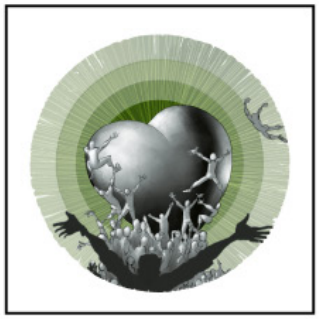
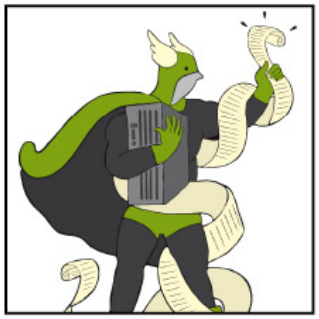
IBM

IBM SOFTWARELAND 2009.
SOLUZIONI INTELLIGENTI PER PROSPETTIVE CHE CAMBIANO.




Domenico Ercolani

Rational. software

Le soluzioni Rational a garanzia della sicurezza delle applicazioni web e rispetto della compliance

Compliance and Security secondo IBM

Gestione delle identità e controllo degli accessi alle risorse aziendali: le soluzioni TIVOLI

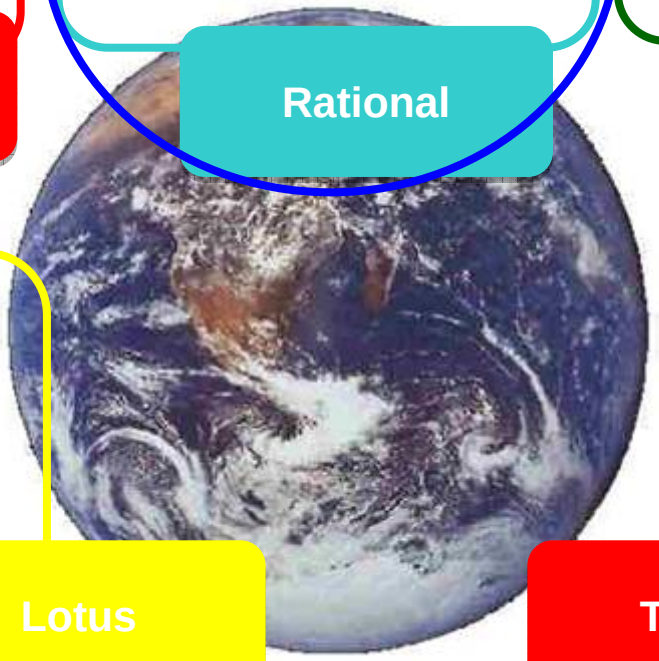
Tivoli

Le soluzioni Rational a garanzia della sicurezza delle applicazioni e il rispetto della compliance

Rational

Il rispetto delle normative legali e di settore per la privacy dei dati e il records management

Information Management



Protezione preventiva e controllo dello spam, virus e contenuto delle email per il tuo ambiente di posta Domino, con Lotus Protector

Lotus

Gestione del rischio, rispetto delle leggi e delle policy aziendali, report standard conformi alle normative

Tivoli

Agenda

- Rational Software
- Compliance
  - Compliance Management per SW Team
  - Compliance Applicazioni / Portali
- Sicurezza
  - Sicurezza delle applicazioni web

Agenda

- Rational Software
- Compliance
  - Compliance Management per SW Team
  - Compliance Applicazioni / Portali
- Sicurezza
  - Sicurezza delle applicazioni web

IBM Rational software

Un partner strategico per la "business innovation & trasformation"

Governance e gestione del ciclo di vita del software

Imperativi del Business

- Capacità globale
- Flessibilità
- "Time to Market"
- Gestione dei rischi e delle conformità

Rational. software

Governare i processi di business legati allo sviluppo ed al rilascio di software e sistemi

Anni di provata esperienza sui processi e sul successo dei clienti

Innovazione e Trasformazione del Business

- Allineamento
- Controllo
- Efficienza

Business, Governance e Sviluppo

Valore di Business

Controllo e flessibilità

Efficienza e costi

PRIORITA' e IMPATTO sul BUSINESS

- Enterprise Architecture/ Architectural Frameworks
- Product Portfolio Management
- Measurement & Reporting
- Production

