Cyber Security- A Challenge Shared

Colin Murphy

Auditor General for Western Australia

Office of the Auditor General Western Australia

Right Click 2011

Technology Communication Engagement Security

Institute of Public Administration Australia WA

Cyber Security - a challenge shared

Colin Murphy
Auditor General for Western Australia

30 September 2011

Office of the Auditor General
Serving the Public Interest

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

A continuum, ranging from finance to providing assurance about agency controls and compliance and reporting on agency performance

Assurance Audits	Compliance & Information Systems Audits	Performance Audits
Issue opinions on financial statements, controls and performance indicators	Review aspects of public administration affecting controls and compliance with legislation and standards. Includes information systems	Provide Parliament with analyses of program and operational performance, recommending opportunities for improvement when appropriate

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:

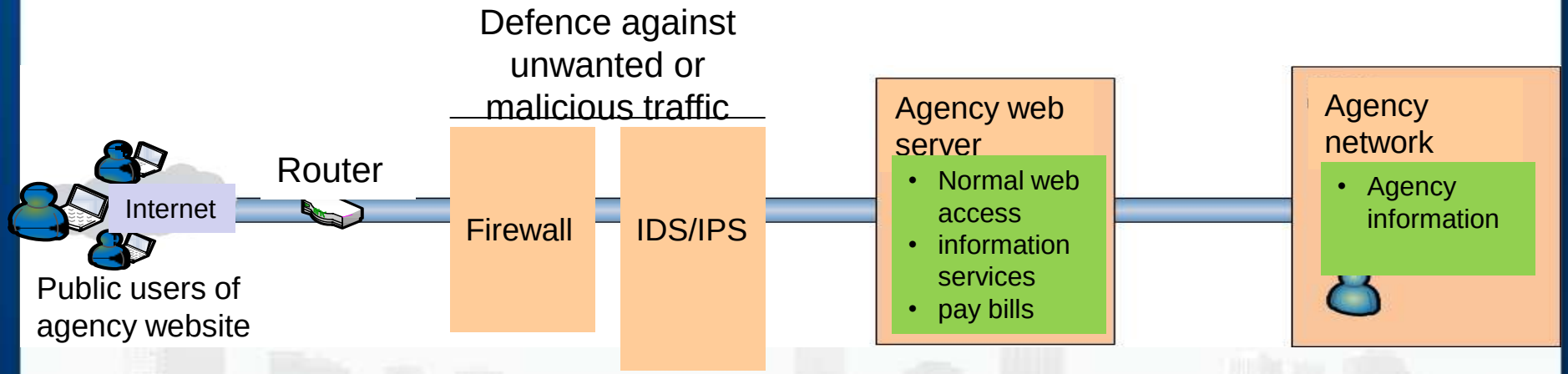
- Scans
- USBs
- ECU – Security Research Centre
- Police involvement

