le Best Practice di Security Testing
con quelle utilizzate per
gestire il progetto?

Combinare differenti Best Practice



Come utilizziamo PRINCE2 in un progetto di Security Testing?

Applichiamo PRINCE2 a un progetto di Security Testing



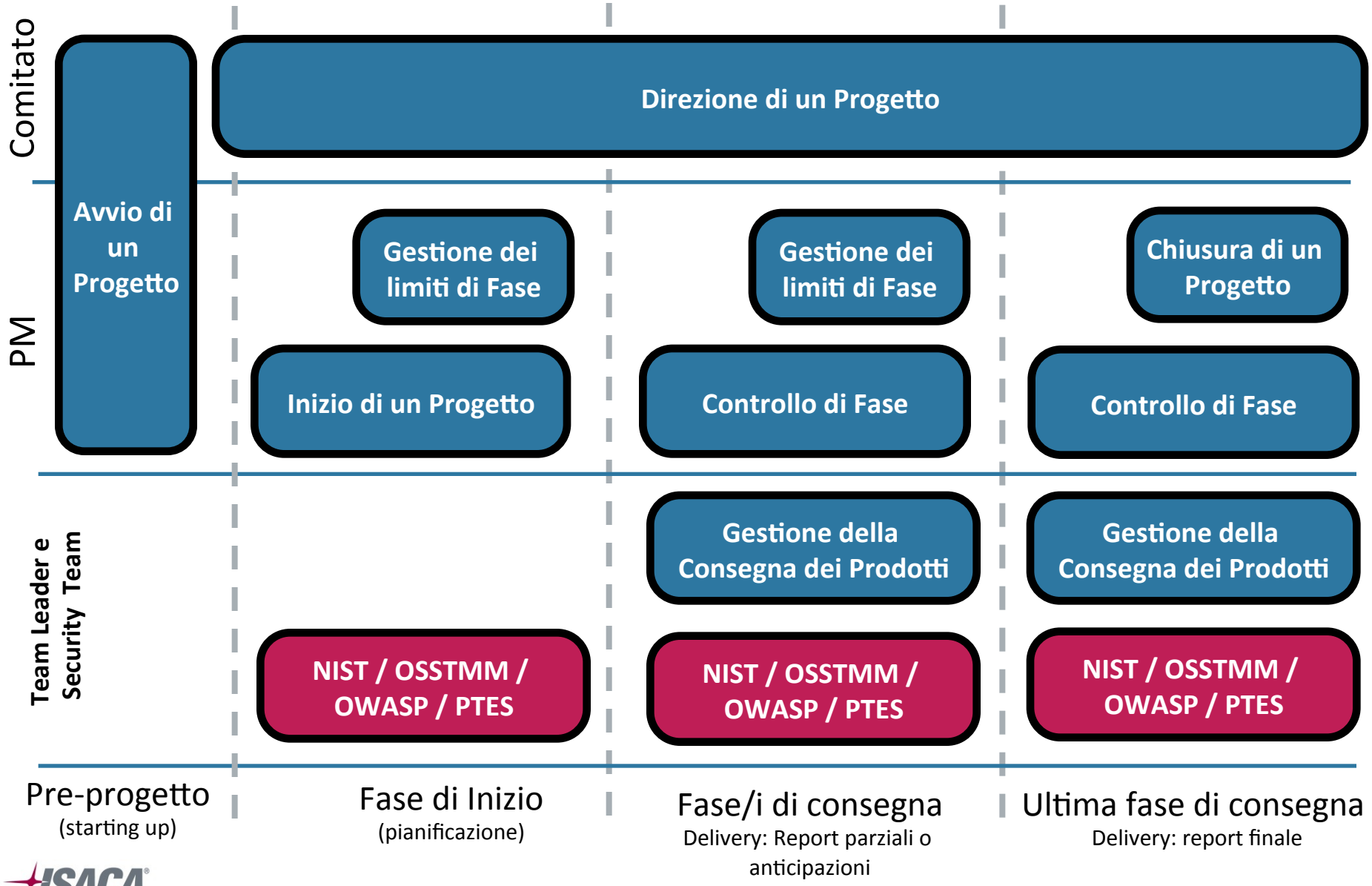
- Stesura del Business Case preliminare : definizione della necessità e dei benefici che il committente desidera conseguire
- Raccolta dei requisiti di alto livello, cioè non eccessivamente dettagliati

- Pianificazione
- Documentazione: scelta dei template, identificazione della documentazione necessaria e relativa redazione (se non abbiamo tutte le informazioni solo in versione preliminare)

- Verifica delle condizioni di ingresso
- Svolgimento attività tecnica secondo l'ambito e l'approccio definito
- Produzione Reportistica
- Presentazione e accettazione del prodotto di progetto

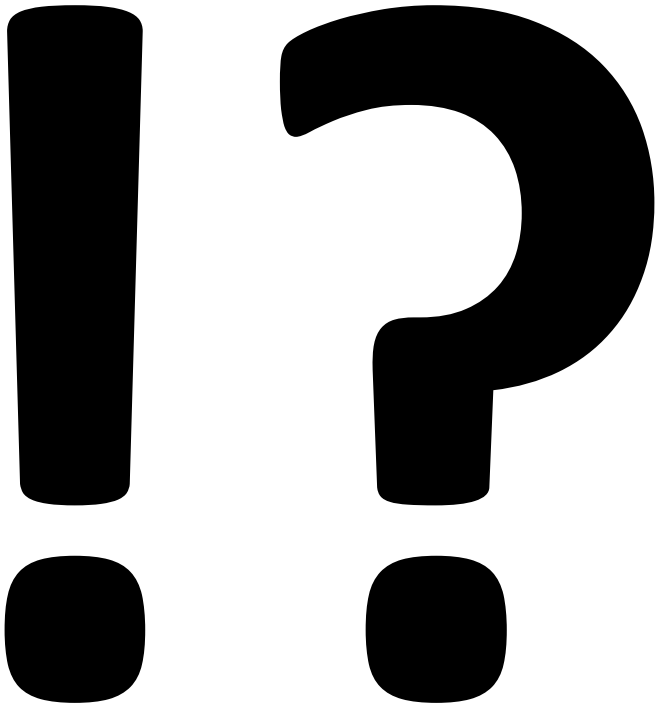
- Azioni post-progetto consigliate e verifica dei Benefici (p.e. attività di re-test, azioni di rientro per ridurre le vulnerabilità)

Come strutturare un progetto di Security Testing con le BP



ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

DOMANDE?



Agenda

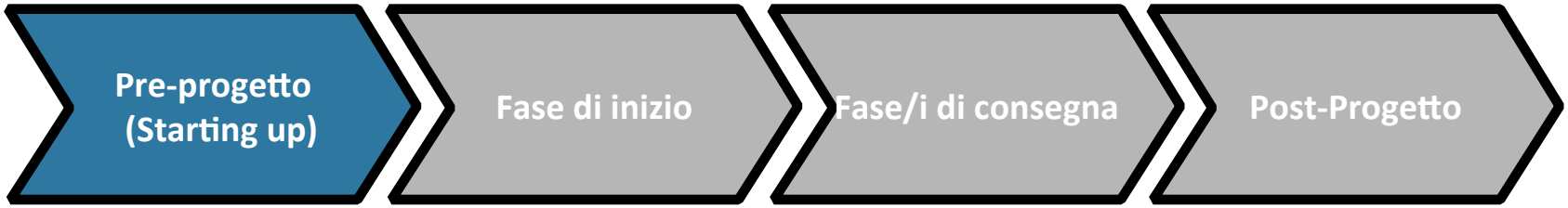
Parte B - Esempio di un progetto di Security Testing

In questo modulo vediamo come si può sviluppare in fasi un progetto di Security Testing.

