Practical Tools for Privacy Audit

Laura Bell
Security Consultant
Lateral Security (IT) Services Limited

LATERAL | SECURITY

Privacy Audit

two words guaranteed to put fear into the hearts of men, women and c-level executives

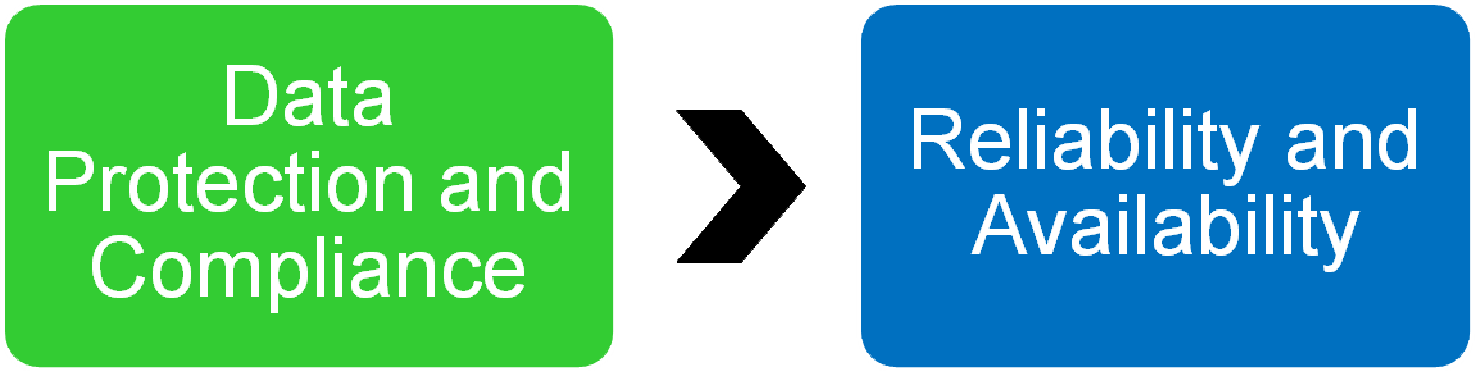
LATERAL | SECURITY

"Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data"

Guidance from the ICO, 27 March 2008 and 9 February 2010

LATERAL | SECURITY

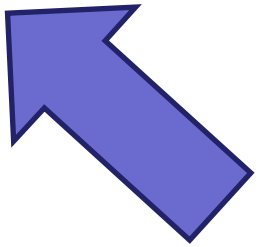
Audit Priorities



LATERAL | SECURITY

Privacy Frameworks

- COBIT – Document G13
- Global Technology Audit – Managing and Auditing Privacy Risks
- ISO/IEC 29100:2011 - Security techniques: Privacy framework