- Requirements Definition & Management
- Release Management

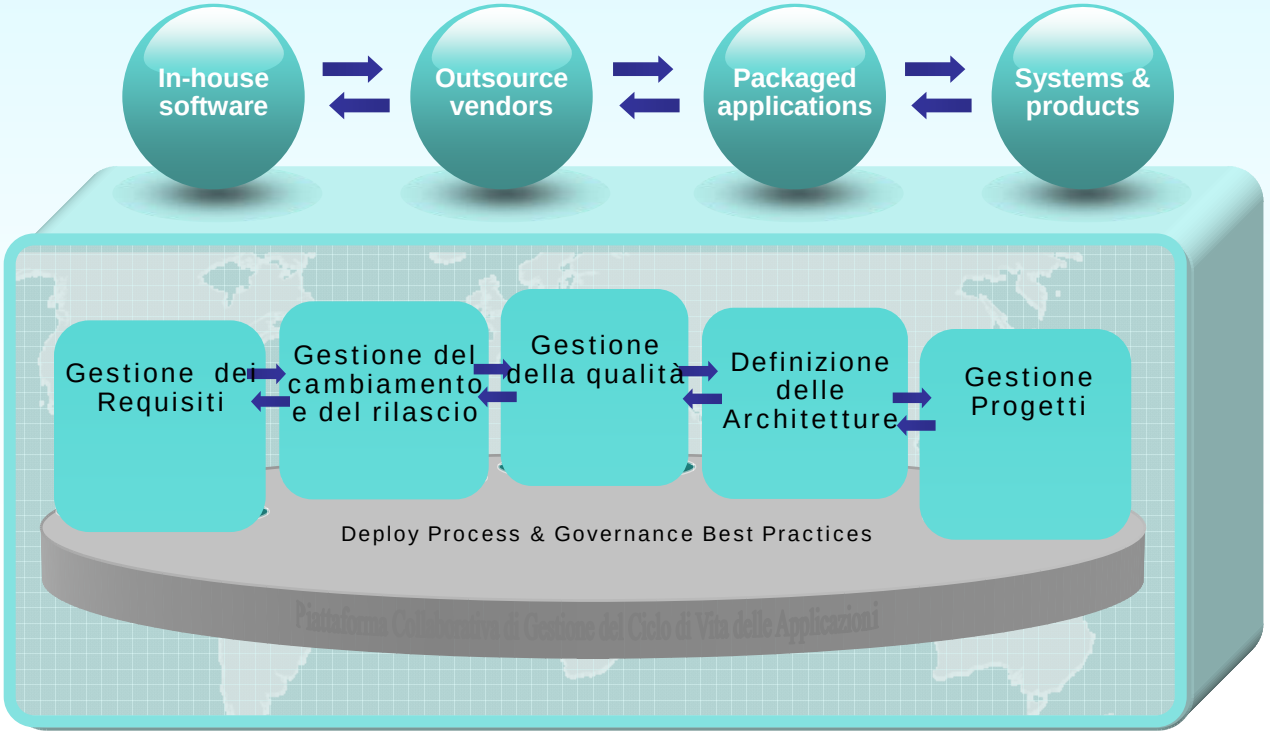
- Analysis & Design
- Construction
- Configuration & Change Mgmt
- Asset Management & Reuse
- Quality Management

Business ***Organizzazione*** ***Team*** ***Individuo***

IBM Rational Software Delivery Platform

Rational. software

***Soluzioni** che aiutano i clienti ad incrementare il VALORE e le performance dei loro investimenti nello sviluppo software*



- ***Produttività***
- ***Sviluppo Agile***
- ***Gestione di team distribuiti***
- ***Governance***
- ***Gestione del rischio***
- ***Compliance***

Agenda

- Rational Software
- Compliance
  - Compliance Management per SW Team
  - Compliance Applicazioni / Portali
- Sicurezza
  - Sicurezza delle applicazioni web

Compliance scenario

BANK FOR INTERNATIONAL SETTLEMENTS

United States Department of Health & Human Services

NASD

Sarbanes-Oxley Act

IAS

Basel II

ISO27001

PCI DSS

OSHA

HIPAA

21CFR11
(Electronic Signature records for Food and Drug)

Patriot Act
(anti money laundering)

Gramm Leach-Bliley Act
(Financial confidentiality of non public info)

W3C

DoD 5015.2 / PRO
(Certification of electronic records mgt SW products)

ACORD

International Accounting Standa Board

SEC 17a-4 / NASD 3010/3110
(Brokers, records for all correspondence)

NYSE

FEDERAL TRADE COMMISSION
FOR THE CONSUMER

The Federal Reserve Board

U.S. Food and Drug Administration

U.S. Department of Health and Human Services

Compliance management per SW teams

1) “Definisci cosa devi fare”

