

Cyber Security- A Challenge Shared

Colin Murphy

Auditor General for Western Australia
Office of the Auditor General Western
Australia



Cyber Security - a challenge shared

Colin Murphy
Auditor General for Western Australia

30 September 2011





Today's presentation

1) Information systems performance audit (2011)

- Cyber security in government agencies

2) Ongoing application and general computer controls audits

- Application controls
- General computer controls





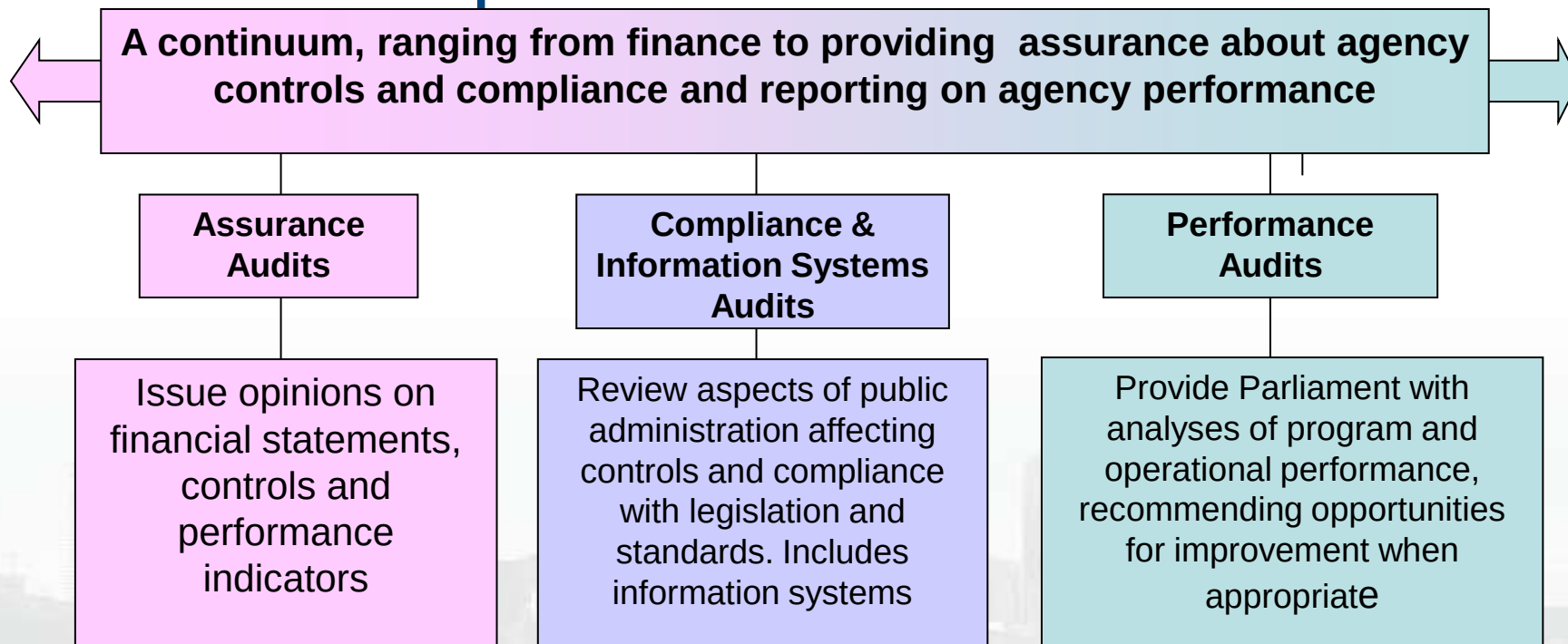
The role of the AG

- Provide information to Parliament
- Independent and impartial
- Public sector accountability
- Serving the public interest





Reports to Parliament





Information Systems audits

Previous reports:

- cyber security
- databases and portable storage devices
- personal and sensitive information
- disposal of hard drives
- wireless security
- critical infrastructure
- virus protection
- ongoing capability maturity models





Cyber security in Government agencies

- **Reliance** - WA government agencies rely heavily on the Internet to deliver services and conduct business
- **No boundaries** - an Internet presence exposes agency computer systems to “cyber attack” from anywhere in the world
- **Real risk** - the cyber security threat is no longer an emerging threat - it exists now and is growing
- **Internal threat** - a risk not often considered is the risk of attack from within



What did we do?