Andiamo a vedere in dettaglio cosa
accade nelle 4 fasi che abbiamo visto in precedenza:

- Pre-progetto
- Fase di Inizio
- Fase/i di consegna successive
- Post-progetto

Agenda



Pre-progetto (fase di 'Starting up')

- Il Business Case e il Project Brief
- Il Prodotto di Progetto
- Le informazioni da raccogliere (requisiti di alto livello)
- Top Tips

Fase di pre-progetto (starting up del progetto)

L'input è il **mandato di progetto**, può essere una telefonata, una e-mail, un incontro o un accordo commerciale.

Il **pre-progetto** è la fase di 'starting up' in cui il progetto viene solo avviato ed ha lo scopo di verificare ad alto livello la sua **validità** e **fattibilità.**

Uno degli output principali è il **Business Case** che verrà inserito, insieme ad altra documentazione ritenuta rilevante, in un 'faldone' chiamato **Project Brief**. Questi documenti di gestione sono la base per la fase successiva in cui si 'costruirà' la struttura di controllo del progetto.

Mandato di progetto: quali sono le necessità?

Perché si da il **mandato** per avviare un progetto di Security Testing? Le necessità possono essere molteplici.
Di solito i **driver/necessità di progetto** caratteristici sono:

- **Compliance** a Leggi, Norme e Regolamentazioni (es. ISO 27001, PCI-DSS)

- **Gestione del Rischio per difendere il business** (es. garantire che dati, infrastrutture e applicazioni siano sufficientemente sicure)

Cosa contiene il Project Brief?

Il **Project Brief** è un faldone che contiene **definizione** e **scopo** del progetto, obiettivi, **Business Case** (preliminare), **Descrizione del Prodotto del Progetto**, **Approccio**, Struttura del **Team** e **Ruoli**. Può venir aggiunta altra documentazione se ritenuta rilevante, p.e. il manleva firmata da cliente e fornitore.

Vedremo ora i documenti di gestione peculiari: Business Case, Descrizione del Prodotto del Progetto e Struttura del Team

Business Case - Obiettivo

Uno dei princìpi di PRINCE2® indica che ogni progetto deve avere "**giustificazione commerciale continua**", questo vale anche per il Security Testing.

La giustificazione è contenuta nel documento di gestione che si chiama **Business Case** che deve rispondere alla domanda:

vale la pena di iniziare il progetto?

Business Case - Contenuto

Un **riepilogo** esecutivo, i **motivi**, le **opzioni** commerciali, i **benefici** e i **controbenefici**, **tempi**, **costi**, valutazione dell'**investimento** e **rischi** principali.

*La **sicurezza è un investimento!!!***

*Le ricerche dimostrano che ha un **ROI** che va **dal 5% al 21%***

Business Case – Esempio (estratto)

- **Identificativo documento:** CodCliente_CodProg_CodDoc_Ver
- **Riepilogo Esecutivo:** Raccomandiamo di eseguire le valutazioni di sicurezza per le 10 applicazioni già identificate come critiche ed esposte su internet per clienti terzi. Così da aumentare il livello di sicurezza generale ed essere compliant.
- **Motivi:** Essere ragionevolmente certi che le applicazioni siano sicure e protetti dai danni di immagine.
- **Opzioni Commerciali:**
  - Non fare nulla: rimanere consapevoli dell'esposizione a potenziali danni economici e d'immagine e alla potenziale perdita di clienti.
  - Fare il minimo: controllare solamente le applicazioni più critiche.
  - Fare qualcosa: mettere in sicurezza le applicazioni esistenti e stabilire un ciclo di sviluppo e implementazione sicuro di applicazioni e sistemi.
- **Benefici:**
  - Riduzione dell'80% delle vulnerabilità attuali già dopo il primo mese dalla messa in produzione.
  - Riduzione del 50% dei costi di risoluzione degli incidenti informatici rispetto all'anno passato.
- **Controbenefici:** Non sarà possibile modificare le applicazioni durante i test. Tempi più lunghi per il rilascio in produzione
- **Rischi Principali:**
  - Un rischio è che siano divulgate le informazioni riservate come risultato di disattenzione del personale o compromissione/furto dei sistemi, con l'effetto di perdita d'immagine ed economica. Pertanto sarà richiesta la firma di un "Patto di Riservatezza" e le attività si svolgeranno solo su sistemi interni.
  - Un rischio è che il personale esterno non sia abbastanza abile nell'identificare le problematiche come risultato di scarsa preparazione, con l'effetto di non identificare tutte le vulnerabilità. Pertanto saranno richieste nella gara certificazioni riconosciute a livello internazionale relative ai test di sicurezza e il curriculum dettagliato che garantisca sufficiente esperienza nel campo della sicurezza.

Business Case – Esercizio (15 minuti)

Scenario: Una grande azienda vuole essere ragionevolmente certa che le sue applicazioni siano sicure per evitare danni d'immagine o perdite economiche.

Scrivere il Business Case.

Riepilogo esecutivo: in breve, quali sono i benefici e il ritorno sull'investimento?
Motivi: perché intraprendere il progetto?

Opzioni commerciali: quali sono le opzioni analizzate (non fare nulla, fare il minimo o fare qualcosa)?
Benefici: quali sono i risultati positivi e misurabili che mi aspetto del progetto?
Contro-benefici: quali sono i risultati percepiti come negativi, generati dal progetto?

Tempistica: quali sono le tempistiche del progetto?
Costi: Quali sono i costi del progetto?
Valutazione dell'investimento: qual'è il rapporto tra costi, benefici e contro-benefici?
Rischi principali: Quali sono i rischi principali correlati al progetto?

Business Case – Top Tips

- Il Cliente e il Fornitore hanno **due Business Case differenti.**
- Il Business Case del fornitore prevede solitamente il ritorno economico; oppure lavora in perdita per poter **acquisire nuovi Clienti** e/o **segmenti di mercato**.
- I due Business Case dovrebbero essere **compatibili**.

Descrizione del Prodotto di Progetto - Obiettivo

Quando si decide di fare un progetto (anche di Assessment) va definito anzitutto **cosa ci aspetta dal progetto** e **cosa dovrà rilasciare**. PRINCE2® fornisce un prodotto di gestione con questo scopo: la **Descrizione del Prodotto di Progetto**

Descrizione del Prodotto di Progetto - Contenuto

Se il Prodotto di Progetto è un **report** che documenta i risultati dell'Assessment, la Descrizione contiene le informazioni che lo descrivono, come l'**obiettivo**, la **composizione**, la **derivazione** (da dove provengono le informazioni), le **competenze** richieste per portare a compimento il progetto, le *aspettative* di **qualità** e le relative *tolleranze*. Ultimo ma non meno importante il *metodo* e le *responsabilità* per l'**accettazione**.

Descrizione del Prodotto di Progetto - Qualità

La **qualità** (le caratteristiche/requisiti) che deve avere il risultato e gli standard da seguire sono elementi influenzano molto la **quantità di lavoro relativo costo**.

*(p.e. utilizzo di standard quali **OSSTMM** e **OWASP** o il calcolo del punteggio tramite **CVSS v2**)*

Esempio di Composizione del Report di Security Testing

PTES consiglia di strutturare il report **su più livelli**, uno di alto livello che si focalizza sugli impatti e sintetizza i risultati e uno di approfondimento tecnico che specifica i risultati e propone soluzioni. L'OSSTMM consiglia di includere sempre le informazioni di Contesto.

