



Ministero  
dell'Economia  
e delle Finanze

# La PA è in movimento: le proposte di Consip

Matteo Cavallini



consip



## Lo scenario e l'esigenza

Veracode ha realizzato uno studio su oltre 1400 applicazioni verificandone lo stato di vulnerabilità

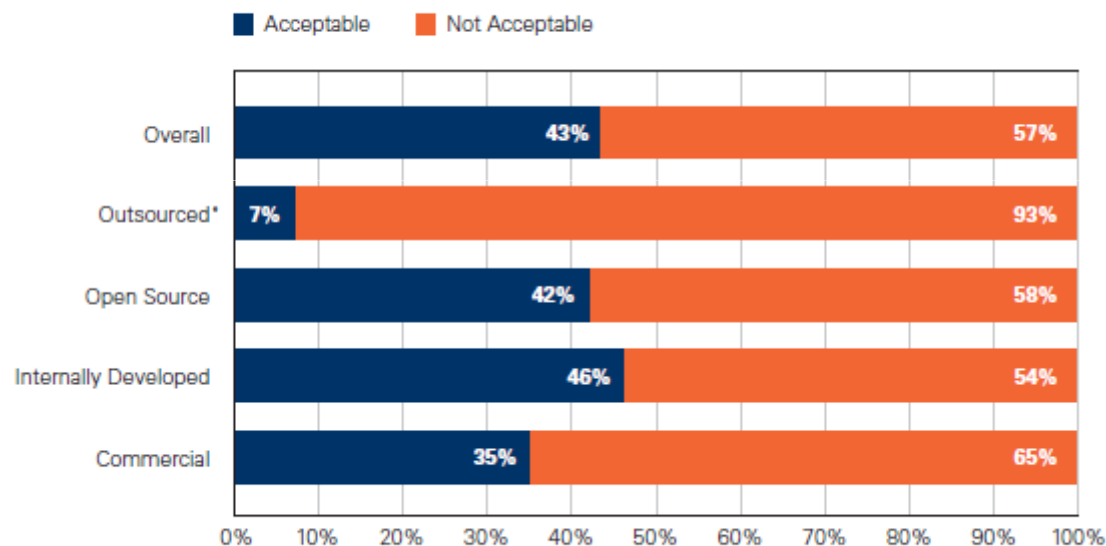


Figure 3: Supplier Performance on First Submission (Adjusted for Business Criticality)



Veracode ha realizzato uno studio su oltre 1400 applicazioni verificandone lo stato di vulnerabilità