Disegna un processo di sviluppo in linea con le normative a cui sei soggetto

- “Business / Technicals controls” e workflow
- Approvazioni, autorizzazioni, punti di controllo, “separation of duties”

2) “Fai quello che hai definito

Automatismi per rafforzare l’aderenza del processo

- Strumenti per la guida del processo, workflow automatizzati, tools che guidino al “corretto comportamento”

3) “Sii capace di dimostrare”

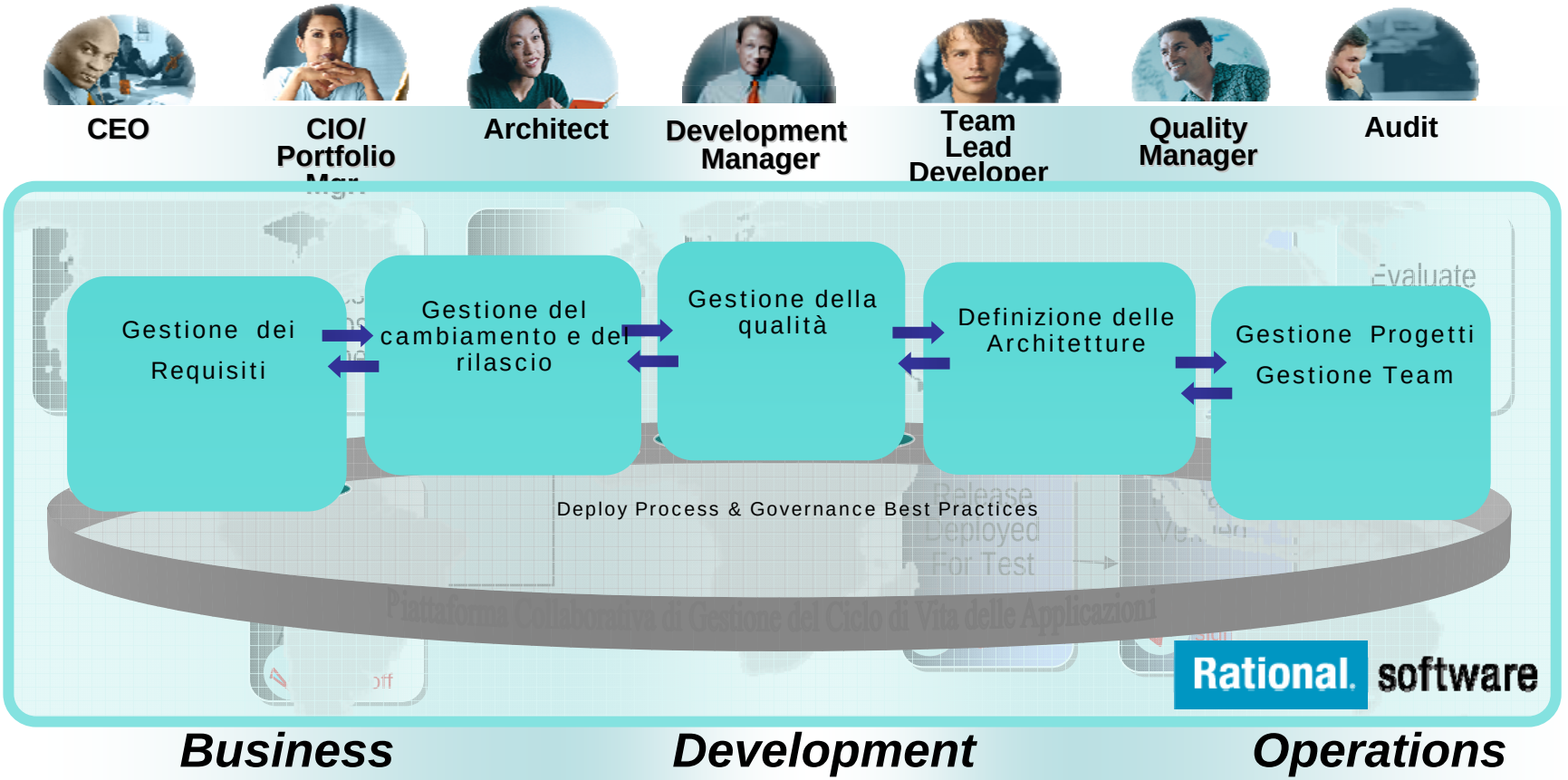
Generazione automatica della documentazione per l’audit

- Reports per l’Audit, Tracciabilità di quanto avviene nell’ambito della “software delivery organization”

4) Utilizza la compliance come vantaggio per il business

- Analizza le metriche del progetto e del processo
- Persegui il miglioramento continuo

Un esempio di processo di compliance



Compliance per applicazioni / portali web

Il Portale e le applicazioni rese disponibili attraverso il web sono un importante strumento per la comunicazione aziendale e parte integrante dei processi di business.

