Penetration Testing

How Government Can Achieve Better Outcomes

Delivered by Murray Goldschmidt, Chief Operating Officer

Cyber Security for Government Conference, 25&26 October 2011, Sydney

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd

Sydney
Level 8, 66 King Street
Sydney NSW 2000
Australia

Melbourne
Level 10, 401 Docklands Drv
Docklands VIC 3008
Australia

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

Penetration Testing

Penetration Testing

- is a series of activities with the objective to determine current technical security posture
- includes testing of effectiveness of protective controls which can be used to [6,7]:
  - deduce effectiveness of detective & responsive controls
  - identify opportunities for improvement in information security governance (in support of ISM/S)
- is one security assessment method

Why?

Because

"Foolproof systems don't take into account the ingenuity of fools." — Gene Brown.

Agenda

- Effective Outcomes:
  - Dependencies
  - Getting the Balance Right
    - Balance - Making Informed Decisions
    - Depth of Testing vs Time
  - Cloud & Regulation - AU Govt
  - Pen Testing – The Broader Picture
  - Conclusions

Effectiveness of Outcomes

Dependent on:

Limitations

- Point in time
- Environmental (test/dev/prod)
- Negative testing (only proves the presence of flaws)
- Funding is finite
- Business Continuity
- Resources to remediate
- Abused as check box testing (compliance)

Constraints

- Scope
- Time
- Budget

Capability

- Methodology/approach
- Experience
- Skill
- Tools

Deliverable

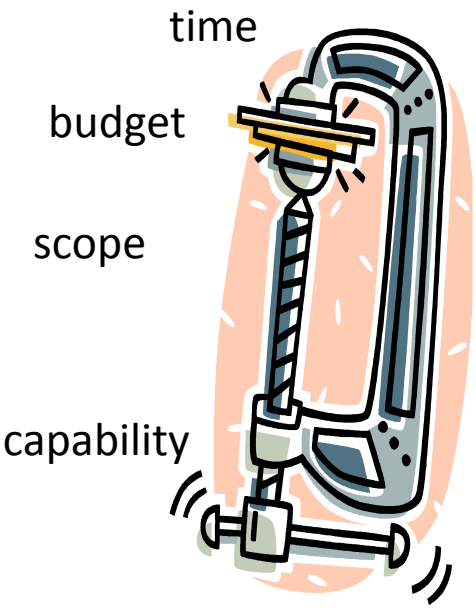
- Ease of use
- Accuracy of findings (no false positives)
- Ability to articulate technical & business risk
- Technical findings should include precise actions to remediate
- Anatomy of attack should incl all details to reproduce the exploit
- Root cause analysis (fix the cause not symptom)
- Exec Summary with adequate info for C Level
- Threat/Risk centric not system centric

Agenda

- Effective Outcomes:
  - Dependencies
  - Getting the Balance Right
    - Balance - Making Informed Decisions
    - Depth of Testing vs Time
  - Cloud & Regulation - AU Govt
  - Pen Testing – The Broader Picture
  - Conclusions

Where is the Squeeze?

- Time
- Budget
- Scope
- Capability



Implication on Outcome?

A Good Outcome?

No issues!

A Good Outcome?

Client side attack

Input validation

Click jacking

Remote control

Trojan

Buffer overflow

File upload

Man in the middle

User Enumeration

Cookie hijacking

SQL injection

A Good Outcome?