Assessed the ability of fifteen agencies to detect and respond to cyber threats, using:

- Scans
- USBs
- ECU – Security Research Centre
- Police involvement



USB
Key

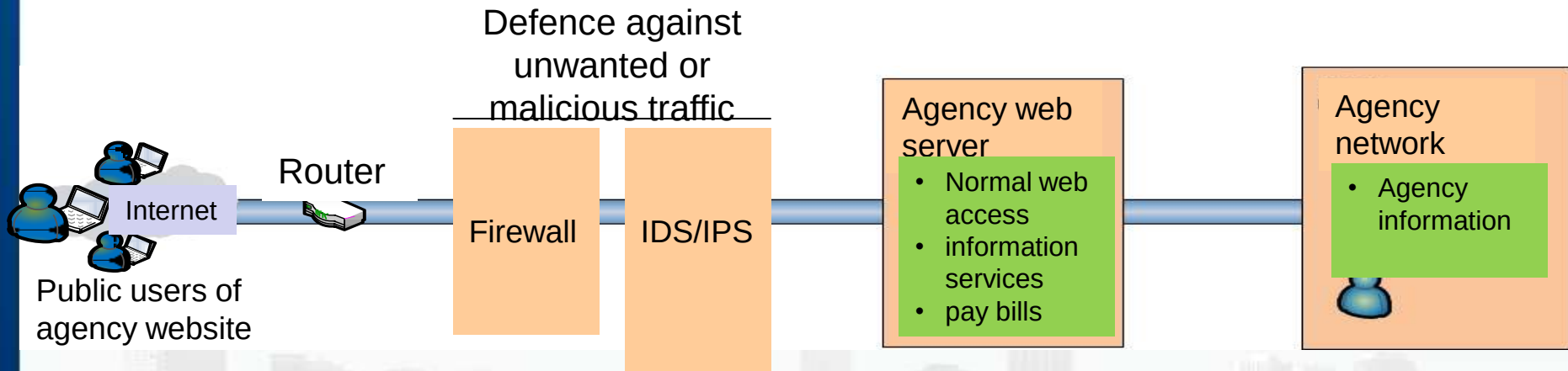


What we found...

- Fourteen of fifteen agencies failed to detect, prevent or respond to any of our hostile scans
- We accessed the internal networks of three agencies without detection
- Eight agencies plugged in and activated the USBs we left lying around
- Agencies lack of a risk based approach to computer security