a little light reading

LATERAL | SECURITY

Types of Privacy Audit

Proactive

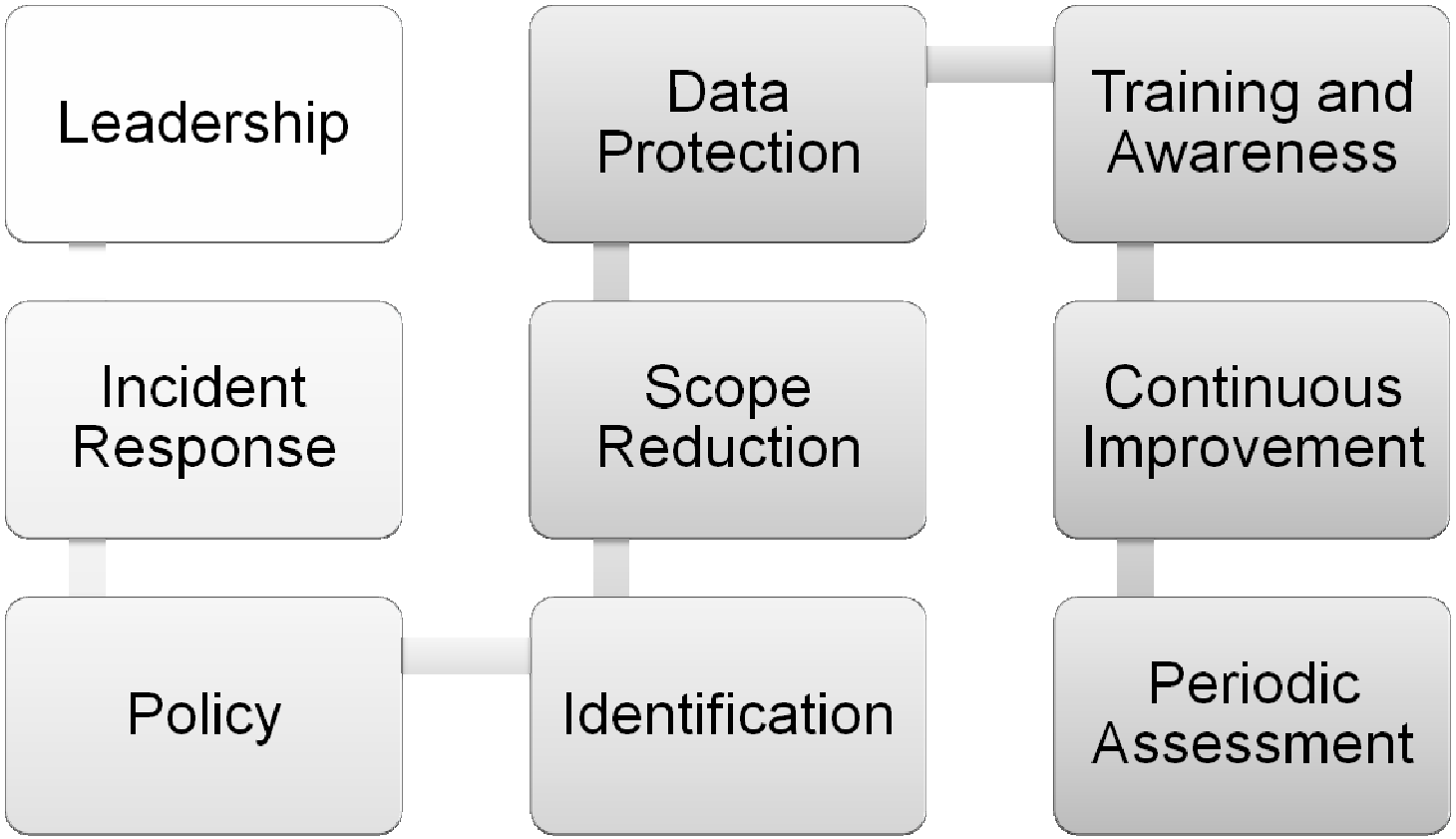
- Collaborative and transformational
- Know in advance what is really going on
- Fix before you fail
- Reduce risk
- Hard to justify, when nothing is burning

Reactive

- Adversarial and Punitive
- Most commonly occur when something has gone wrong (Google, Facebook)
- Damage assessment and limitation
- Often publicly scrutinised
- Expensive

LATERAL | SECURITY

Privacy Audit Lifecycle



LATERAL | SECURITY

Privacy Leadership

- Someone to own privacy for the organisation
- Governance groups, teams, steering committees – pick your poison
- Ensure the right representatives are on it
- Link to KPIs, create accountability
- Privacy needs steering