It's Up to You

The outcome is a function of the inputs

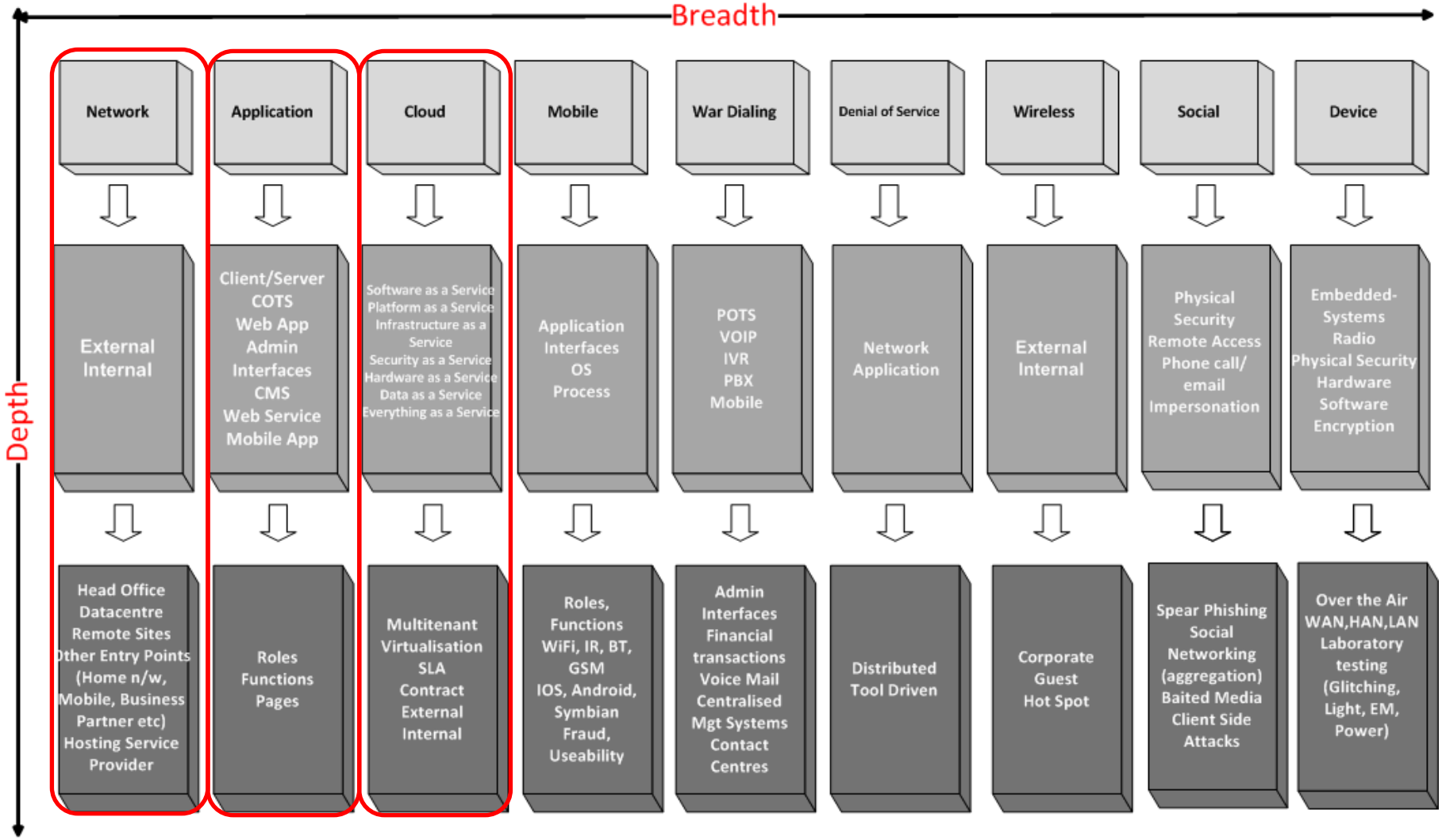
Before Testing

- Determine what it is that you are protecting
- Determine implication of a breach
- Know your data:
  - Where is it?
  - What is it?
- Risk Assessment – define depth and breadth of scope