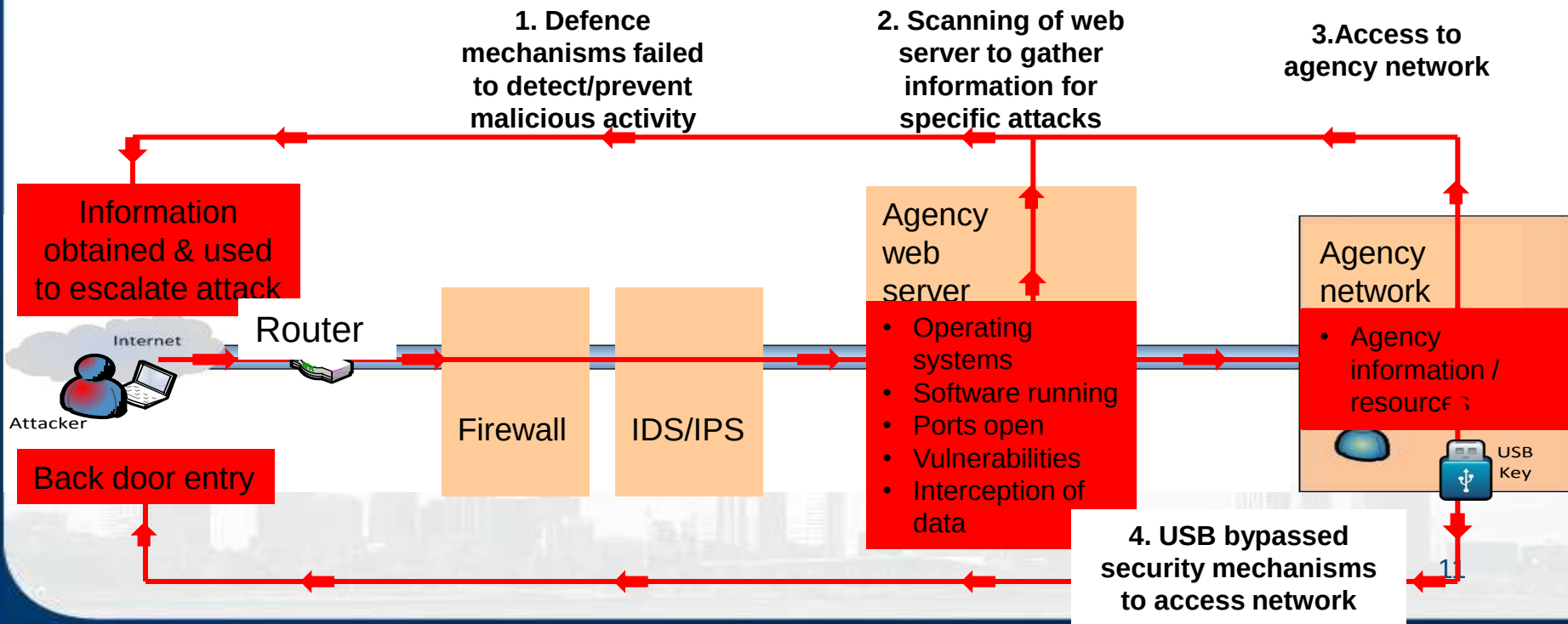


Simple representation of an agency with an internet web site





What we found...





Extensive media coverage...



WA govt open for cyber

Updated: 17:01, Wednesday June 15, 2011

At least 14 West Australian government agencies don't or respond to a cyber attack, the auditor general has found.

The Office of the Auditor General engaged Edith Cowell University to conduct a security audit of 15 government agencies including the health, transport and the Fremantle Port Authority and Western Power.

In his report, the Auditor General said these attacks were prolonged and continuous in an effort to have the

Auditor General said the attacks

Delimiter

Just Australia. Just technology.

WA Govt has zero IT security

Featured News - Written by [Renai LeMay](#) on Wednesday, June 15, 2011



Western Australia's auditor-general has released a report which details the fact that none of a wider range of agencies in the state are currently able to protect themselves against their IT infrastructure — or even check for vulnerabilities.

In the report published today and available on the Delimiter website, it reveals his office recently conducted a security audit of 15 agencies in the state, including major agencies such as Health, those with sensitive information and the Attorney-General, and others such as



THE AUSTRALIAN

Watchdog cyber sting exposes security lapses

Amanda O'Brien, [The Australian](#), June 16, 2011 12:00AM

THE Barnett government is facing a major security scare after investigators hacked into a string of government departments and accessed confidential information without being detected.

The state's Auditor-General, Colin Murphy, used an elaborate sting operation over two months to test cyber security in 15 agencies holding sensitive data about businesses and individuals.

All but one agency did not even detect the cyber attack, shocking the agency watchdog.

Using simple software obtained from the internet, Mr Murphy was easily able to access passwords, documents and material that "simply should not have been accessed by anybody externally".