Per questo è importante curarne la qualità e la compliance con le normative di riferimento.

Quali sono i rischi?

- Clienti che abbandonano la navigazione (link non accessibili, errori applicativi, lentezza nel caricamento delle pagine)
- Controversie legali
- Aumento dei costi di supporto
- Danno all'immagine aziendale

Rational Policy Tester

- **Qualità**

- **Accessibilità**

- **Privacy**

Agenda

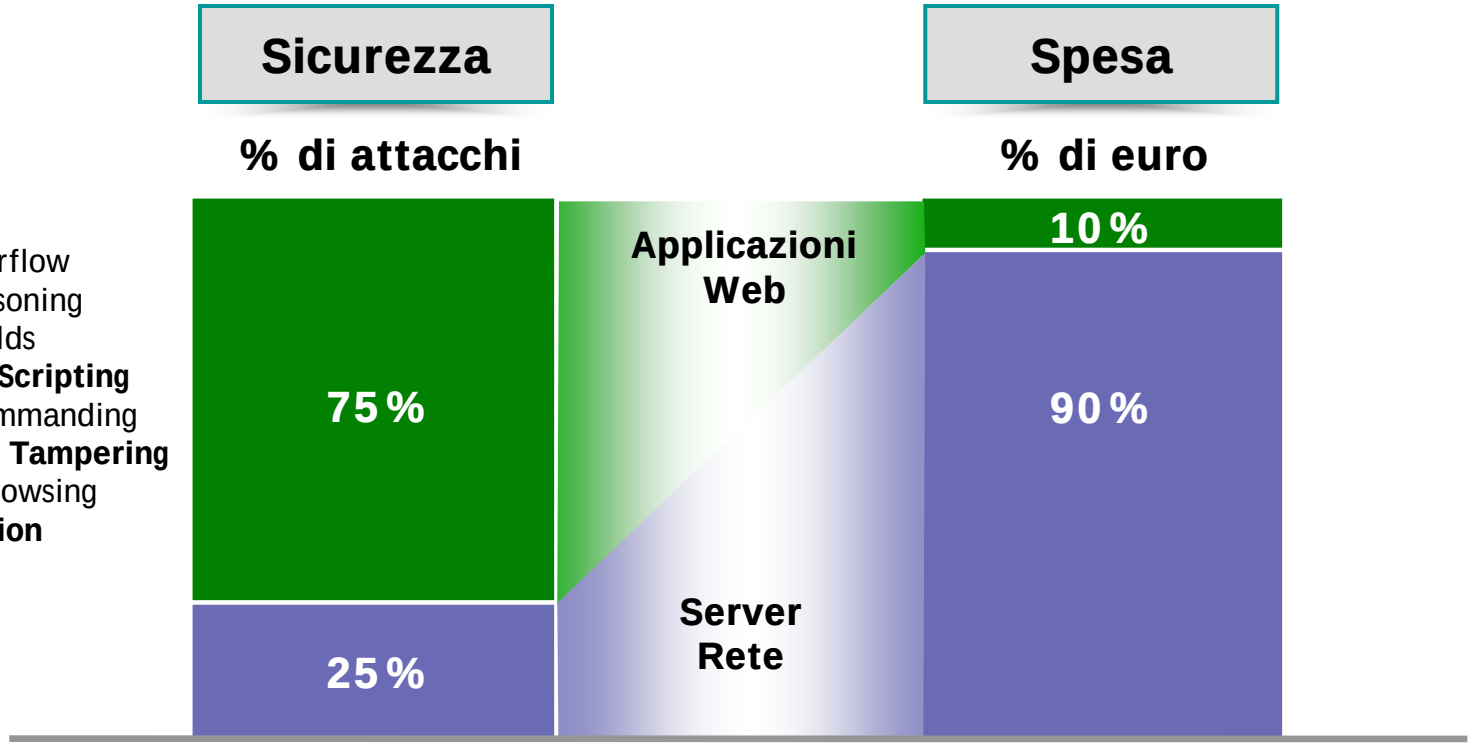
- Rational Software
- Compliance
  - Compliance Management per SW Team
  - Compliance Applicazioni / Portali
- Sicurezza
  - Sicurezza delle applicazioni web

Sicurezza delle applicazioni web: In Italia siamo tranquilli ?

