

“Making Your Information Security Policy Useful” – Stephen Coates – AppSec NZ 2021



1



2

Fri 12/02/21
3:25pm

1

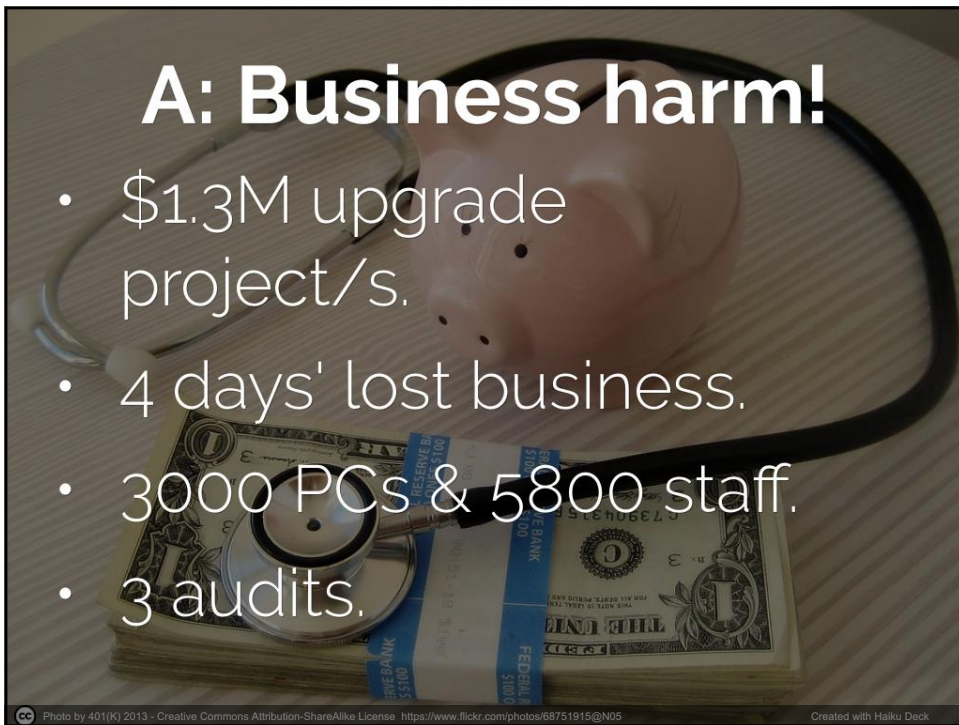
Q: What's the potential value of your information security policy?



3

A: Business harm!

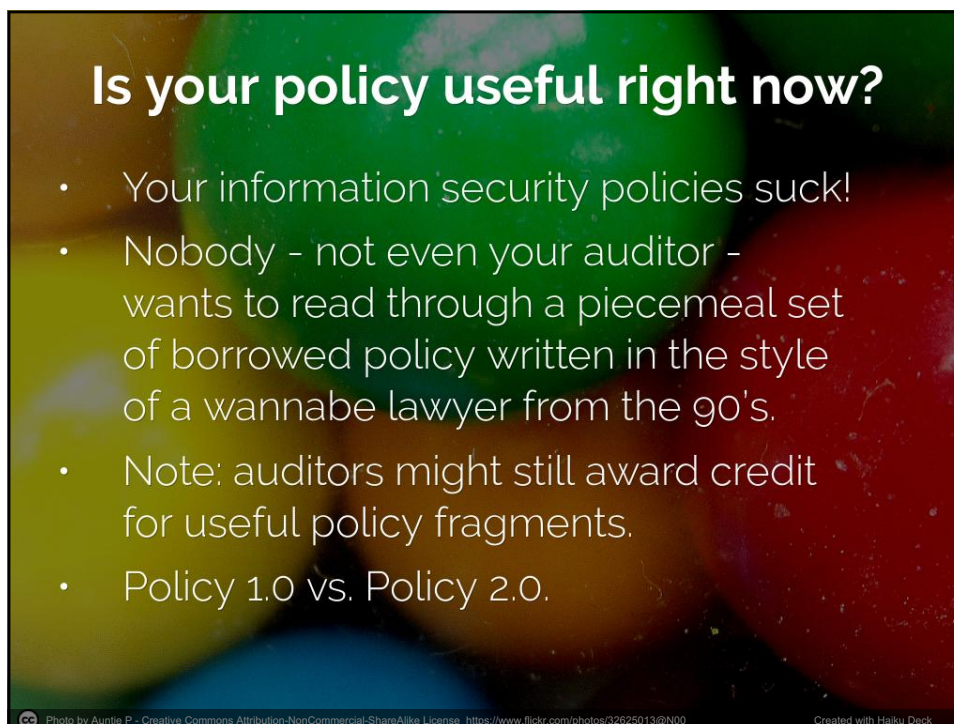
- \$1.3M upgrade project/s.
- 4 days' lost business.
- 3000 PCs & 5800 staff.
- 3 audits.