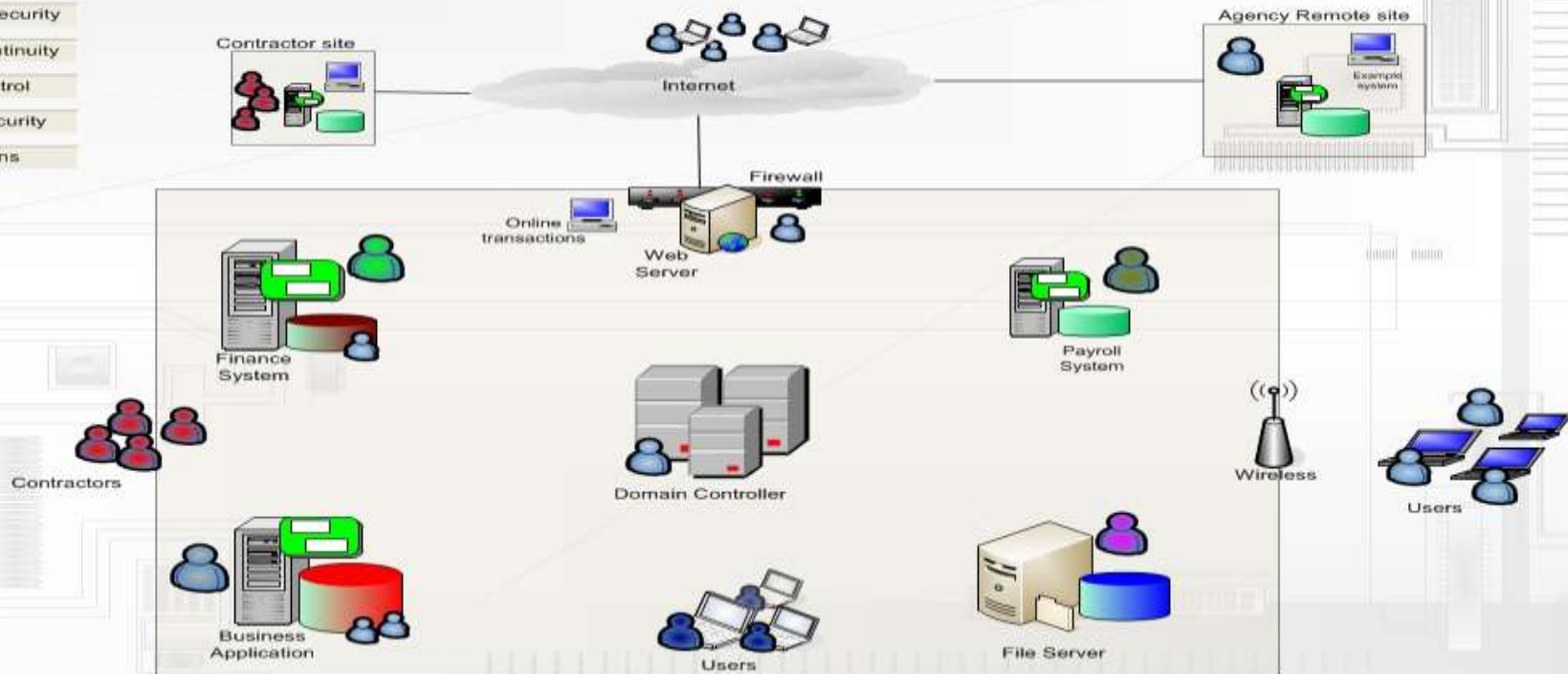
What should be done?

- Identify and manage information security risks within an overall risk management framework
- appropriately configure mechanisms for detecting cyber threats from the Internet
- perform regular information security awareness training for staff
- ensure they have a good understanding of the services being provided by security consultants



Computer controls

IT Risks
Information Security
Business Continuity
Change Control
Physical Security
IT Operations





Computer application controls

Each year we review a selection of key applications relied on by agencies to deliver services to the general public

- Failings or weaknesses in these applications have the potential to directly impact other organisations and members of the general public





What did we do?