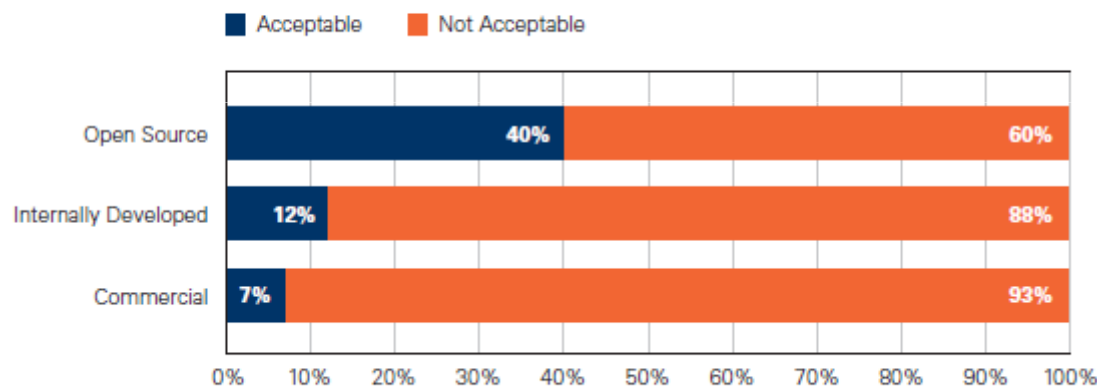


Figure 5: OWASP Top 10 Compliance by Supplier on First Submission

# Lo scenario e l'esigenza

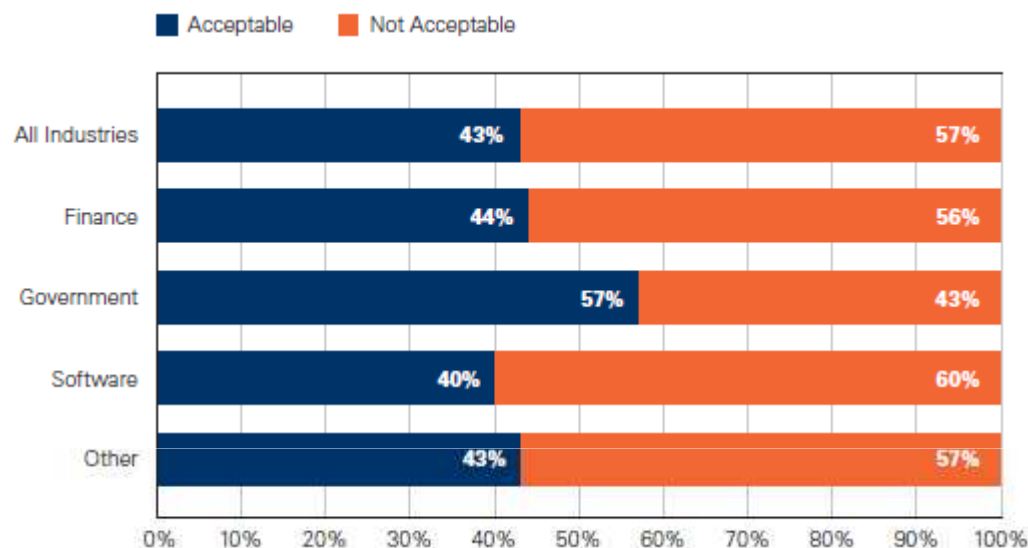


Figure 18: Application Performance by Industry on First Submission  
(Adjusted for Business Criticality)