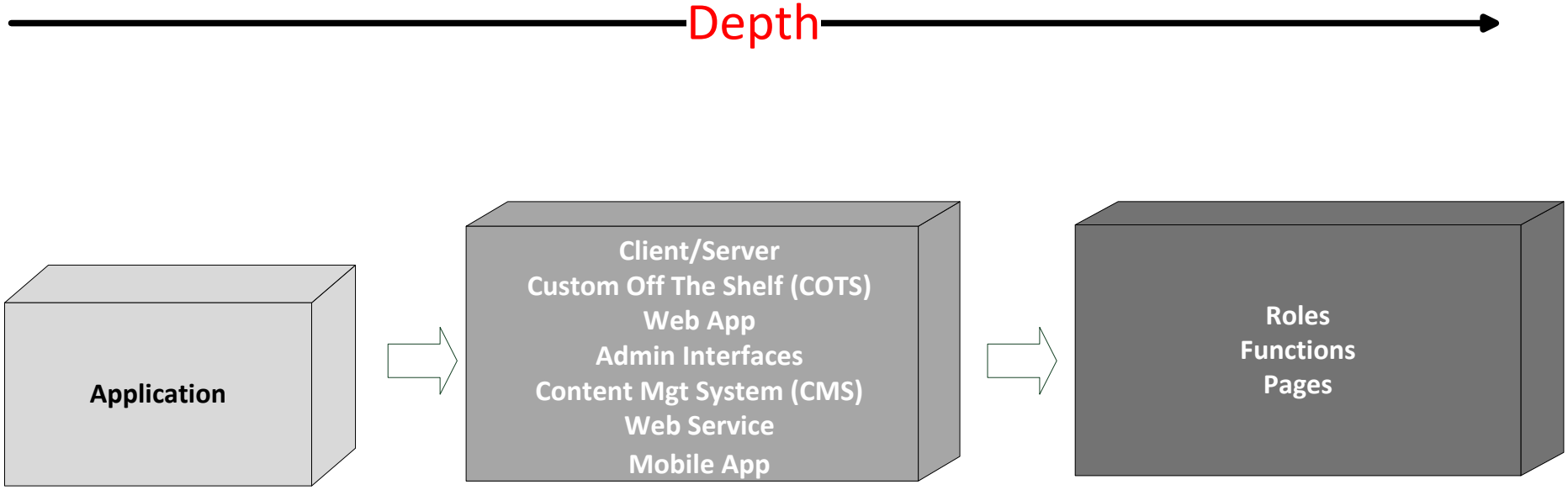
Agenda

- Effective Outcomes:
  - Dependencies
  - Getting the Balance Right
    - Balance - Making Informed Decisions
    - Depth of Testing vs Time
  - Cloud & Regulation - AU Govt
  - Pen Testing – The Broader Picture
  - Conclusions