- Obiettivo ed organizzazione del documento
- Approccio e Metodologia
- Contesto (p.e. bersaglio e periodo della valutazione)
- Sintesi esecutiva
- Dettagli tecnici
- Legenda

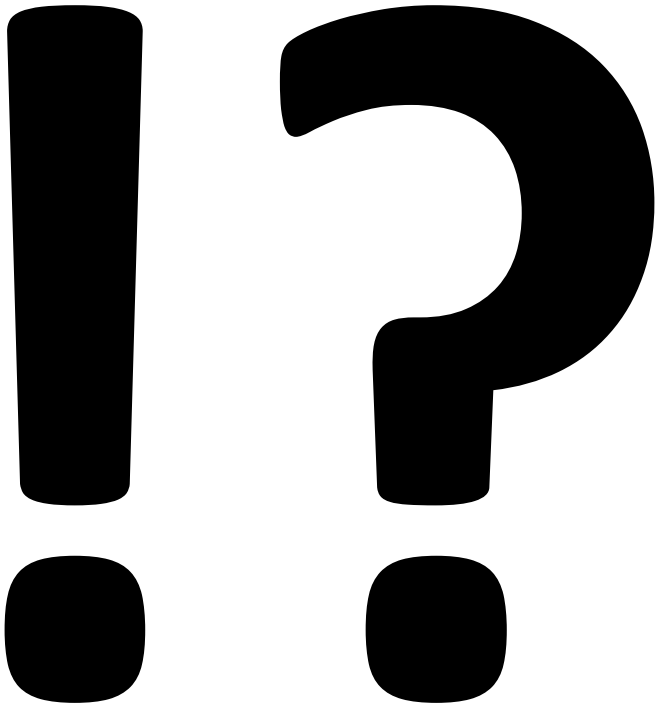
Nota: il Cliente potrebbe chiedere un report personalizzato

Top Tips – Promemoria giornaliero

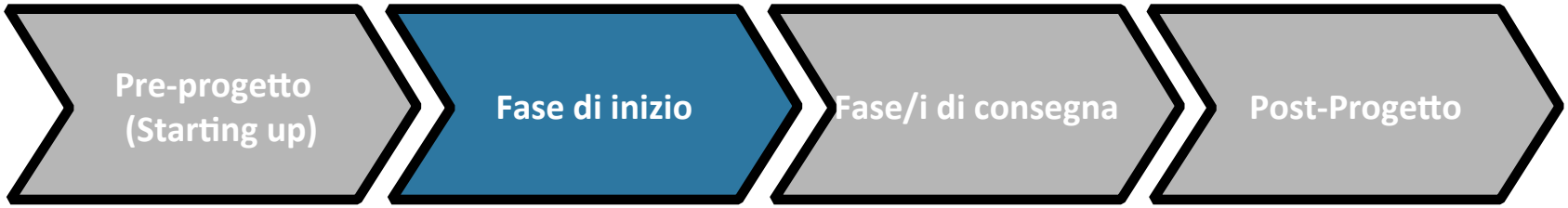
La **prima attività** di gestione da fare quando si viene nominati Project Manager è creare il proprio **Promemoria Giornaliero**, il "diario di bordo" che contiene tutte le informazioni rilevanti.

Data di Inserimento	Problema, azione, evento o commento	Persona Responsabile	Data obiettivo	Risultato
2012-12-XX	Richiesta di informazioni da <Referente Cliente>	Simone	2012-12-XX	Pianificare Riunione
2012-12-XX	Richiesta per attività relativa a <Attività>	Simone	2012-12-XX	Stima spannometrica

DOMANDE?



Agenda



Fase di Inizio

- Requisiti
- Stima
- Piano di Progetto
- Manleva e Regole di Ingaggio

L'inizio: Inizio di un Progetto e Limite di Fase

L'*input* è il **Project Brief**.

La *fase* si struttura in due processi: l'*Inizio di un Progetto che* ha lo scopo di impostare la **solide basi** per l'intero progetto; la *Gestione del Limite di Fase* si occupa di verificare lo stato della fase precedente, pianificare quella successiva e fornisce un **momento decisionale** per capire se procedere o meno.

Gli *output* principali sono la **Documentazione di Inizio del Progetto** e il **Piano di Progetto**. E' inoltre pianificata in dettaglio la fase successiva con il relativo **piano**.

Agenda

Requisiti

Quali sono i requisiti che nella vostra esperienza sono più importanti in un progetto di Security Testing secondo voi?

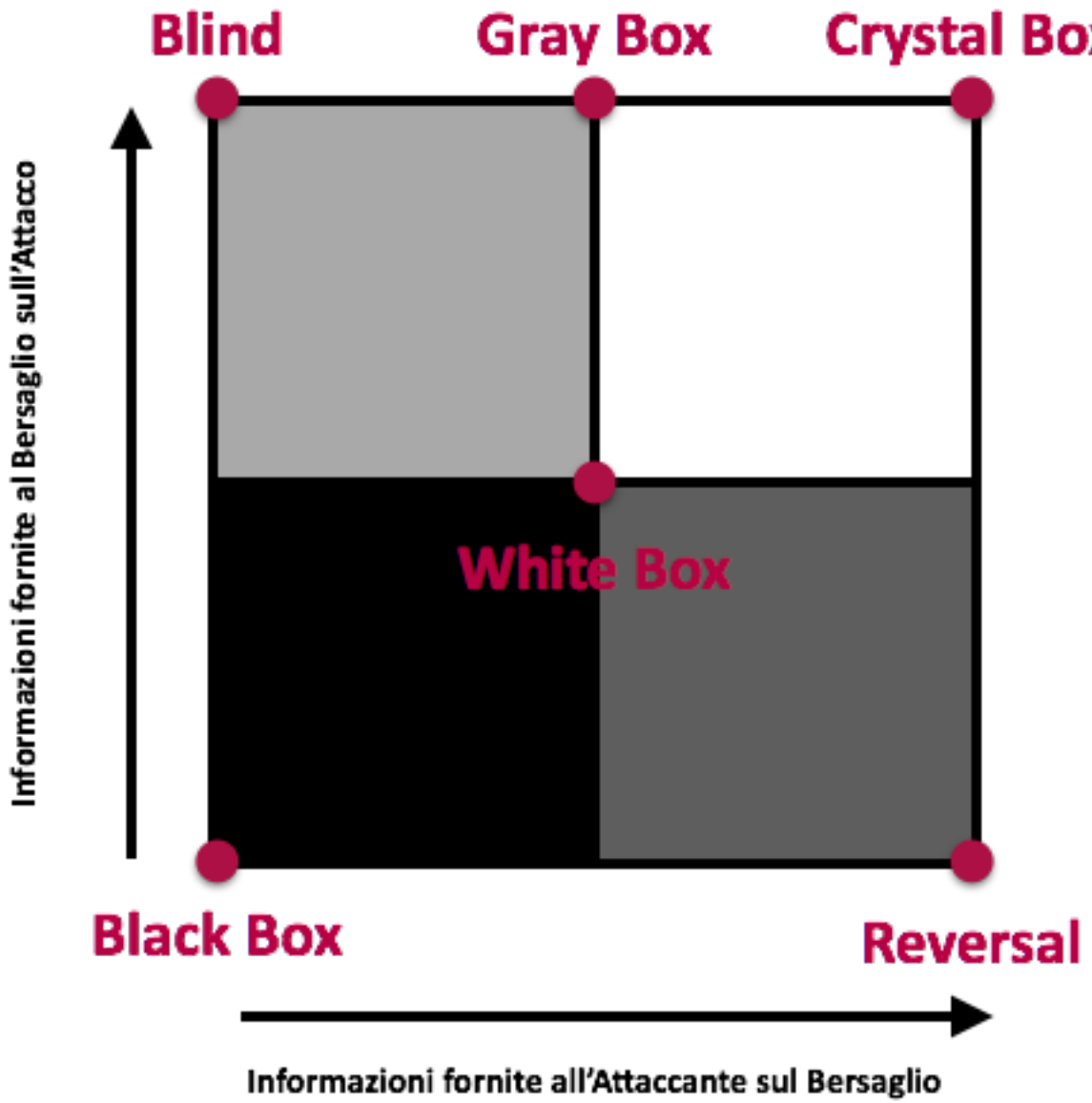
Scriveteli!