Una falsa percezione:
“Le nostre applicazioni Web sono sicure”

La realtà: sicurezza e spesa non sono bilanciati

- Buffer Overflow
- Cookie Poisoning
- Hidden Fields
- **Cross Site Scripting**
- Stealth Commanding
- **Parameter Tampering**
- Forceful Browsing
- **SQL Injection**
- Etc…

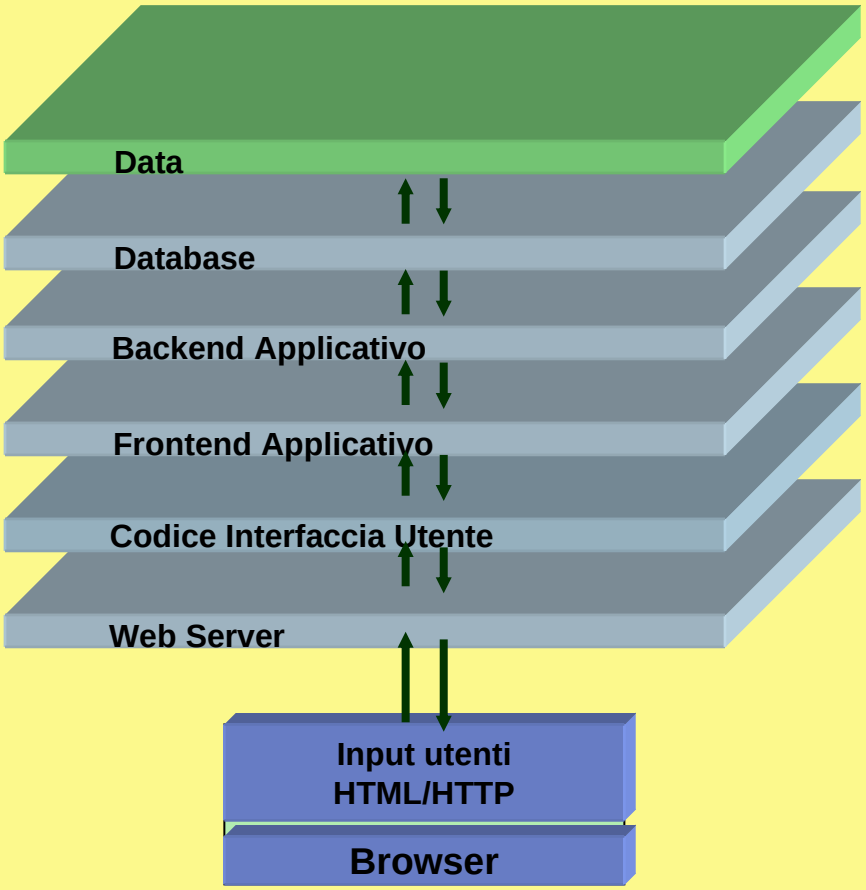


75% degli attacchi alla sicurezza informatica sono diretti verso il livello delle applicazioni Web

2/3 di tutte le applicazioni Web sono considerate vulnerabili

Sources: Gartner

Come è fatta un'applicazione Web e perchè può essere vulnerabile?



I flussi di input e di output passano attraverso ogni livello dell'applicazione.

Una vulnerabilità in uno dei livelli può causare danni all'intera applicazione.

Le soluzioni di sicurezza per la infrastruttura non indirizzano questa problematica

- **Firewalls e IPS (Intrusion Prevention System) non possono bloccare tutti gli eventuali attacchi al livello applicativo**
  - La porta 80 deve essere disponibile per essere utilizzata
- **Strumenti di scansione della rete non identificano eventuali vulnerabilità applicative**
  - Nessus, IBM ISS, Qualys, Nmap, etc.
- **Chi sviluppa applicazioni Web non ha conoscenze adeguate di sicurezza applicativa**
  - 64% degli sviluppatori non sono confidenti di poter scrivere applicazioni sicure (fonte Microsoft Developer Research)

Maturità del modello di “Security Test”

Evoluzione della “Web Application Security”

Nothing

Oursourced

Vulnerability Assessment affidati a società specializzate per le applicazioni più critiche