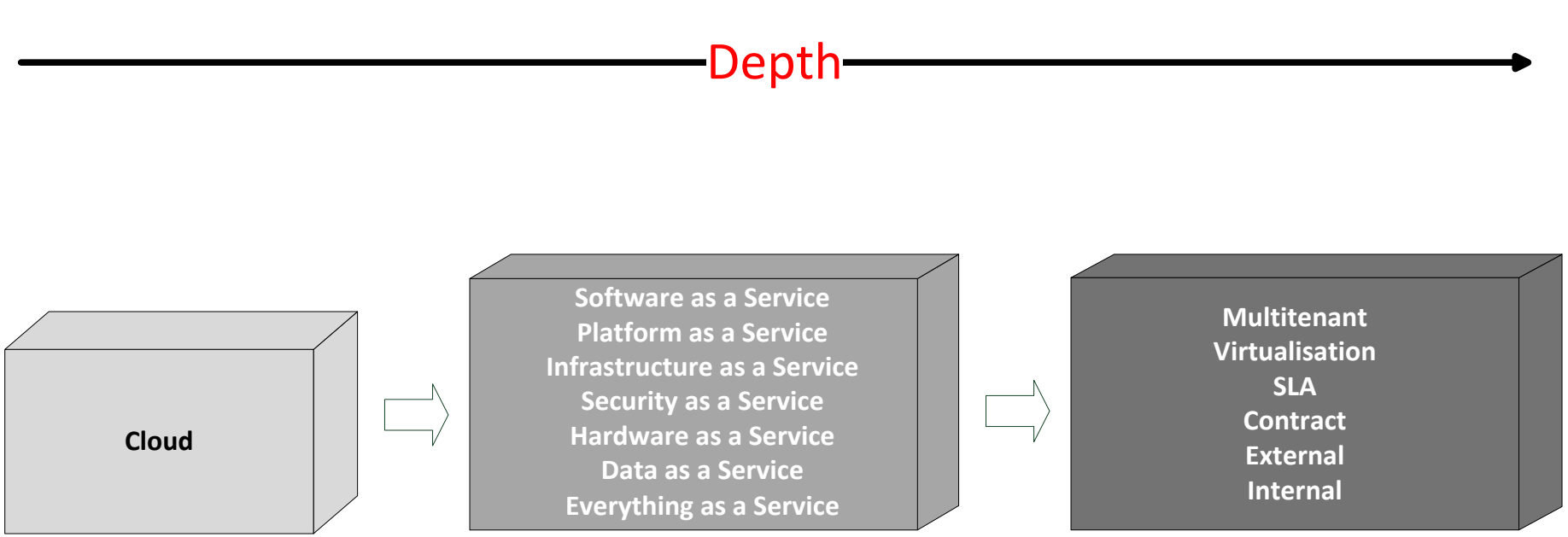
Breadth & Depth of Scope



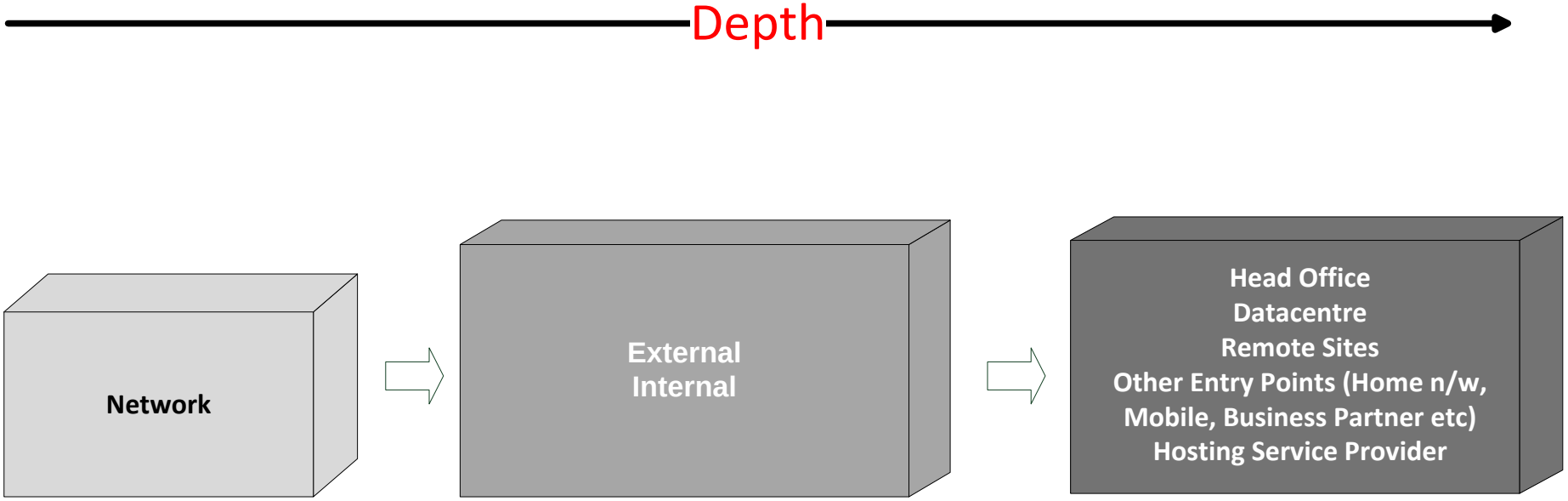
Breadth & Depth of Scope



Breadth & Depth of Scope



Breadth & Depth of Scope



Capability

Methodology → **DISCIPLINES:**
Network
Application
Social Engineering
Advanced Persistent Threat
Cloud
Mobile
Wireless

Experience → **MATURITY:**
Heritage
Track Record
Research Lab
Vulnerability
Analysis

Skill → **COMBINATION:**
Fundamentals (Network, Operating System, Application)
Intuition
Process
Finesse & Accuracy