We assessed adequacy of controls across five applications:

- Treasury and Finance - Office of Shared Services eBusiness
- Landgate - SLIP – Shared Land Information Portal
- Government Employees Superannuation Board - Capital
- Fisheries - FLAMS – Fishing Licensing and Management System
- Police - SAP – Enterprise Resource Planning System ERP

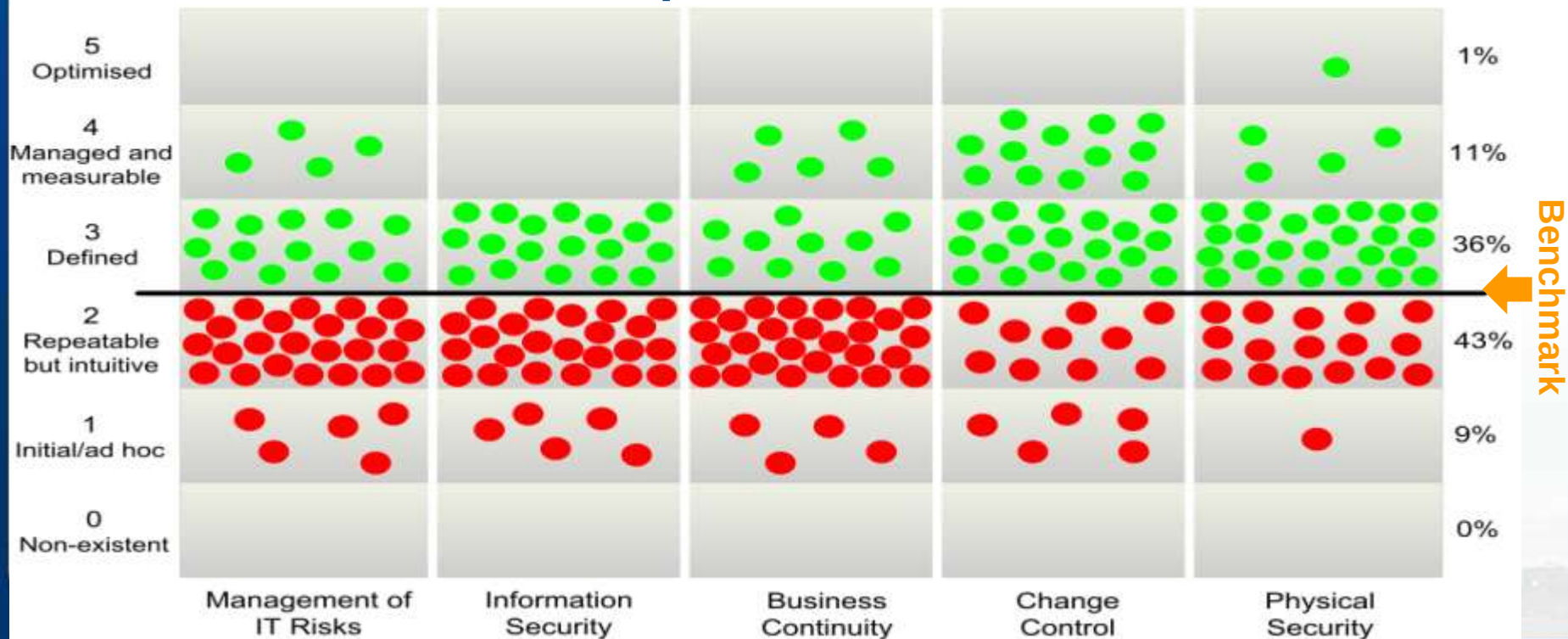


What we found... application controls

	Treasury & Finance	Landgate	GESB	Fisheries	Police	
Controls over data entered into the application to ensure it is accurate, complete and authorised						 Significant Moderate Minor No issue
Controls over data to ensure it is processed as intended in an acceptable time period						
Controls over stored data to ensure it is accurate and complete						
Outputs, including online or hardcopy reports, are accurate and complete						
A record is maintained to track the process of data from input, through the processing cycle to storage and to the eventual output						
Access controls are in place and user accounts are managed.						