In-House Tactical

Audit da parte dell’Ufficio Sicurezza e/o QA sulle applicazioni in Produzione o in Pre-Produzione

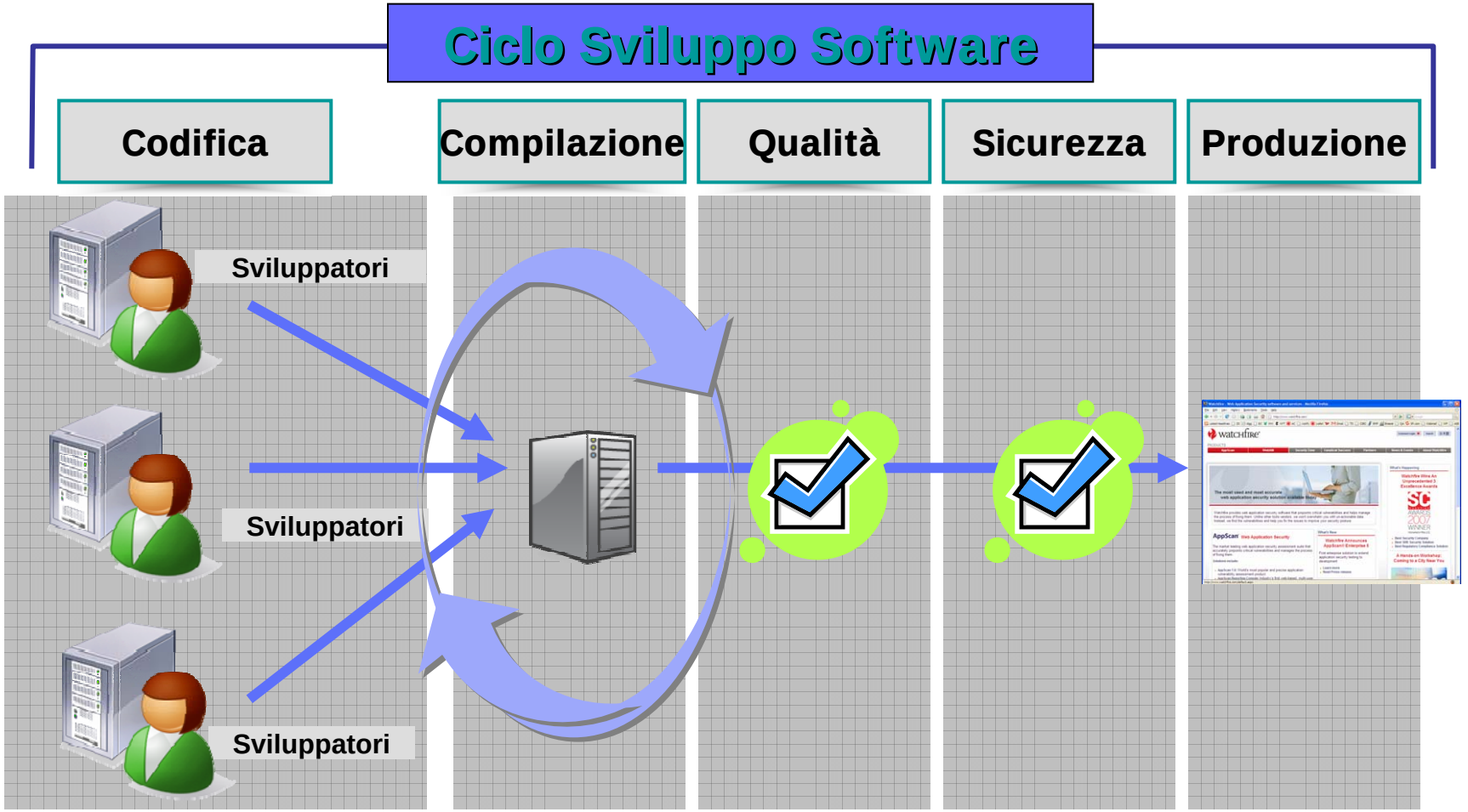
In-House Evangelization

Condivisione dei risultati degli Audit con gli Sviluppatori e definizione di metodologie di sviluppo sicure basate sulle “best-practice”

In-House Strategic

Sicurezza pienamente integrata nel ciclo di vita delle applicazioni e parte Integrante del processo di Quality Assurance

Perchè è importante gestire la sicurezza durante l'intero ciclo di sviluppo?