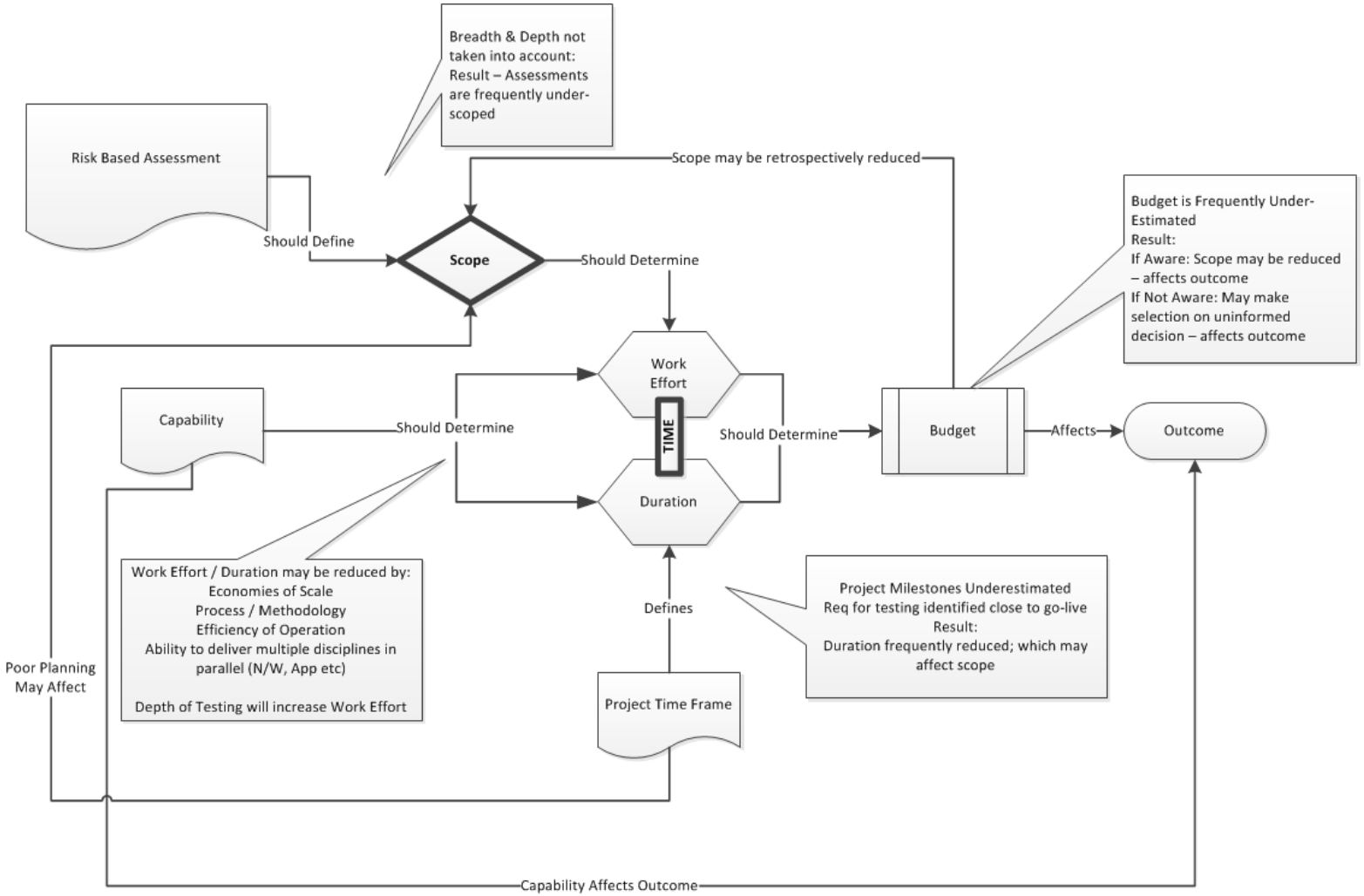
Tools → **SUITE:**
Open Source (various)
Commercial (various)
Custom Written (various)
Custom Written Exploit Code

Me

Time & Budget

- Risk Assessment should define scope
- Budget buys you time
- Time dependent on scope (breadth & depth) and capability
- An underestimated budget will impact:
  - Time
  - Scope
  - Capability
- Outcome is affected

Time & Budget



Interdependencies, aligned with commonly accepted methodologies: PRINCE2 and PMBOK