USB Key

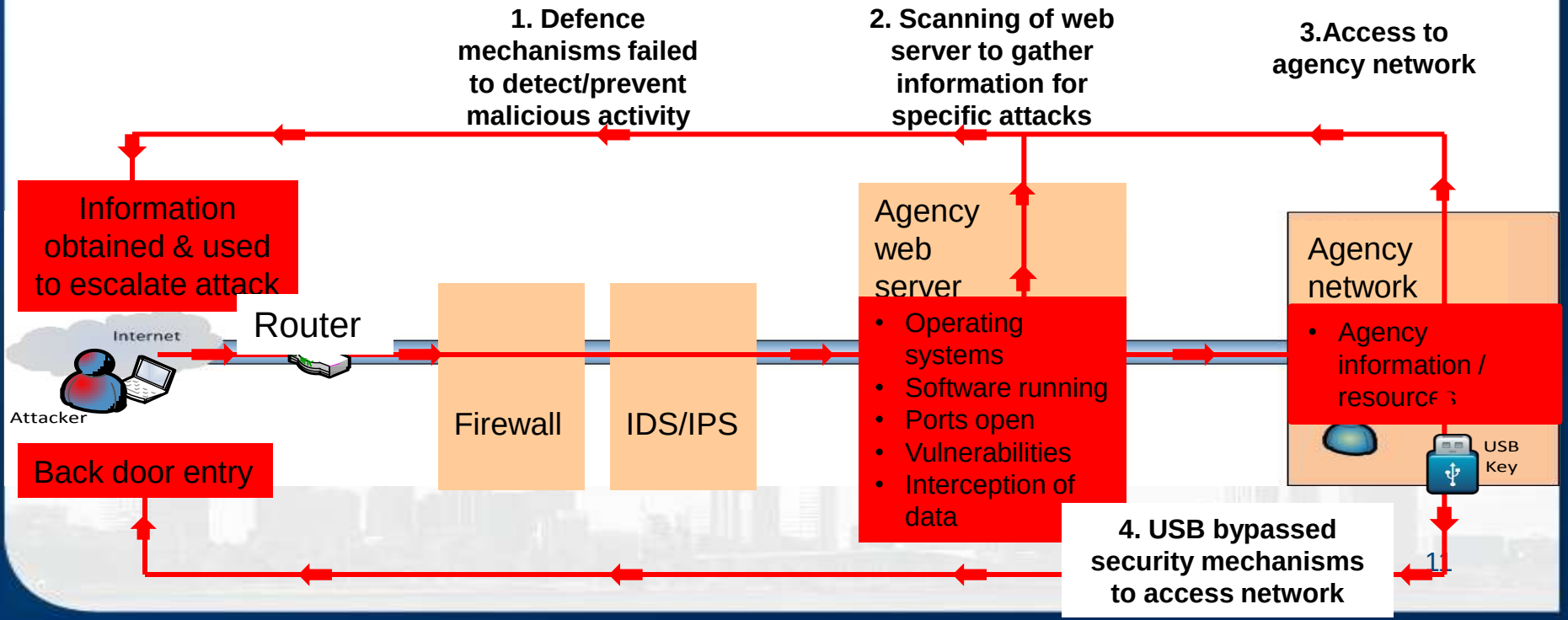
What we found…

- 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…



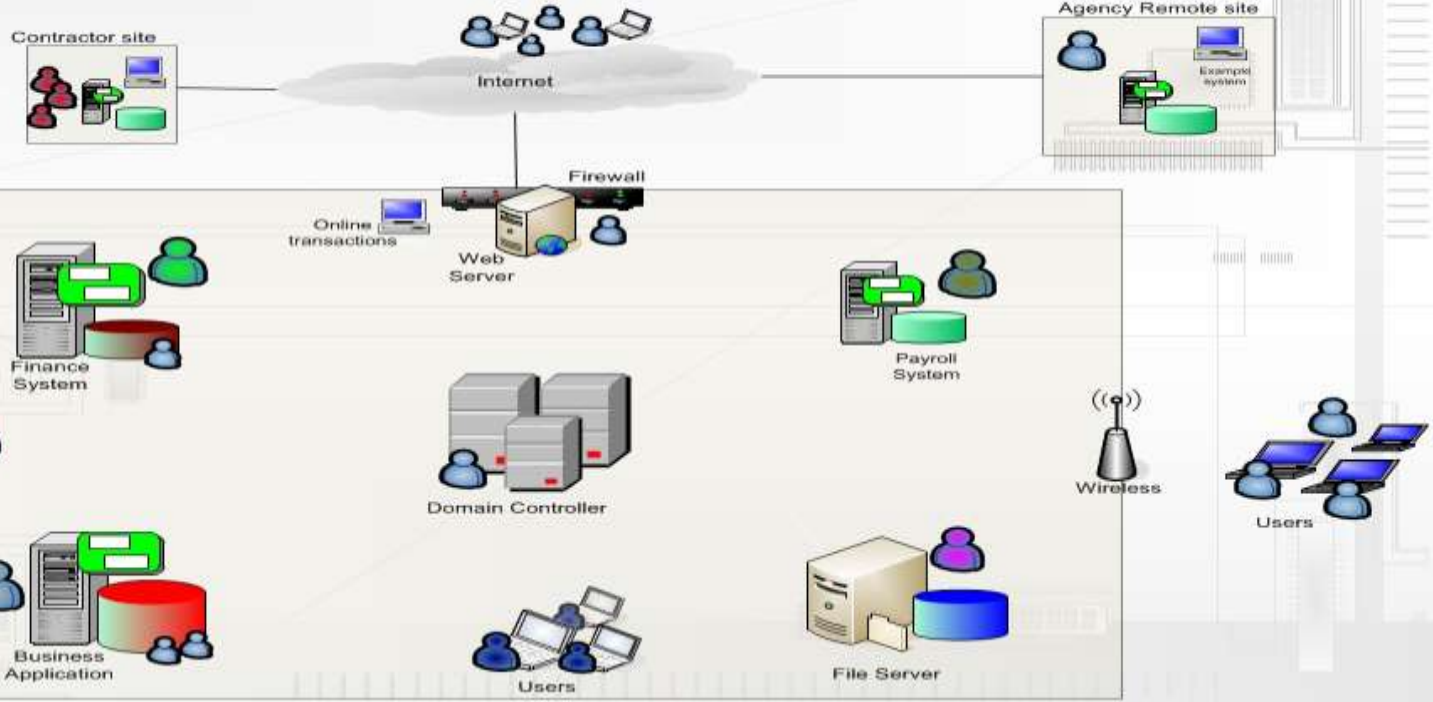
Extensive media coverage…

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