Requisiti da definire secondo l'OSSTMM

L'OSSTMM consiglia di definire, per ogni Security Test una serie di informazioni. Sono i requisiti necessari per il Test:

- **Target e ambiente**: Cosa vogliamo proteggere, qual' è la zona di ingaggio e lo scope (es. **una determinata applicazione web, una rete, un IP**)
- **Vettore**: Come gli analisti interagiranno con il target, p.e. **tramite Internet, in loco oppure in VPN**.
- **Tipo di Test**: p.e. Black Box, White Box o Crystal Box. A seconda del tipo di test cambia l'obiettivo e le informazioni da reperire per l'esecuzione del test.
- **Regole di Ingaggio**: per regolare i rapporti tra cliente e fornitore e il comportamento del fornitore e dei suoi analisti (es. **nessuna modifica ai sistemi o applicazioni durante i test**).

Tipi di Test secondo l'OSSTMM



Definire un Security Test con PTES per Reti e Sistemi

- **Scopo e Motivazione**
  - Perché si vuole fare il Security Test?
  - E' per motivi di Compliance? In caso quali?
- **Tempistiche**
  - Quando deve essere eseguita l'attività?
    - Orario lavorativo?
    - Orario serale/notturno?
    - Giorni lavorativi o nei week end?
- **Ambito/Vettore**
  - **Larghezza**: Quanti IP devono essere analizzati in totale? Esterni? Interni? Come raggiungere la rete interna?
  - **Profondità**: In caso di accesso a un sistema cosa fare?
- **Ambiente**
  - Ci sono dei dispositivi che possono influire con l'attività? (es. WAF, IPS, IDS…)

Definire un Security Test con PTES per Applicazioni Web

- **Scopo e Motivazione**
  - Qual' è la motivazione del test?
  - E' per motivi di Compliance? In caso quali?
- **Ambito/Tipo di Test**
  - **Larghezza**: Quante applicazioni? Quante pagine statiche? Quante pagine dinamiche? Quanti profili utente saranno utilizzati?
  - **Profondità**: E' possibile analizzare il codice sorgente? E' previsto l'invio di documentazione? Sarà possibile fare analisi statica sull'applicazione? Sarà possibile fare del fuzzing? Test sulla logica applicativa? Test sui ruoli? Sono previste delle scansioni tramite l'utilizzo delle credenziali?

Requisiti – Esercizio (10 minuti)

Scenario: Il Cliente vuole valutare un'Applicazione Web critica per il suo Business. Siamo alla riunione di kick-off per raccogliere i requisiti insieme al Cliente in modo da avere le informazioni per eseguire la stima.

Definire la lista delle domande a cui deve rispondere il Cliente.

Requisiti – Esempio per Applicazione Web

- **Identificativo documento:** CodCliente_CodProg_CodDoc_Ver
- **Scopo e Motivazione**
  - Perché si vuole fare il Security Test? Compliance? Quali?
  - Tipologia di Test
- **Tempistiche**
  - Giorni: lavorativi o week end
  - Orari: lavorativo, serale o notturno?
- **Ambito**
  - **Larghezza:** Quante applicazioni (ip/url*)? Quante pagine statiche, dinamiche o funzionalità? Quante pagine dinamiche? Quanti profili utente?* Esclusioni?
  - **Profondità:** E' necessario sfruttare tutte le vulnerabilità in maniera estesa? Test da escludere?
- **Vettore**
  - I test saranno svolti sull'ambiente di produzione o collaudo?
  - E' possibile svolgere i test da remoto? Da VPN*? On-site*?
- **Ambiente**
  - Ci sono dei sistemi che possono influire con l'attività? (es. WAF, IPS, IDS…)
  - Chi è il proprietario o il gestore dei sistemi?
- **Riferimenti e regole**
  - Persona in caso di emergenza e responsabile per la firma della manleva. Definire regole di ingaggio specifiche?

Agenda

Stima

Stima

Quando si prepara un piano o un'offerta commerciale è importante avere delle stime attendibili.

Purtroppo in buona parte dei progetti è possibile avere una

buona stima solo dopo l'inizio.

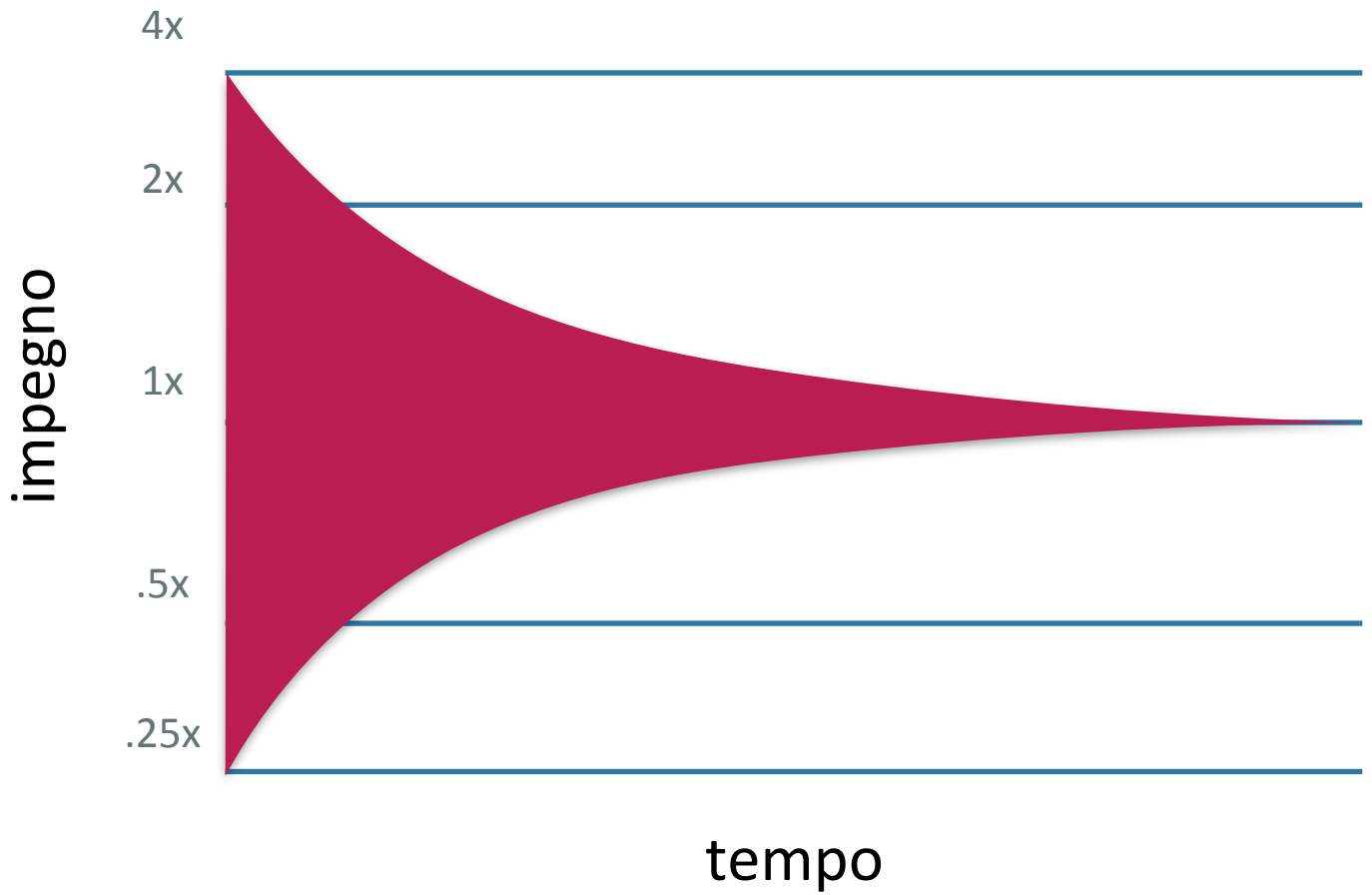
Come fare la stima secondo PTES

Buona parte delle stime **si basano sull'esperienza**.