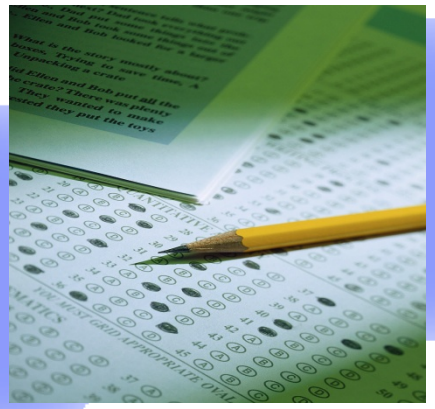


+ Qualità + Sicurezza = Riduzione Costi !!!!

L' 80% dei costi di sviluppo è speso per individuare e correggere i difetti!

During the **coding** phase
$25/defect

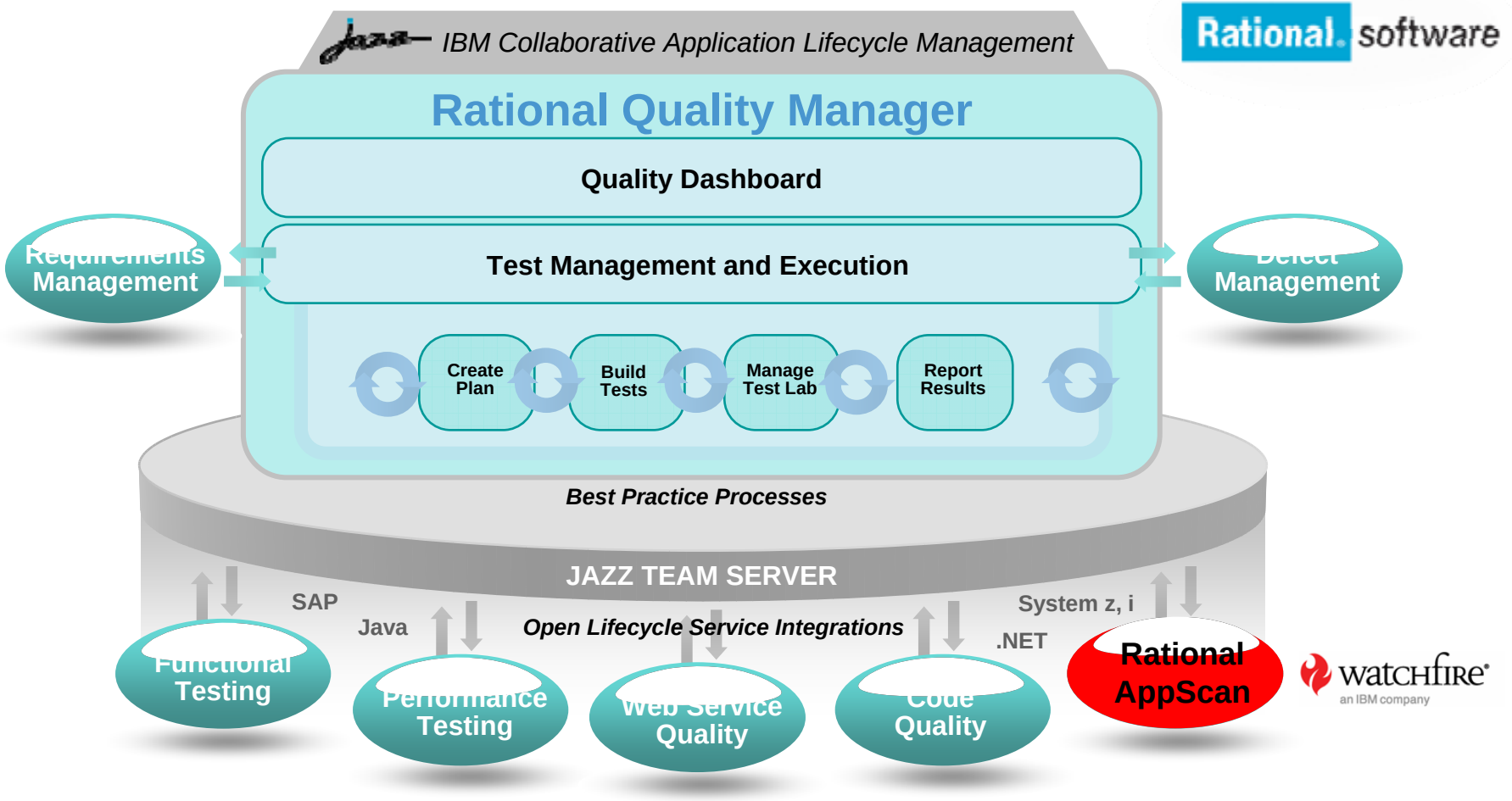
During the **build** phase
$100/defect



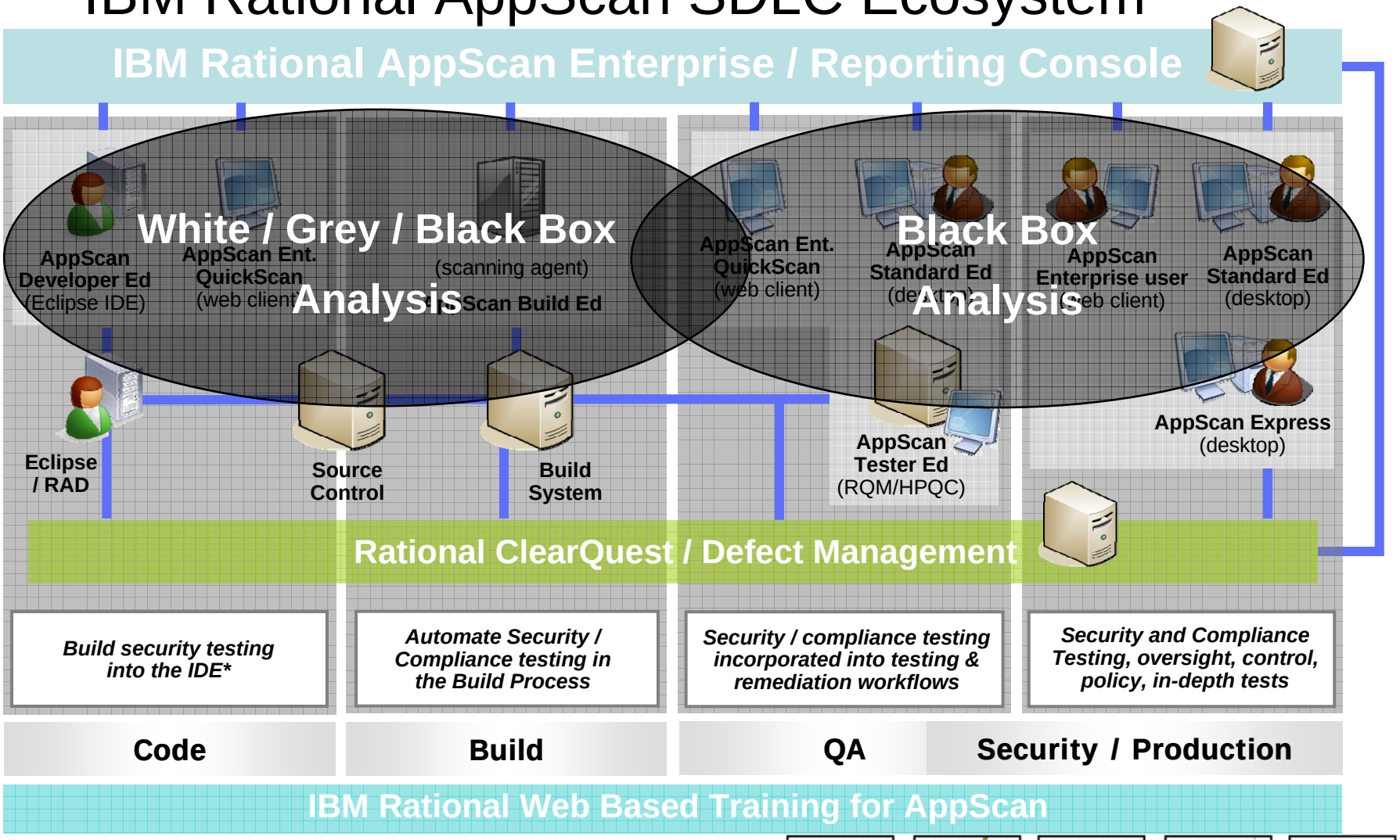
During the
QA/Testing phase
$450/defect

Once released as a product
$16,000/defect

Rational Software Quality Management



IBM Rational AppScan SDLC Ecosystem



D O M A N D E ?

Learn more at:

- IBM Rational software
- IBM Rational Software Delivery Platform
- Process and portfolio management
- Change and release management
- Quality management
- Architecture management
- Rational trial downloads
- developerWorks Rational
- IBM Rational TV
- IBM Rational Business Partners