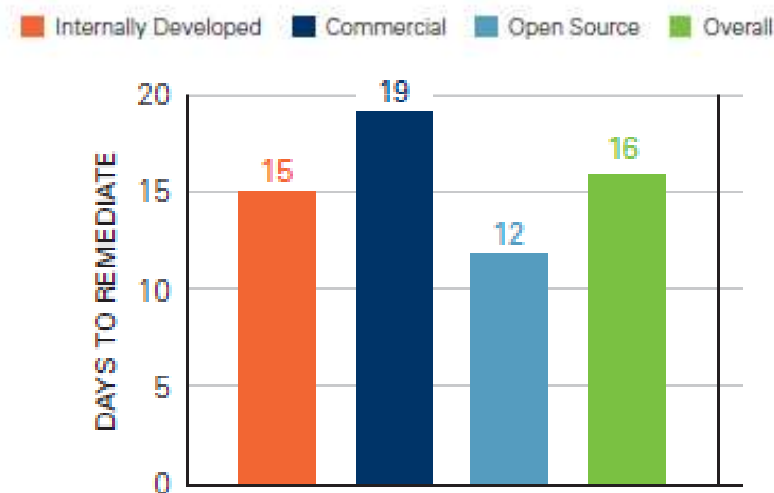


Figure 4: Remediation Performance by Supplier

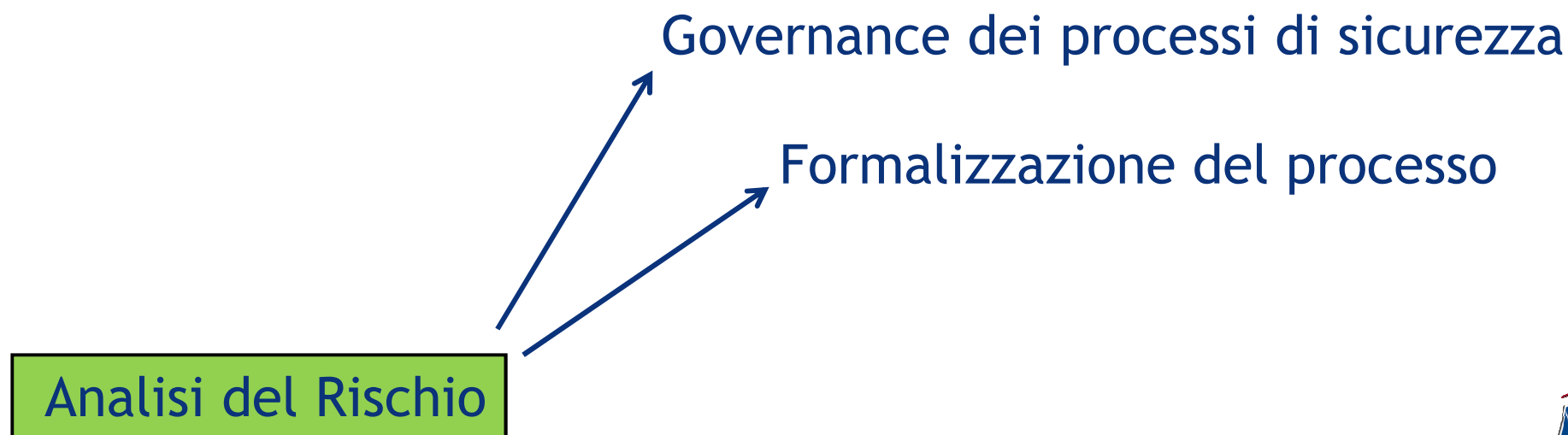
# Lo scenario e l'esigenza

Finance		Software		Government		Other	
Cross-site Scripting (XSS)	54%	Cross-site Scripting (XSS)	30%	Cross-site Scripting (XSS)	87%	Cross-site Scripting (XSS)	45%
Information Leakage	17%	Information Leakage	19%	SQL Injection	7%	CRLF Injection	20%
Cryptographic Issues	7%	Cryptographic Issues	10%	CRLF Injection	2%	Information Leakage	10%
CRLF Injection	6%	CRLF Injection	8%	Information Leakage	1%	Cryptographic Issues	6%
SQL Injection	4%	Directory Traversal	7%	Cryptographic Issues	1%	Directory Traversal	3%
Directory Traversal	3%	SQL Injection	5%	OS Command Injection	<1%	SQL Injection	3%
Buffer Overflow	2%	Numeric Errors	4%	Time and State	<1%	Untrusted Search Path	3%
Time and State	1%	Buffer Overflow	4%	Directory Traversal	<1%	Buffer Overflow	3%
Encapsulation	1%	Error Handling	3%	Credentials Mgmt	<1%	Potential Backdoor	2%
Insufficient Input Validation	1%	Potential Backdoor	3%	Encapsulation	<1%	Time and State	2%
Potential Backdoor	1%	Time and State	2%	API Abuse	<1%	Error Handling	2%
Credentials Mgmt	1%	Buffer Mgmt Errors	2%	Error Handling	<1%	Credentials Mgmt	1%
Error Handling	<1%	Credentials Mgmt	1%	Insufficient Input Validation	<1%	API Abuse	1%
API Abuse	<1%	API Abuse	1%	Race Conditions	<1%	Encapsulation	1%
Buffer Mgmt Errors	<1%	Encapsulation	<1%	Buffer Mgmt Errors	<1%	Insufficient Input Validation	<1%

