Information Security Manual

WHAT IT IS, AND ITS IMPACT ON PUBLIC SECTOR PROJECT DELIVERY

How this presentation is going to work….

- We’re pretty open, informal guys

- Everything we say is considered UNCLASSIFIED and the information is freely available to the public on the internet

- If you want to say something – Raise your hand and stop us! Speak Up!

- Everything we say is “Common Sense”!!!

AGENDA

- Who ARE we?
- What is the ISM?
- Common Misconceptions
- Common Issues
- Scenario 1
- Scenario 2
- Current Trends

- Q & A

Who are We?

OR WHY YOU OUGHT TO LISTEN TO US

James Mouat

- Wears a lot of hats (literally and figuratively);
- Career is focused on Information Security, Policy and Compliance Management;
- Background in Systems and Networking;
- Active in several local InfoSec communities;
- Regularly attends special interest groups and conferences such as Ruxcon, SIG, ACSC and ACS;
- Working on an ISM project on the side;
- Works on a multitude of private engineering projects;
- Works as a Visual-Jockey for nightclubs and festivals;
- Runs an FM Radio Station;
- All of the above WHILE renovating his house.

Kevin Landale

- Doesn’t like Hats, but tends to figuratively wear a fair few;
- Career is focused on Tech Consulting, Strategy and Project Management;
- Background in Networking, Business Analysis and Web Development;
- Active in several local technology-related communities;
- Regularly attends events by the ACS, Canberra Innovation Network, UNAA, ISACA, IIBA, etc.;
- Working as a casual tutor and mentor at the ANU;
- Working on a few side projects;
- Works as a photographer and blogger;
- Runs a blog;
- All of the above WHILE playing video games and reading manga.

What is the ISM?

What is the ISM?

- The Information Security Manual (ISM) is a publication by the Australian Signals Directorate (ASD) as the **standard** which governs Information Security of Government Information Technology Systems.

- It was originally called ACSI 33 until 2005, when it was renamed as the ISM.

- Updated and re-published on an Annual basis.

- The current edition was release in April 2015, and consists of 932 controls.

Common Misconceptions

Common Misconceptions

- IT Security are far too draconian! I want access to Facebook/Instagram/Snapchat !!!

- IT Security isn't important to this project. We'll worry about it later!

- The IT Security Approvals process for our system is too hard and takes too long! The IT Security team/branch take forever!

Common Misconceptions – BUSTED!

- IT Security are far too draconian! I want access to Facebook/Instagram/Snapchat !!!
    - <james to insert info>

- IT Security isn't important to this project. We'll worry about it later!
    - <james to insert info>

- The IT Security Approvals process for our system is too hard and takes too long! The IT Security team/branch take forever!
    - <james to insert info>

Common Issues

Common Issues

- Project Cost blow outs
- Project Schedule blow outs
- Inadequate internal skilled resources
- Inadequate understanding of the role of the ISM as a compliance tool

Common Misconceptions – BUSTED!

- IT Security are far too draconian! I want access to Facebook/Instagram/Snapchat !!!
    - <james to insert info>

- IT Security isn't important to this project. We'll worry about it later!
    - <james to insert info>

- The IT Security Approvals process for our system is too hard and takes too long! The IT Security team/branch take forever!
    - <james to insert info>

The Importance of the ISM

Importance of the ISM

- <James to recap high-level points about the importance of the ISM>

Scenario 1

Scenario 1

- Hypothetical product in the Cloud, some slides etc with…
- Make it super basic scenario, kinda like:
- Talk about commonly what happens; eg Business team engages cloud provider/consultant. Consultant & Business team sells a idea to exec. exec sign off on it and hand to technical people to nut out details; technical people sort out the stuff and sign off on it and then when it goes to UAT/Prod, talk to Security team about any holes/signoff - fail

Scenario 1 – Resolution

- Consultants understand Agency requirements. (ISM & ASD cloud computing security considerations - http://www.asd.gov.au/publications/protect/cloud_computing_security_considerations.htm)
- Business team engages with IT Security to help scope requirements with Solution provider
- Sell idea to Exec - oh look we should be compliant because of XYZ
- Technical dudes implement technical controls along with Solution provider
- Solution goes to UAT/Prod, have IT Sec review solution and audit effectiveness of security controls; provides feedback to Business team on residual risks.
- Business team can make an informed decision

Scenario 2

AUDIENCE PARTICIPATION

Scenario 2

- Anyone here with a scenario that they’re okay to discuss?
- Anyone?
- Anyone?
- Bueller?

Scenario 2

- Hypothetical product in the Cloud, some slides etc with…
- Make it super basic scenario, kinda like:
- Talk about commonly what happens; eg Business team engages cloud provider/consultant. Consultant & Business team sells a idea to exec. exec sign off on it and hand to technical people to nut out details; technical people sort out the stuff and sign off on it and then when it goes to UAT/Prod, talk to Security team about any holes/signoff - fail

Scenario 2 – Resolution

- Consultants understand Agency requirements. (ISM & ASD cloud computing security considerations - http://www.asd.gov.au/publications/protect/cloud_computing_security_considerations.htm)
- Business team engages with IT Security to help scope requirements with Solution provider
- Sell idea to Exec - oh look we should be compliant because of XYZ
- Technical dudes implement technical controls along with Solution provider
- Solution goes to UAT/Prod, have IT Sec review solution and audit effectiveness of security controls; provides feedback to Business team on residual risks.
- Business team can make an informed decision

Importance of the ISM – Recap

- Copy the previous Importance of the ISM slide and insert here.

Q & A

Thank You

James Mouat
@joflixen
http://james.mouat.net.au/ism/
http://au.linkedin.com/in/jamesmouat
Kevin Landale
@craftyninja
http://www.thecraftyandnudge.com
http://au.linkedin.com/in/landalekevin