



# Application Security

**OWASP**  
31-07-July

**Jamuna Swamy**  
**Speaker**  
**Hexaware Technologies**  
jamunas@hexaware.com  
9790997743

Copyright © The OWASP Foundation  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the OWASP License.

**The OWASP Foundation**  
<http://www.owasp.org>

# Application Security

## ■ Agenda

- ▶ Threats Landscape
- ▶ Application Threats
- ▶ Survey Samples
- ▶ Secure SDLC Process
- ▶ Security \_ Non functional requirements
- ▶ Mitigation
- ▶ Awareness Level
- ▶ Role of OWASP

# Threats Landscape

- Non availability of resources, Data integrity loss, loss of confidentiality of sensitive information
  - ▶ Attack can be directly on to the information
  - ▶ Attack can be through application vulnerability
  - ▶ Attack can be internal
  - ▶ Attack can be from outside
  - ▶ Attack can be compromising the IT infrastructure
  - ▶ Attack due to Natural Disaster/Man made disaster

# Application Threats

- Social Engineering
- Non segregation of Duties
- Improper Control Validation
- Improper coding
- Improper Security Testing
- Non availability/ non execution of compensating controls

# Confidence in house developed applications



- A majority of applications in use at our organization are commercial off-the-shelf applications. 23%
- Not at all confident - we haven't done enough to assess and mitigate vulnerabilities. 20%
- Somewhat confident - we haven't had any issues to date. 35%
- Very confident - we've assessed our risks and tested our security. 22%

# Confidence in third party applications



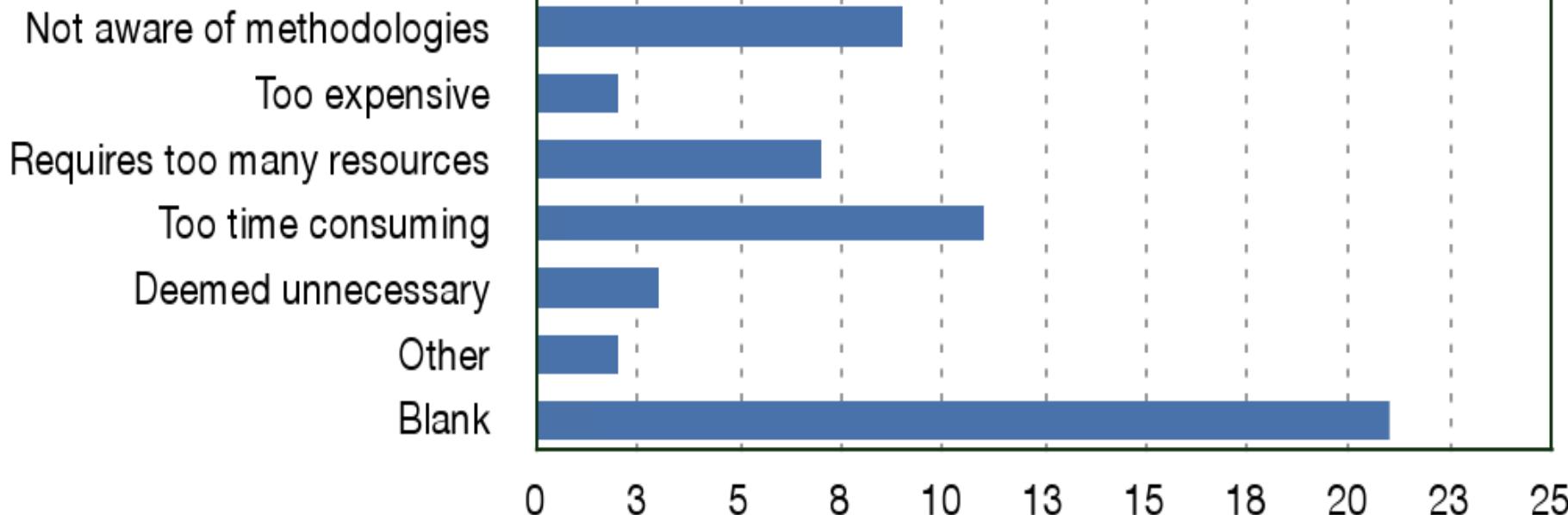
Not at all confident - they haven't done enough to assess and mitigate vulnerabilities. 21%