Table 6: Vulnerability Distribution by Industry

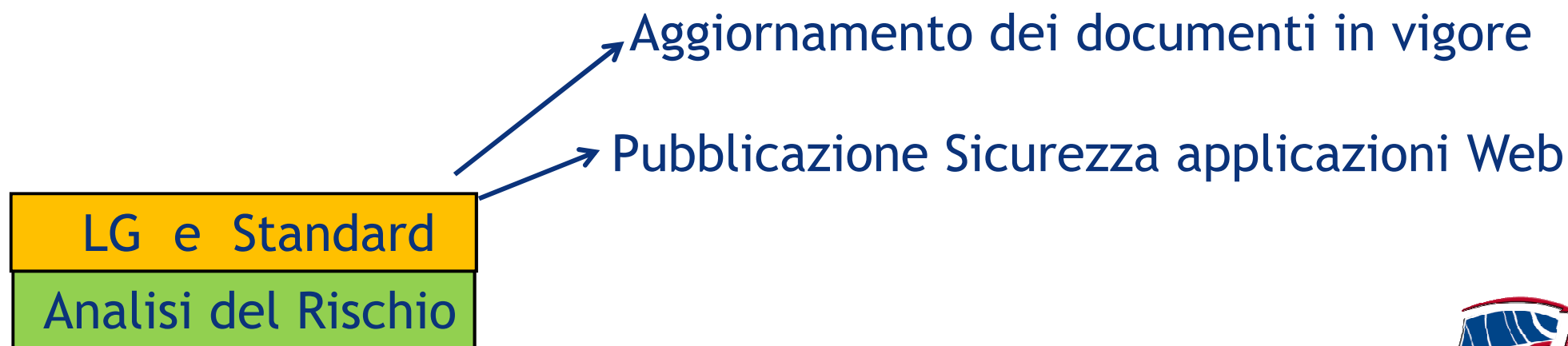
## Le attività di Consip

Consip ha definito il proprio approccio alla sicurezza applicativa



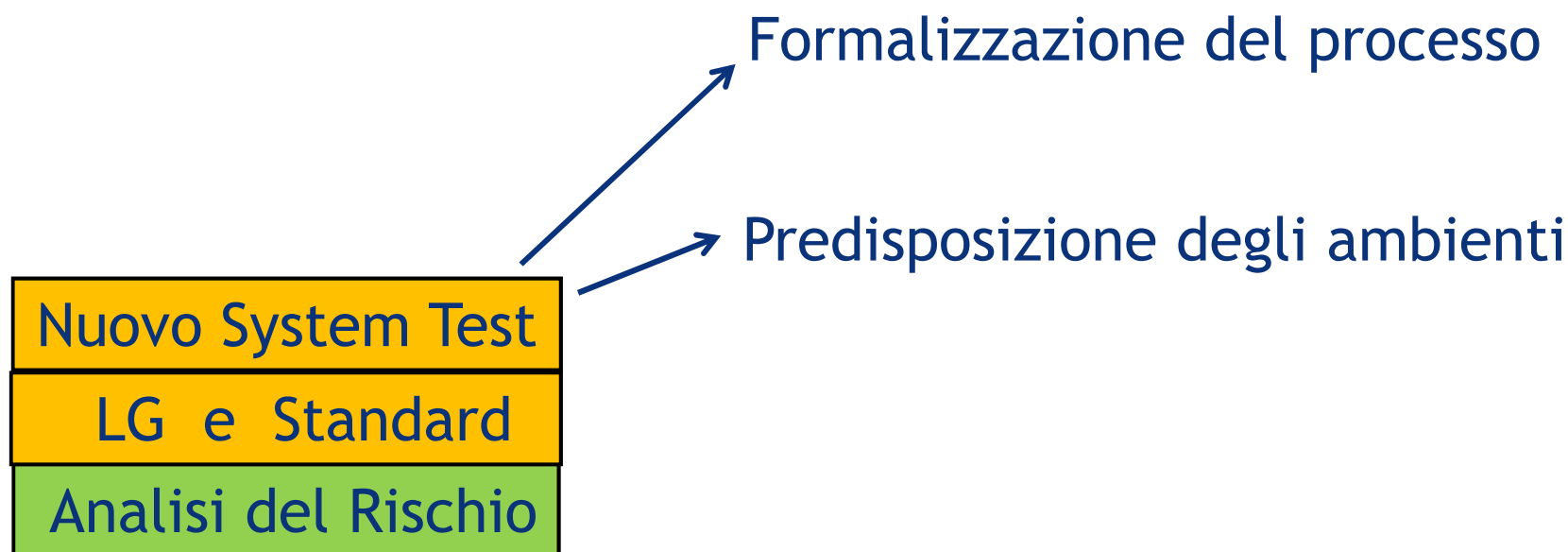
## Le attività di Consip

Consip ha definito il proprio approccio alla sicurezza applicativa



## Le attività di Consip

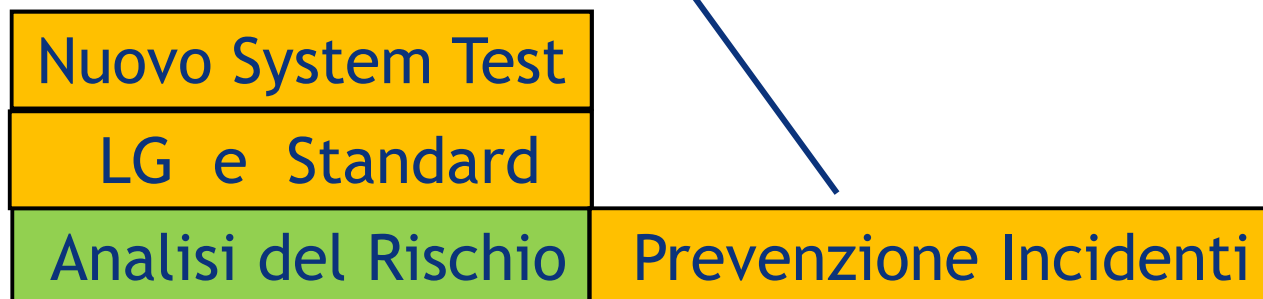
Consip ha definito il proprio approccio alla sicurezza applicativa