Quanto ci è voluto per testare in profondità l'ultima volta un'applicazione simile? Quanto ci è voluto per quella quantità di IP?

Rivedi le tue e-mail e i log delle scansioni e **aggiungi** un **20%** per avere un margine ragionevole.

Il cono d'incertezza



Chi deve fare la stima?

Far eseguire la stima a **chi realizzerà il prodotto**, quindi i tecnici.

Per la pianificazione assumere che le risorse saranno produttive solo per l'**80% del tempo**.

Attenzione!!!

Redigere il **Report** può occupare metà del tempo necessario per l'intera attività tecnica.

Agenda

Piano di Progetto

Il **piano di progetto** descrive **come** e **quando** si devono raggiungere gli obiettivi identificando le risorse, le attività e i principali prodotti specialisti da rilasciare.

Piano di Progetto - Composizione

PRINCE2® consiglia di inserire nel piano la **descrizione**, i **prerequisiti**, **dipendenze**, **assunzioni**, **lezioni** apprese, come **monitorare e controllare** il piano, **budget** e **tolleranze**, i **prodotti** da rilasciare, Tempi (**orari, giorni, durata**) e **risorse** coinvolte.

Piano di Progetto - Esempio

- **Identificativo documento:** CodCliente_CodProg_CodDoc_Ver
- **Descrizione:** Cliente XX - Penetration Test della Rete Esterna
- **Prerequisiti:** Lista delle reti, Manleva firmata, Regole di ingaggio definite
- **Lezioni incorporate:** Escludere dai test Web l'host 127.0.0.1 in quanto fragile
- **Monitoraggio e controllo:** Inviare mail di inizio e fine attività come da template concordato rif. 123
- **Descrizione dei Prodotti:** Template concordato rif. 456
- **Cronogramma:**
  - Inizio: 11-01-2014
  - Durata del test: 2 settimane
  - Consegna del report: 2 settimane dopo la chiusura dei test
  - Tempistiche: Giorni lavorativi (Lun-Ven) in orari di ufficio (09:00-18:00 ora italiana)
- **Risorse:** Tester #1 e Tester #2

Manleva e Regole di Ingaggio

Manleva

La Manleva è una dichiarazione scritta con la quale il Cliente, o più in generale il firmatario solleva il Fornitore dagli eventuali effetti negativi causati dall'attività del progetto. E' un **prerequisito all'avvio dell'attività tecnica**.

Le Regole di Ingaggio dell'OSSTMM prevedono che:

- B6 - Performing security tests against any scope without explicit written permission from the target owner or appropriate authority is strictly forbidden.
- C9 - Contracts should limit liability to the cost of the job, unless malicious activity has been proven.
- C12 - The client must provide a signed statement which provides testing permission exempting the Analysts from trespass within the scope, and damages liability to the cost of the audit service with the exception where malicious activity has been proven.

Le Regole di Ingaggio dell'OSSTMM (1/3)

Le regole di ingaggio di OSSTMM per un Security Test definiscono le **linee guida operative** e **le opportune pratiche** di marketing e vendita, esecuzione e nella gestione dei risultati dei test. Le regole influenzano pesantemente il lavoro del Project Manager, i rapporti tra Cliente e Fornitore e i **documenti formali richiesti**. Per esempio:

- ***C8*** *- With or without a Non-Disclosure Agreement contract, the security Analyst is required to provide confidentiality and non-disclosure of customer information and test results.*
- ***C13*** *- Contracts must contain emergency contact names and phone numbers.*
- *C14 - Contracts must contain the process for future contract and statement of work (SOW) changes.*
- *D17 - The scope must be clearly defined contractually before verifying vulnerable services.*

Le Regole di Ingaggio dell'OSSTMM (2/3)

Altre utili regole di ingaggio per il Project Manager sono:

- ***E19*** *- The test plan may not contain plans, processes, techniques, or procedures which are outside the area of expertise or competence level of the Analyst.*
- ***F21*** *- The Analyst must always operate within the law of the physical location(s) of the targets in addition to rules or laws governing the Analyst's test location.*
- *F22 - To prevent temporary raises in security for the duration of the test, only notify key people about the testing. It is the client's judgment which discerns who the key people are; however, it is assumed that they will be information and policy gatekeepers, managers of security processes, incident response personnel, and security operations staff.*
- *F23 - If necessary for privileged testing, the client must provide two, separate, access tokens whether they be passwords, certificates, secure ID numbers, badges, etc. and they should be typical to the users of the privileges being tested rather than especially empty or secure accesses.*

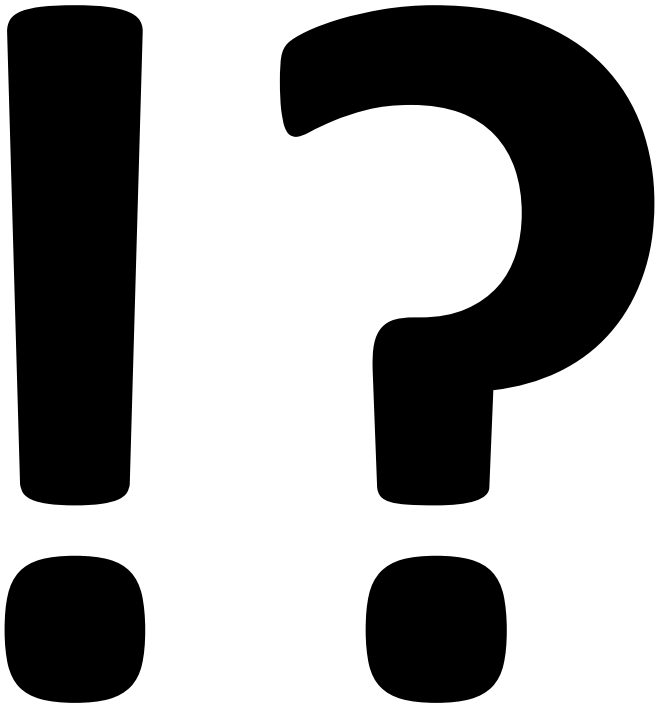
(continua)

Le Regole di Ingaggio dell'OSSTMM (3/3)

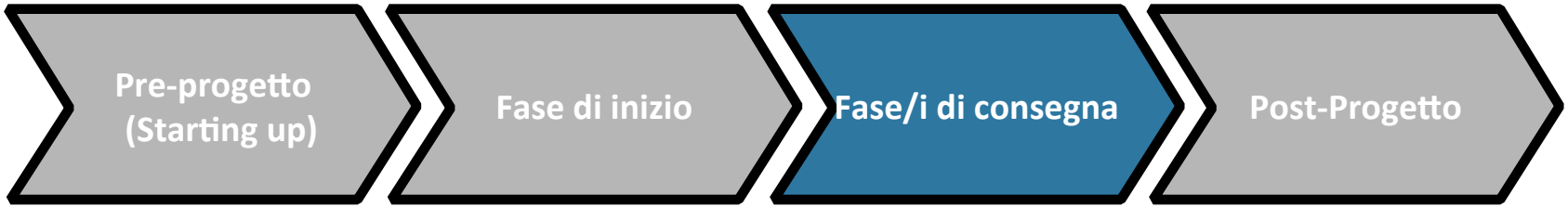
(segue)

- *G35 - Client notifications are required whenever the Analyst changes the testing plan, changes the source test venue, has low trust findings, or any testing problems have occurred.*
- *G40 - The client must be notified when the report is being sent as to expect its arrival and to confirm receipt of delivery.*
- ***G41** - All communication channels for delivery of the report must be end to end confidential.*

DOMANDE?