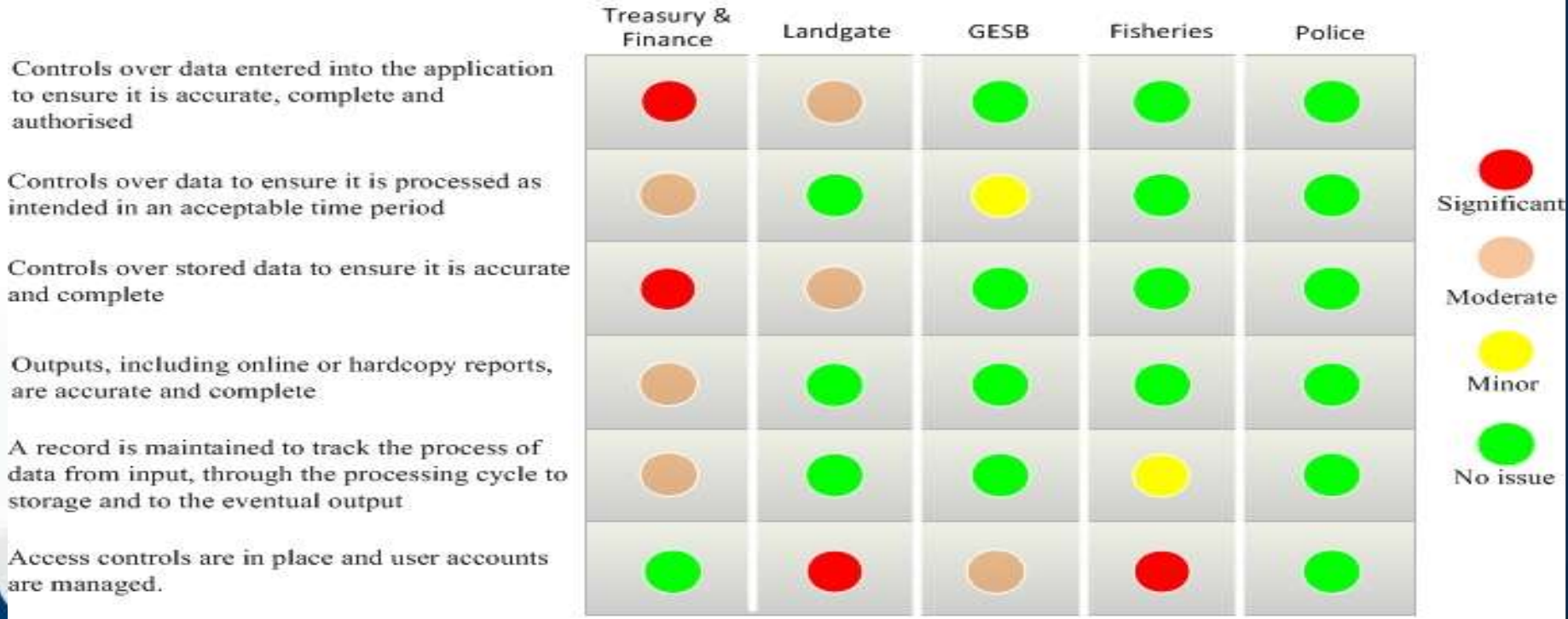
- Failings or weaknesses in these applications have the potential to directly impact other organisations and members of the general public

What did we do?