## Le attività di Consip

Consip ha definito il proprio approccio alla sicurezza applicativa

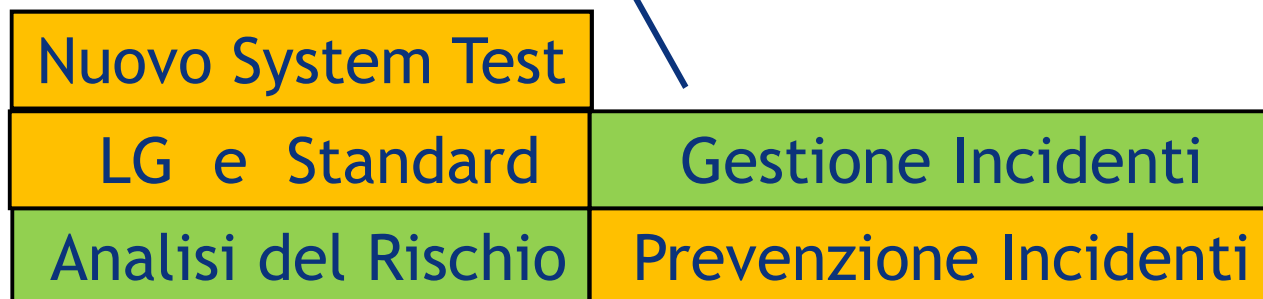
Tool e procedure per la gestione dei livelli di rischio



## Le attività di Consip

Consip ha definito il proprio approccio alla sicurezza applicativa

Tool e procedure per il contenimento degli incidenti



Nuovo System Test	
LG e Standard	Gestione Incidenti
Analisi del Rischio	Prevenzione Incidenti



## Le attività di Consip

Consip ha definito il proprio approccio alla sicurezza applicativa

Focal Point interno di tematica



Nuovo System Test	Comitato Guida
LG e Standard	Gestione Incidenti
Analisi del Rischio	Prevenzione Incidenti



## Le attività di Consip

Consip ha definito il proprio approccio alla sicurezza applicativa

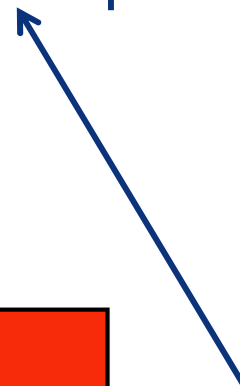


## Le attività di Consip

Consip ha definito il proprio approccio alla sicurezza applicativa

Verifica dell'approccio complessivo

Nuovo System Test	Comitato Guida	
LG e Standard	Gestione Incidenti	Assessment
Analisi del Rischio	Prevenzione Incidenti	Progetti Pilota



## Le attività di Consip

Consip ha definito il proprio approccio alla sicurezza applicativa

Definizione standard per la stesura dei capitolati

?

Nuovo System Test	Comitato Guida	Approccio gara
LG e Standard	Gestione Incidenti	Assessment
Analisi del Rischio	Prevenzione Incidenti	Progetti Pilota



## L'approccio standard - Le domande

Ha senso definire un **approccio singolo**  
di indirizzo di una tematica ad impatto comune?

Esistono nelle altre Amministrazioni approcci diversi?  
**Migliori?**

Il **mondo della fornitura** è già pronto?  
E quale approccio ritiene più opportuno?

L'approccio singolo ha un **impatto negativo sui costi** di sviluppo?



## L'approccio standard - La risposta



Tavolo di lavoro PA/Fornitori per lo sviluppo di  
“Linee Guida per lo sviluppo sicuro di applicazioni Web per la PA”

Obiettivi di massima:

- Definizione di un approccio all'outsourcing “condiviso” per le fasi di sviluppo, collaudo e manutenzione delle applicazioni Web
- Indicazione delle priorità e dei requisiti



## L'approccio standard - Le modalità

Al Tavolo di lavoro possono partecipare  
tutte le PA e i Fornitori interessati



Il Tavolo sarà guidato da Consip e OWASP Italy

Sarà definito un GdL operativo per la  
stesura della documentazione

Le decisioni saranno prese a maggioranza

## L'approccio standard - Le modalità



Le richieste di partecipazione devono essere inviate  
via mail a [uls@tesoro.it](mailto:uls@tesoro.it) entro il **10 dicembre 2010**

La prima riunione sarà convocata  
entro la prima metà di **gennaio 2011**

# Grazie per l'attenzione

matteo.cavallini@tesoro.it  
uls@tesoro.it