Agenda



Fasi di Consegna e Fase di Consegna Finale

- OSSTMM
- NIST
- OWASP
- PTES

Fasi di Consegna e Fase di Consegna Finale

L'*input* principale è il **Piano di Fase** con i relativi documenti correlati.

La *fase* si struttura in due processi: l'*Controllo di Fase* che ha lo scopo di assegnare, monitorare e controllare il lavoro; la *Gestione della Consegna dei Prodotti che* si occupa di gestire i rapporti tra il Project Manager e il Team Manager (che gestisce i Team di Specialisti).

E' in questa fase che si svolgono le fasi tecniche. Solitamente sono almeno due: l'**attività di testing** & **reportistica**.

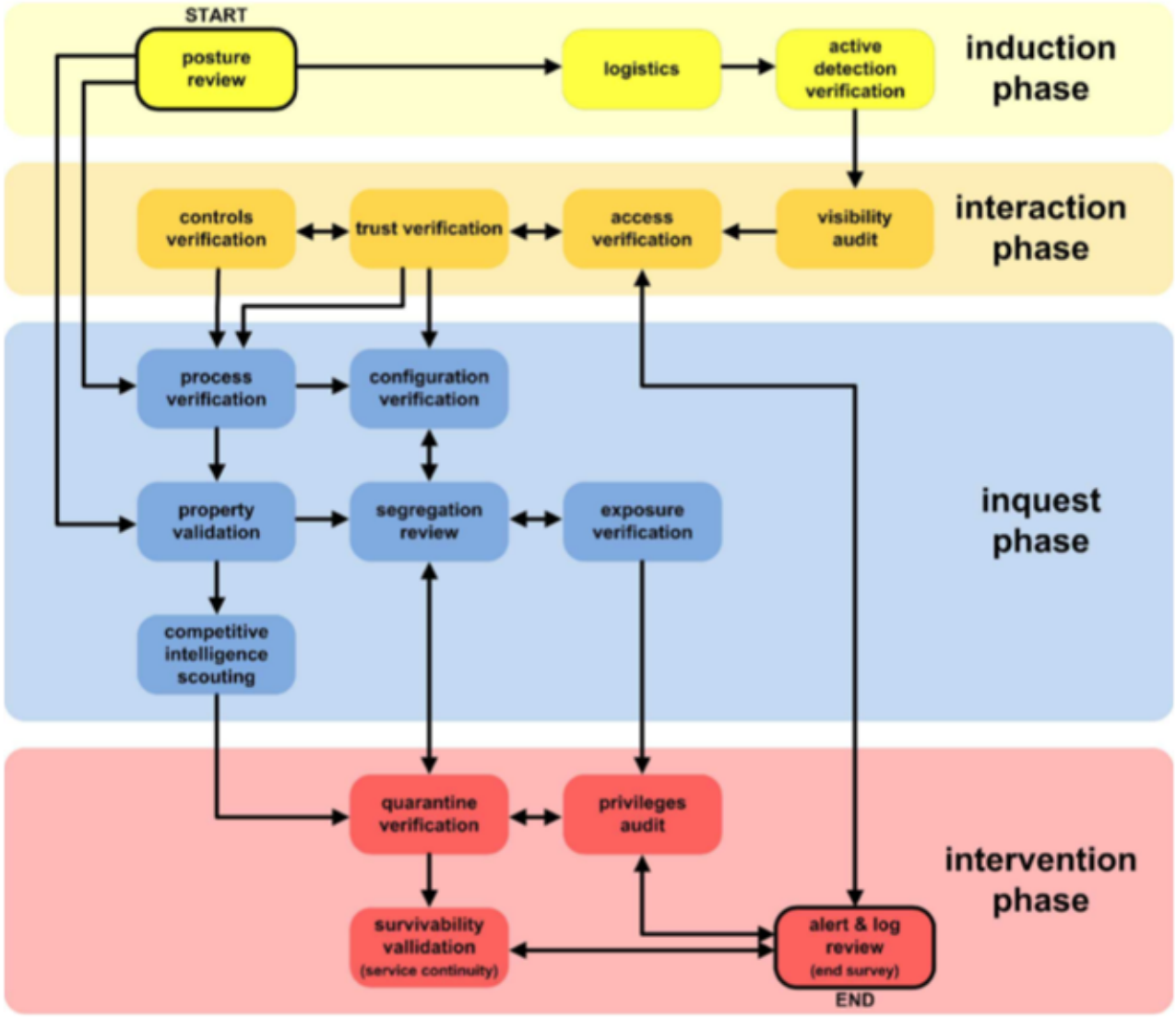
Gli *output* principali sono i **Prodotti di Progetto** e ulteriore documentazione che contiene p.e. le **azioni post-progetto** e il **piano di verifica dei benefici**.

Cosa succede durante le fasi di consegna

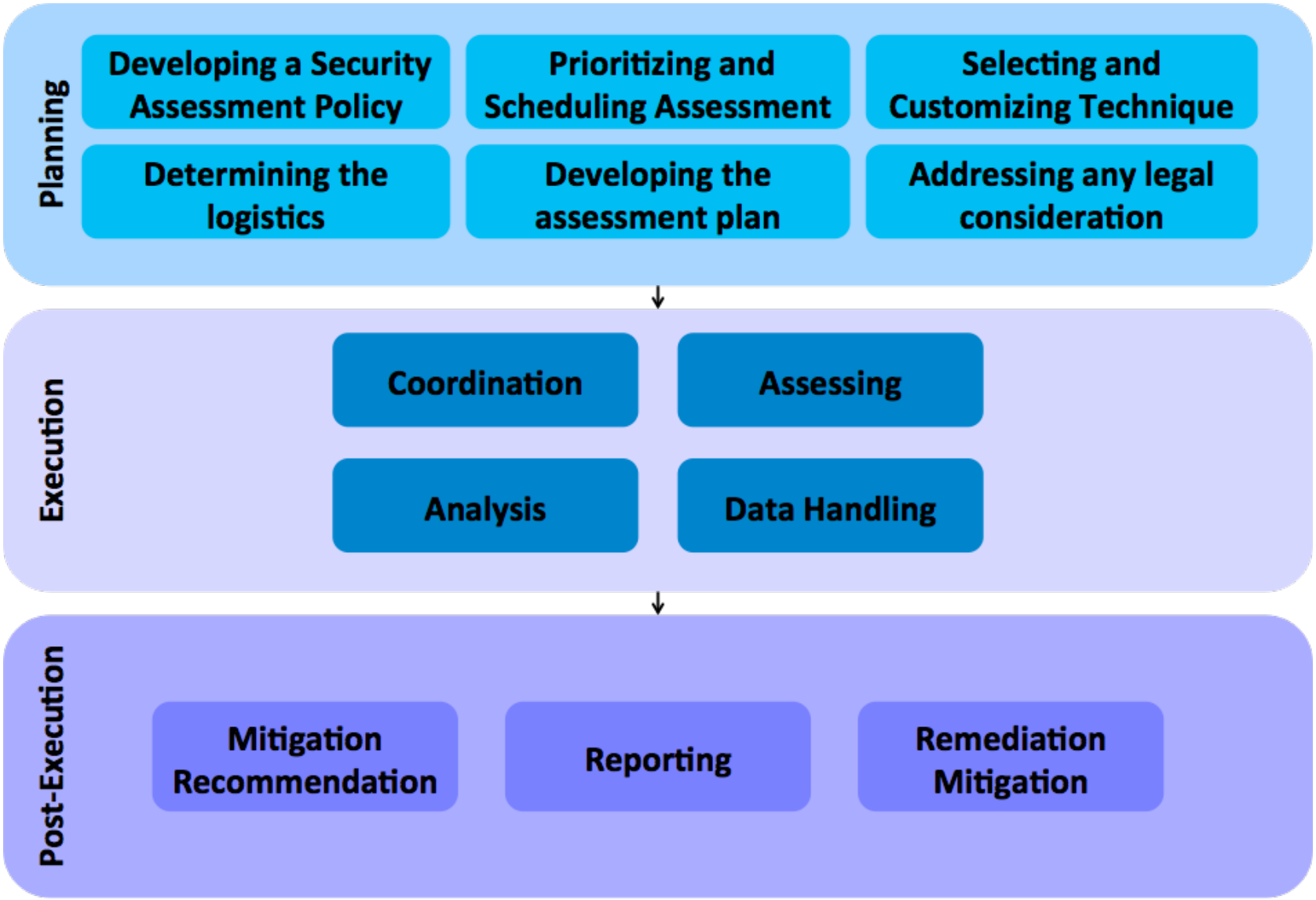
Durante le fasi di consegna saranno svolte le attività tecniche e saranno consegnati i relativi deliverable, nel nostro caso i report.
Andiamo a vedere gli schemi di lavoro del Team di Specialisti così come previsto da:

- OSSTMM
- NIST
- OWASP
- PTES

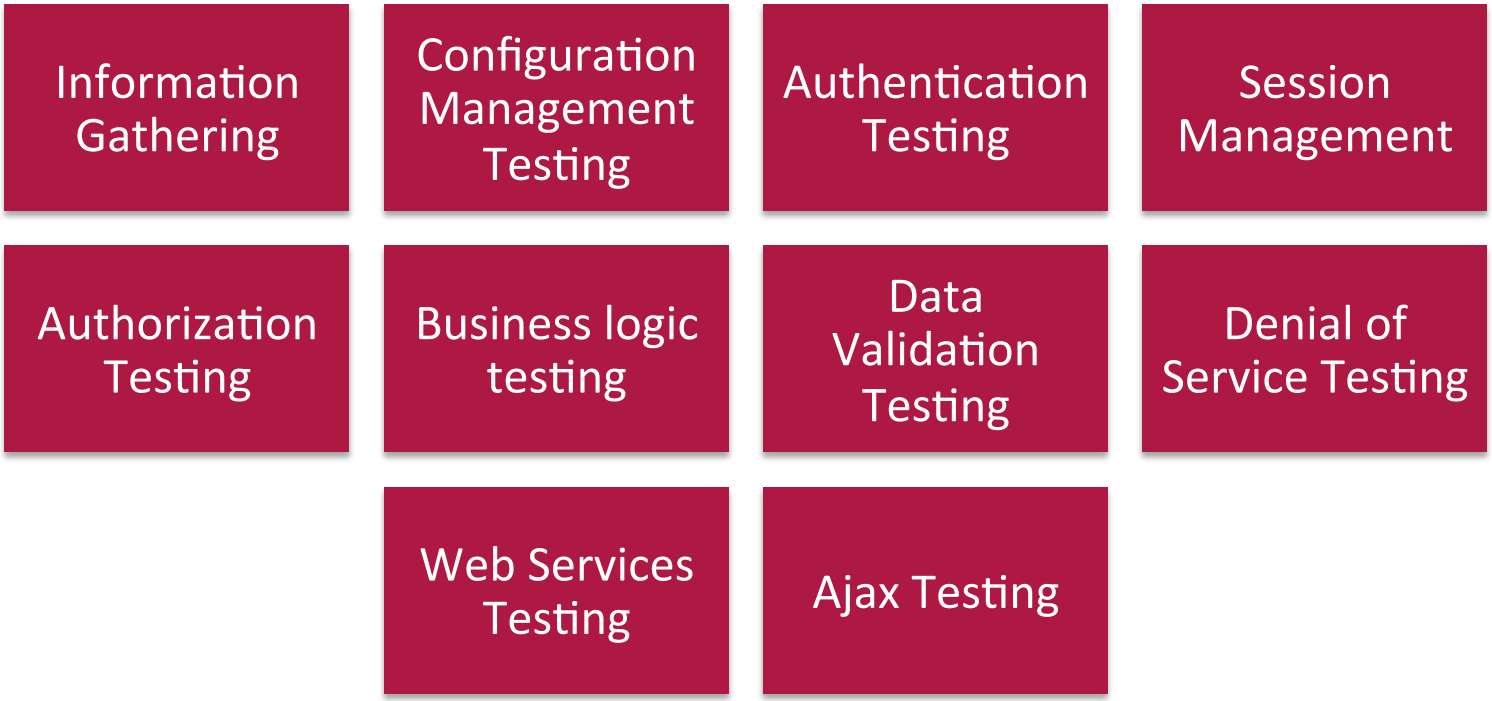
Il Ciclo di Vita di OSSTMM



Il Ciclo di Vita del NIST

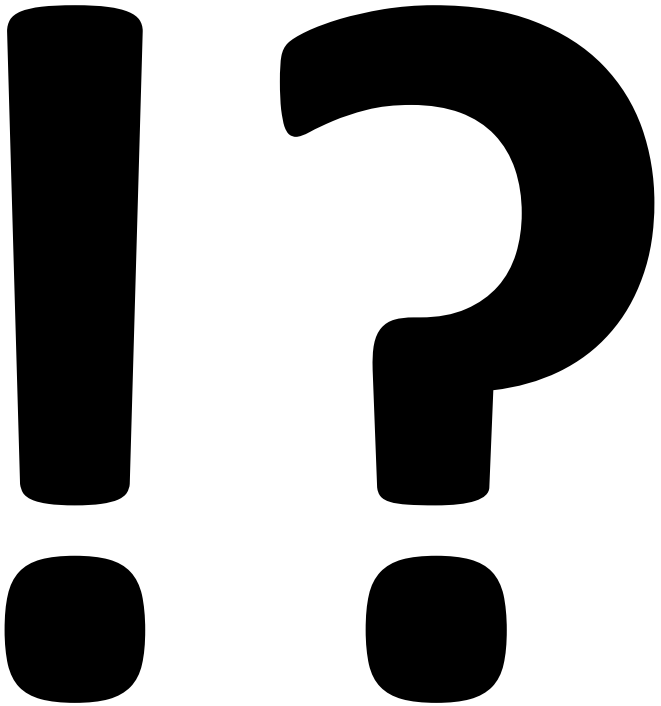


Attività tecniche di OWASP

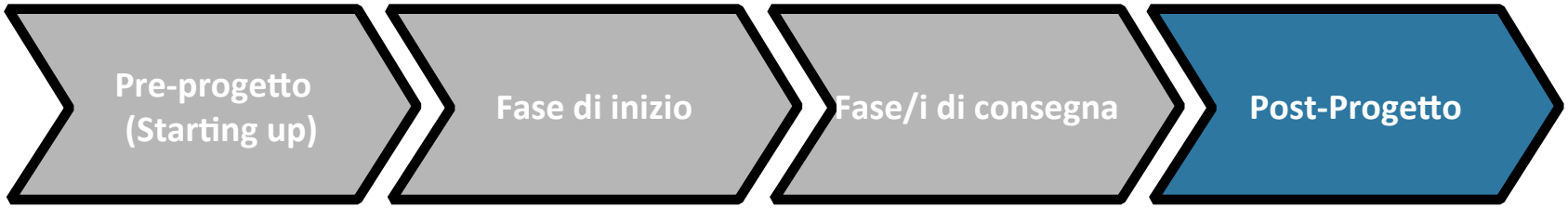


Il Ciclo di Vita di PTES

DOMANDE?