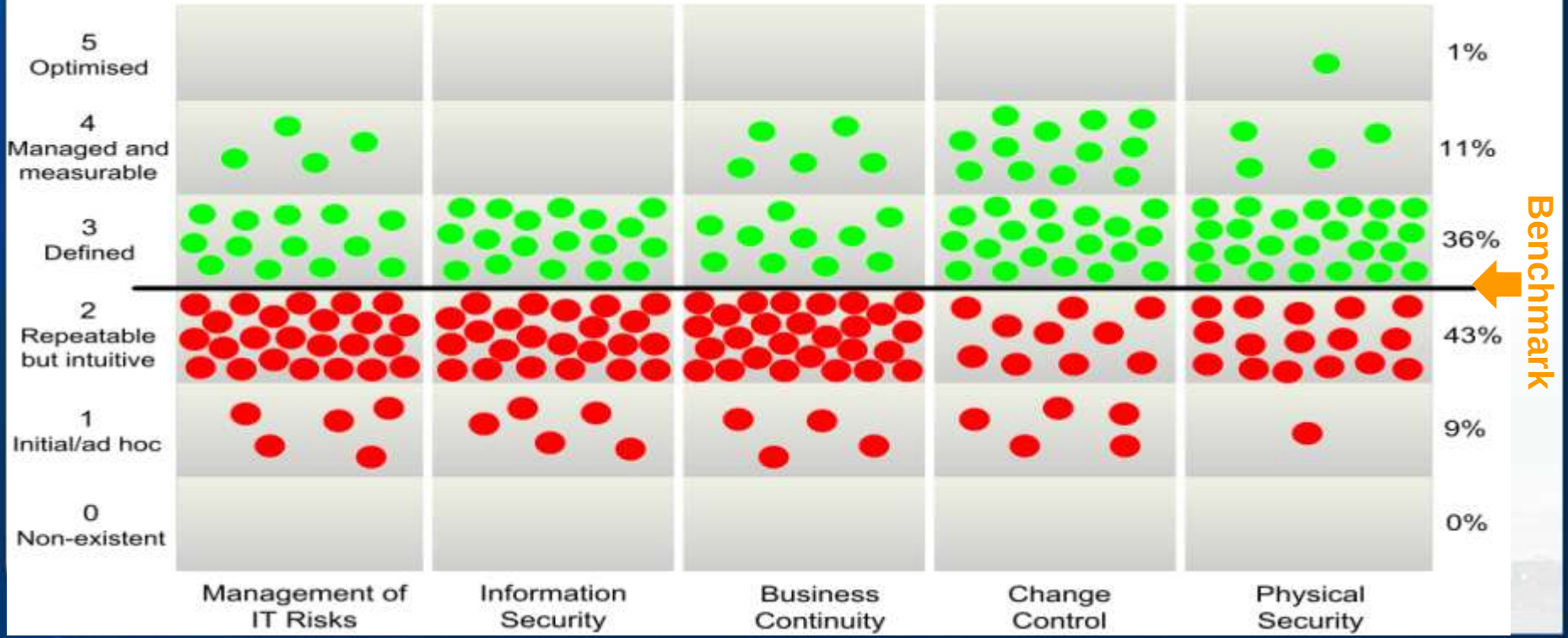
We assessed adequacy of controls across five applications:

- 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

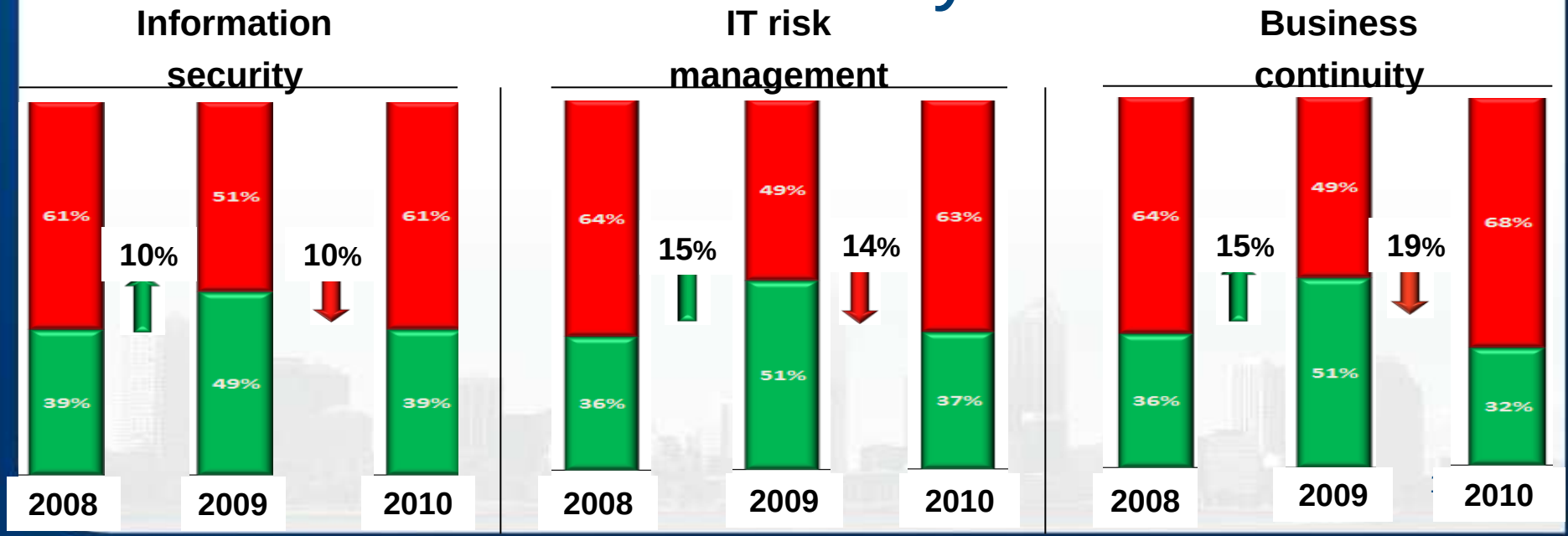
What we found… application controls



General computer controls audits



What we found – security, risk and 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