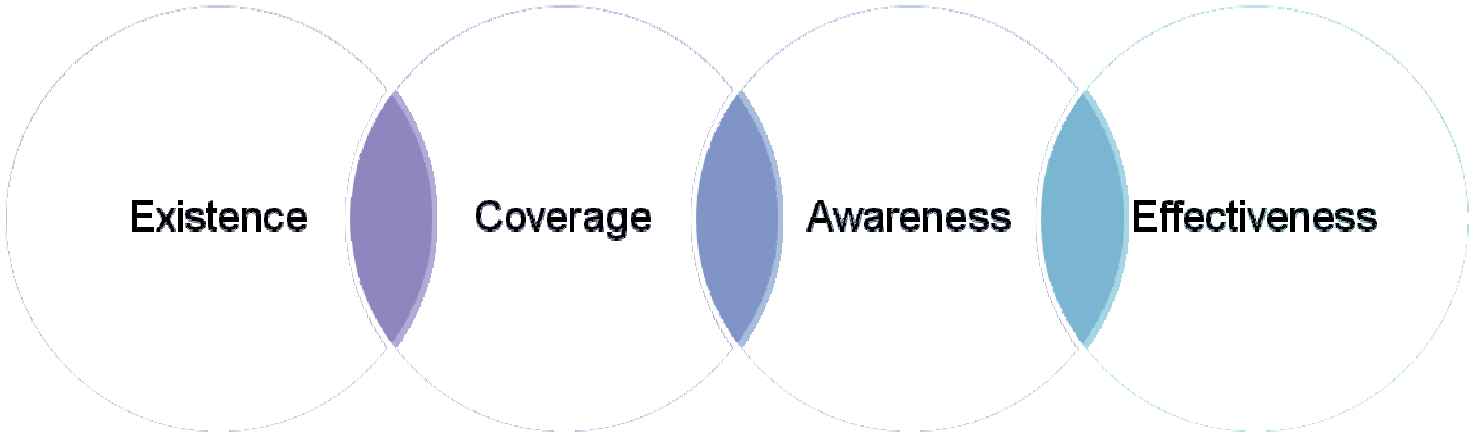
LATERAL | SECURITY

Incident Response

- What will your organisation do in case of data loss?
- How much data needs to be lost for it to become critical?
- What is your policy for informing data owners?
- What are your legal and regulatory obligations in case of breach?
- Where in the world are you operating and will that change things?

LATERAL | SECURITY

Privacy Policy



LATERAL | SECURITY

Data Identification

- Know what you are collecting?
- How classified or sensitive is it?
- Where is your information coming from?
- Why are you collecting it*?
- In what formats, in what quantities?

(*think about active and passive collection)

LATERAL | SECURITY

Data Flows and Stores

- Some data only every transits an organisation
- Some will enter and stay (whether we are conscious of it or not)*

*sometimes what we believe is happening is very different from what is actually happening

LATERAL | SECURITY

Facing Facts

Belief

Reality

LATERAL | SECURITY

Scope Reduction

Identify	• Know what you are storing and where
Prioritise	• Separate out the essentials
Simplify	• Change your systems and processes to only store/collect/process essential data
Secure	• Use industry best practice to secure essential data in transit, at rest and at disposal
Remove	• Safely remove all unnecessary data in accordance with industry best practice

LATERAL | SECURITY

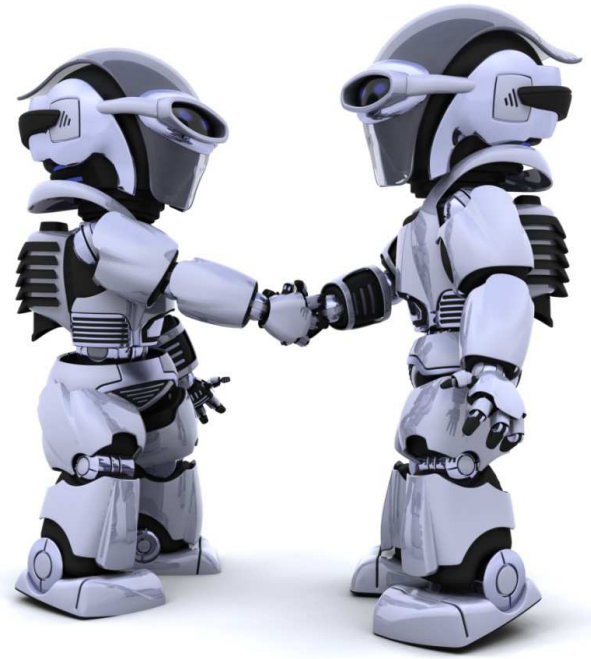
Data Protection and Access

- How easy is it to access personal information?
- What controls are in place?
- Are they being enforced?
- Where are the audit trails and logs?
- How is data protected at rest (cryptography, access rights, account controls)?
- How is data protected in transit?

LATERAL | SECURITY

Data Sharing

- Does the personal information get shared with 3rd parties?
- How much, for what reason and has the owner consented (what do the contracts say)?
- What is the third parties policy on privacy/audit?
- What would happen if your third party got breached?