Somewhat confident - we haven't had any issues to date. 60%

Very confident - they've assessed their risks and tested their security. 19%

# Reasons for not adopting Secure Coding Practices

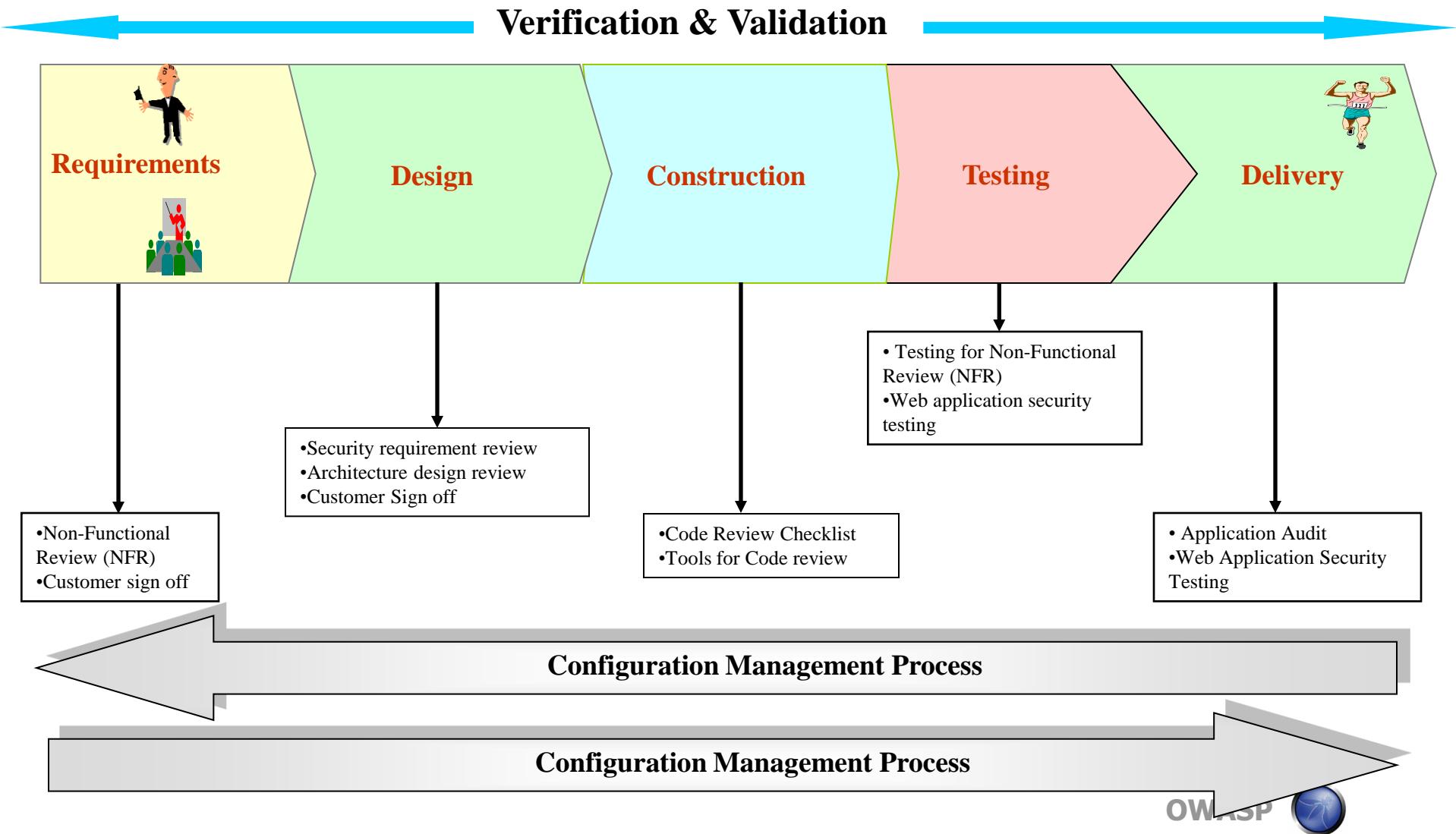
Reasons for Not Adopting



# Driven by PCI DSS Compliance

5. In your recent experience, how much of an organizations Web application security program is driven by PCI-DSS today?		Response Percent	Response Count
A lot (otherwise we'd do nothing)		19.1%	57
Influenced somewhat		47.3%	141
Little to none		33.6%	100
Comments		comments	40
Answered question		answered question	298
Skipped question		skipped question	42