Agenda



Post-Progetto

- I Benefici
- Le azioni post-progetto

Benefici secondo PRINCE2®

Un progetto viene avviato affinché il **Committente/Cliente raccolga dei benefici**, cambiamenti misurabili percepiti come positivi dal Committente e derivati dal completamento del progetto. I benefici vengono **formalizzati nel Business Case**.

Devono essere monitorati e misurati. Alcuni vengono raccolti durante il progetto, altri dopo ed è necessario redigere il **Piano di verifica dei benefici**.

Benefici in un progetto di Security Testing

Solitamente in un progetto di Security Testing i benefici si raccolgono dopo la fine del progetto, p.e. la riduzione del numero delle vulnerabilità presenti.

In questo caso specifico per la verifica è necessario
eseguire un re-test
dopo che è stato implementato il Remediation Plan.

Le azioni post-progetto secondo PRINCE2®

Le azioni post-progetto sono quelle **azioni consigliate** che deve eseguire il committente relative a **questioni**, **rischi** o **attività da intraprendere** *dopo* la chiusura del progetto.

Tali azioni devono essere documentate formalmente.

Per esempio PRINCE2® le riporta nel Rapporto di Fine Progetto e in alcuni Rapporti di Fine Fase.

Le azioni post-progetto in un progetto di Security Testing

Le tipiche azioni post-progetto sono:

- **Seguire i consigli nel piano di rientro** specifico per ogni vulnerabilità trovata, secondo le priorità definite, quindi eseguire attività di re-test.
- Definire e implementare un **processo di Ciclo di Sviluppo Sicuro** per la messa in sicurezza delle applicazioni e dei sistemi che le ospitano.
- Eseguire **attività di Code-Review** sull'applicazione per una maggiore copertura integrando i risultati con quelli del Penetration Test.
- Eseguire il **monitoraggio delle richieste sui sistemi in produzione** per identificare eventuali attacchi, implementare soluzioni di Web Application Firewall (WAF) che permettano di identificare eventuali attacchi e rispondere tempestivamente.

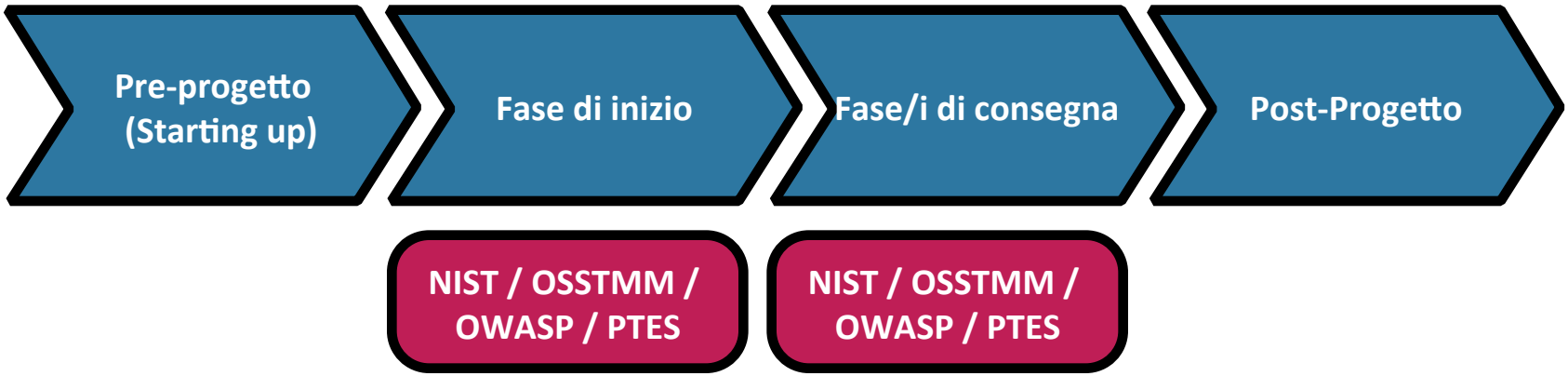
Agenda

Parte C - Conclusioni

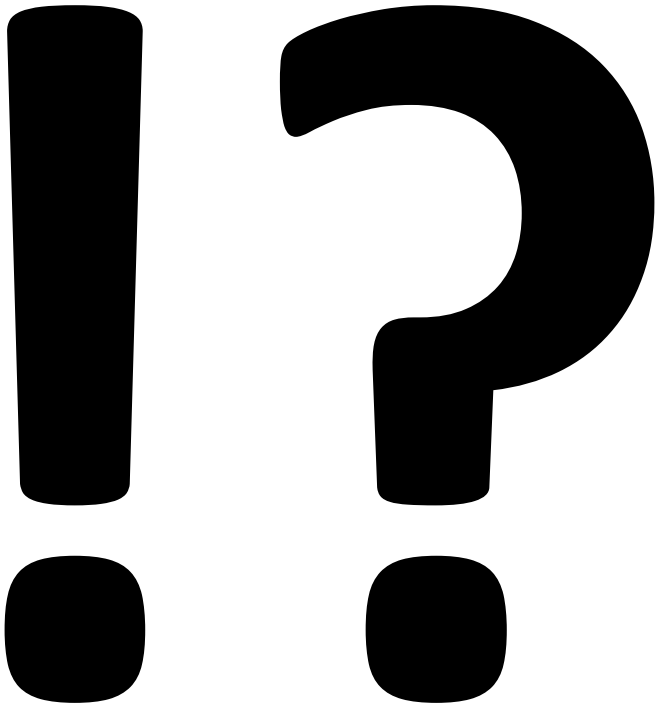
Conclusioni

"Get the best from the best"

Arie Van Bennekum, firmatario del Manifesto Agile



DOMANDE?



Bibliografia & Sitografia

- Office of Government Commerce (OGC), Successo nella Gestione dei Progetti con PRINCE2®,The Stationery Office (TSO), 2011
- Office of Government Commerce (OGC), ITIL® Service Design, 2011
- ISECOM, OSSTMM v4 Alpha, 2013
- U.S. Department of Commerce, NIST SP800-115, 2008
- OWASP, Testing Guide v3, 2008
- PTES, www.pentest-standard.org
- Ponemon Institute, 2013 Cost of Cyber Crime Study, 2013

Note e Copyright

A prescindere dal lavoro presso aziende o clienti o la partecipazione ad organizzazioni i relatori parlano secondo il loro personale punto di vista.

Durante questo seminario divulgativo e gratuito si farà riferimento a **marchi registrati**, che sono di proprietà dei rispettivi proprietari:

- PRINCE2®, ITIL®, M_o_R® sono marchi registrati della AXELOS Limited.
- ISACA® è un marchio registrato dell'Information Systems Audit and Control Association
- COBIT® è un marchio registrato dell' Information Systems Audit and Control Association e dell' IT. Governance Institute.

Ogni riferimento a cose, persone o fatti è puramente casuale, alcuni fatti potrebbero essere inventati (o modificati per renderli anonimi)

Grazie

Simone Onofri

simone.onofri@techub.it

Claudia Spagnuolo

claudia.spagnuolo@yahoo.it