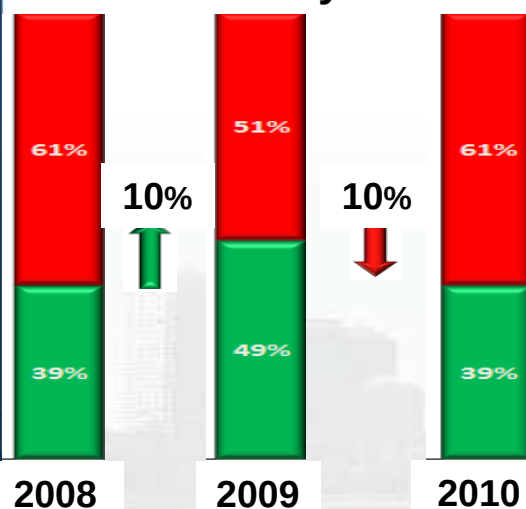
General computer controls audits



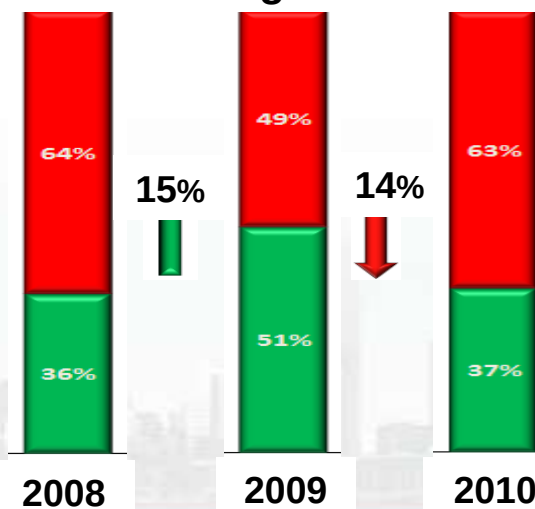


What we found – security, risk and continuity

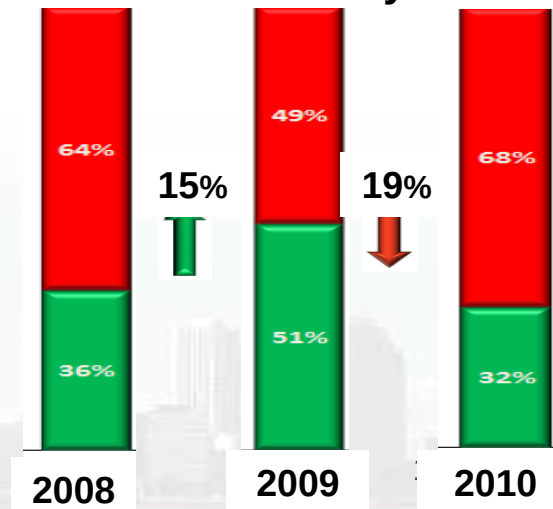
Information
security



IT risk
management



Business
continuity





What should be done?

Policies and procedures – should be in place for key areas

Manage IT risks – ensure risks are identified, assessed and treated

Information security – ensure good security practices are implemented

Business continuity – develop and test continuity and recovery plans

Change control – procedures should be developed and followed

Physical security – prevent unauthorised access and damage to systems



Future Information Systems audit program

- Forward strategy has been approved
- Focus on the areas of:
 - ICT governance
 - Cyber risk
 - Information security – agency gap analysis
 - Progress against key areas (capability assessments)
- *How will your agency measure up?*



Information Systems Audit Report

In summary:

- Provides a unique focus
- Impetus for change
- Internationally recognised
- Reference point for industry
- Significant amount of interest
- **Relevant for *all* agencies, including yours**





Thank you

Colin Murphy
Auditor General

Email: info@audit.wa.gov.au
Website: www.audit.wa.gov.au