# Secure Software Development Lifecycle



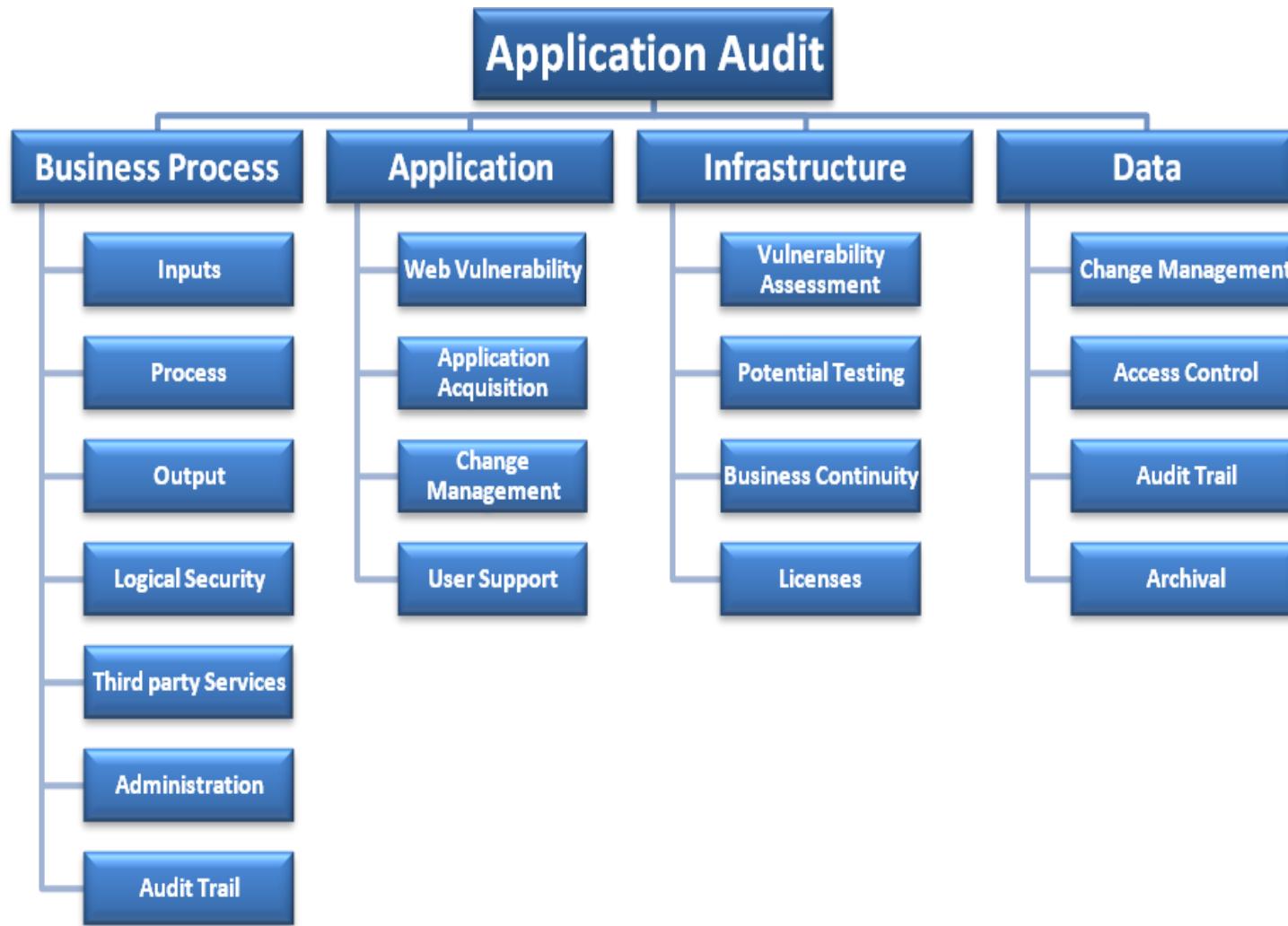
# Security- Non Functional Requirements

- Validations ( input, Processing, Output)
- Identification & Authentication
- Entitlements
- Operational Configurations
- Implementation Configurations
- Audit Trail
- Segregation of Duties

# Mitigation

- Application Security as part of Enterprise Risk Management Program
- Design Review
- Code review using coding standards
- Security Testing as part of System Testing
- Application Audit at frequent intervals
- Application weaknesses to be compensated by administrative controls

# Application Audit - Definition



# Awareness Level

- It is at minimum and slowly improving
- Should be encouraged through forums like ISACA, OWASP, CLASP etc.
- Security Testing should be mandated as part of SDLC framework
- Training, workshop on continuous basis on new threats and mitigation

# OWASP Role

- Should be lauded for pioneering in this area
- Collaborate with other organizations like ISACA, CSI to reach more people

# Q & A