LATERAL | SECURITY

Training and Awareness

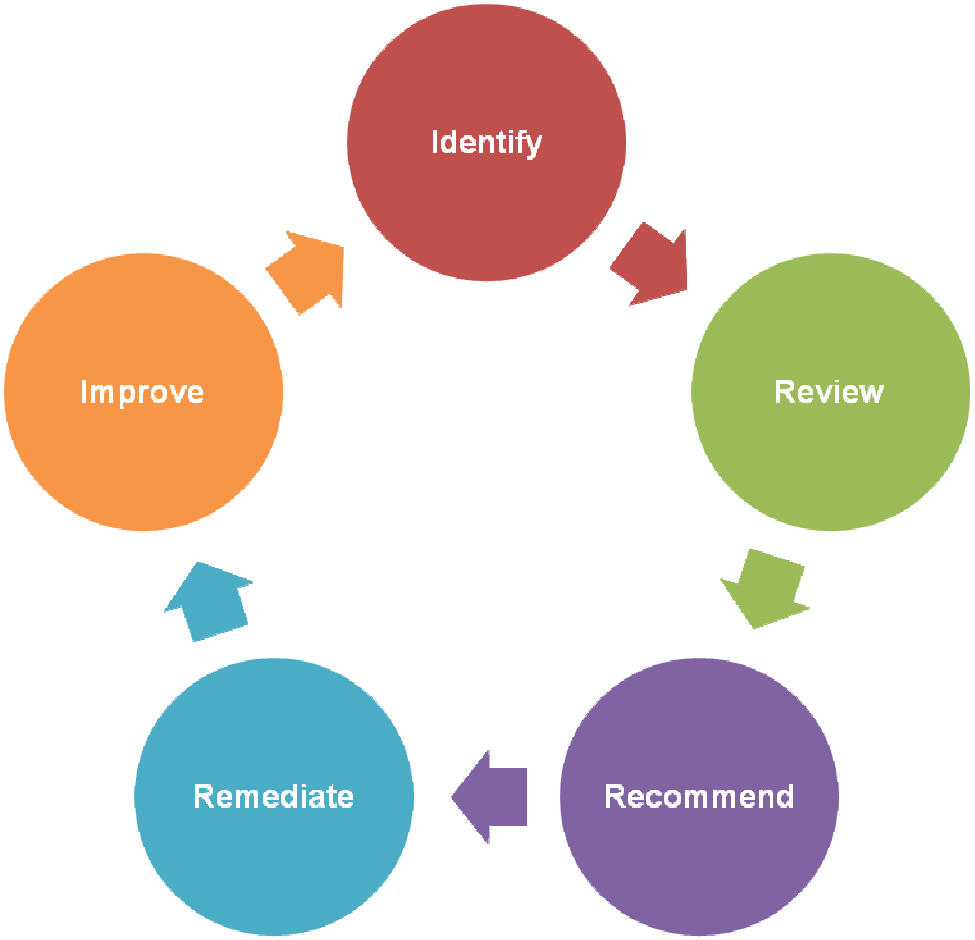
- What training are staff given about handling personal information?
- How often are they trained?
- How can they seek help or ask questions?
- How can they report issues?
- Is the message consistent with the policy?
- Can you measure its effectiveness?

LATERAL | SECURITY

Continuous Improvement

LATERAL | SECURITY

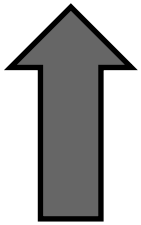
Periodic Assessment



LATERAL | SECURITY

Finding an Auditor

"a new breed of investigator, auditor, records manager and electronic data protection specialist"



crikey that's quite the hybrid

so don't be afraid to shop around

LATERAL | SECURITY

Further Reading

- http://www.isaca.org/Knowledge-Center/Standards/Documents/Gx31PrivacyGuideline.pdf
- IIA :GTAG 5 – Managing and Auditing Privacy Risks
- http://www.legislation.govt.nz

LATERAL | SECURITY

Any Questions

Laura Bell
laura.bell@lateralsecurity.com
+ 64 9 377 0700
+64 210 786827

LATERAL | SECURITY