Agenda

- Effective Outcomes:
  - Dependencies
  - Getting the Balance Right
    - Balance - Making Informed Decisions
    - Depth of Testing vs Time
  - Cloud & Regulation - AU Govt
  - Pen Testing – The Broader Picture
  - Conclusions

Depth of Testing vs Time

- Short timeframe – limited expectation:
  - Run scan tools
  - High-level research specialised tools and techniques
  - Execute and validate findings
  - Write report – some findings might be generic without detailed technology specific fixes
- Reasonable Timeframe – Value oriented outcome
  - Do all above
  - Familiarise with new technology
  - Download and install software and look for bugs or potential mis-configuration options that can be set by user
  - Write custom tools and exploit code
  - Write detailed report with technology specific recommendations that can be implemented without the customer having to do any additional research

Agenda

- Effective Outcomes:
  - Dependencies
  - Getting the Balance Right
    - Balance - Making Informed Decisions
    - Depth of Testing vs Time
  - Cloud & Regulation, AU Govt
  - Pen Testing – The Broader Picture
  - Conclusions

Cloud & Regulation – AU Govt

- WoG policy position on Cloud Computing: “Agencies may choose cloud-based service where they demonstrate value for money and adequate security”[1]
- … take all reasonable steps to monitor, review and audit agency information security effectiveness, including assigning appropriate security roles and engaging internal and/or external auditors and specialist organisations where required [2]
- … have an obligation to protect the personal information that they hold from loss or misuse and unauthorised access, modification or disclosure [5]
- DSD recommends against outsourcing information technology services and functions outside of Australia, unless agencies are dealing with data that is publicly available.[4]
- Applicability of the Protective Security Policy [3]

Agenda

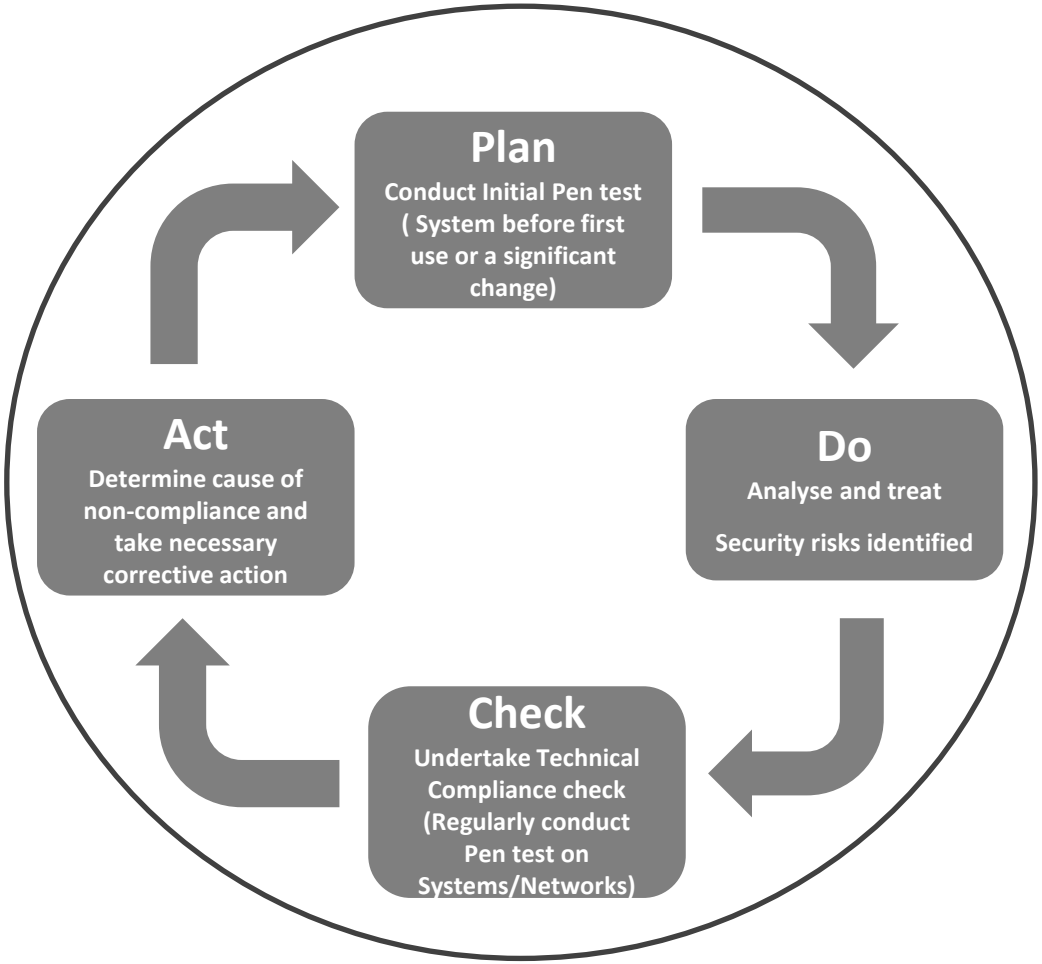
- Effective Outcomes:
  - Dependencies
  - Getting the Balance Right
    - Balance - Making Informed Decisions
    - Depth of Testing vs Time
  - Cloud & Regulation - AU Govt
  - Pen Testing – The Broader Picture
  - Conclusions

Where Does Pentesting Fit In?

Information Security Monitoring

Requirements from Standards and Regulatory Frameworks

AUS Gov - ISM
ISO 27001/2
PCI DSS



Compliance with security standards and regulatory requirements thereby improving the Security Posture

Agenda

- Effective Outcomes:
  - Dependencies
  - Getting the Balance Right
    - Balance - Making Informed Decisions
    - Depth of Testing vs Time
  - Cloud & Regulation - AU Govt
  - Pen Testing – The Broader Picture
  - Conclusions

Conclusion

- Know your data; think data centric not system centric
- Know what you need to test – Risk Assessment to define scope
- Breadth & Depth of scope; work effort (cost) should reflect
- Due to sophistication of attacks, increased requirement for expertise; cannot rely on tools
- Make informed decisions – outcome related to inputs
- Capability a function of methodology + skill + heritage + reporting
- Quality of reporting should be evaluated (Tech+Exec); affects ability to remediate; need to be able to act on the outcome
- Comprehensive testing will cost more than a check box test
- Cloud is an extension of your organisation; risks must be evaluated and treated accordingly
- Use the pentest as an opportunity to evaluate/tune your detection + response capability

References:

[1] Australian Government Cloud Computing Strategic Direction Paper, Dept of Finance, April 2011 Version 1.
http://www.finance.gov.au/e-government/strategy-and-governance/docs/final_cloud_computing_strategy_version_1.pdf

[2] Australian Government Protective Security Policy Framework, AGD, Jan 2011, V1.2
http://www.ema.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_Contents

[3] Securing Government Business. Protective Security Guidance for Executives, AGD, June 2010
http://www.ag.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_ProtectiveSecurityPolicyFrameworkDownloads

[4] Cloud Computing Considerations. DSD, April 2011
http://www.dsd.gov.au/publications/Cloud_Computing_Security_Considerations.pdf

[5] Privacy and the Cloud – speech to Cloud Computing Conference and Expo – 9/9/2010 Office of the Privacy Commissioner.
http://www.privacy.gov.au/materials/types/download/9572/7133

[6] Western Australian Auditor General's Report. Information Systems, Report 4, June 2011.
www.audit.wa.gov.au/reports/pdfreports/report2011_04.pdf

[7] Victorian Auditor-General's Report *Security of Infrastructure Control Systems for Water and Transport,* October 2010
download.audit.vic.gov.au/files/20100610_ICT_report.pdf

[8] Analyzing the Accuracy and Time Costs of Web Application Security Scanners, Larry Suto, Feb 2010

Questions?

Thank you

Recognised as Australia's fastest growing information security and risk management consulting firm through the Deloitte Technology Fast 50 & BRW Fast 100 programs

This presentation will be published at
http://www.senseofsecurity.com.au/research/presentations

Whitepaper will be published at
http://www.senseofsecurity.com.au/research/it-security-articles

Sydney, Melbourne
T: 1300 922 923
info@senseofsecurity.com.au
www.senseofsecurity.com.au