4



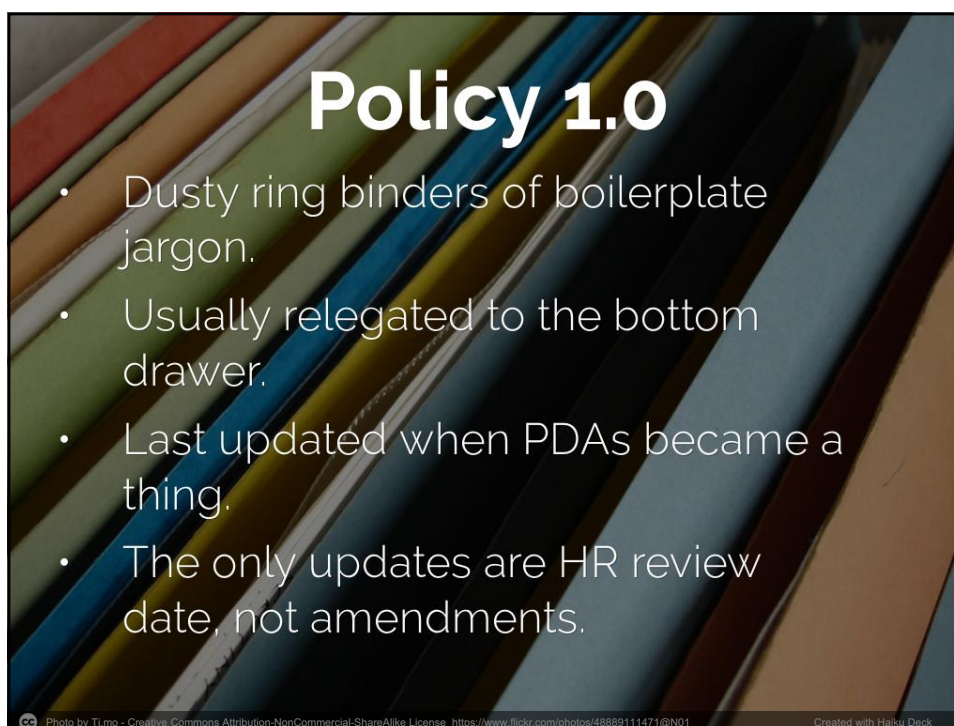
5



6



7



8

Excusing Policy 1.0

1. Adapted policies the boss downloaded.
2. Used up spare consultancy hours.
3. Window-dressed the business for sale.
4. Big customer wanted to see it.
5. Adverse audit findings demanded it.
6. "Boogeyman" for scaring new starters.
7. Group HQ wrote and translated it.
8. We just kept adding to the original set.

Photo by Jon Cellier - Creative Commons No known copyright restrictions https://unsplash.com/@frenchleey7?utm_source=haikudeck&utm_medium=referral&utm_campaign=haikudeck

9

Policy 1.0 remorse

- "We needed your security expertise to enable the business, but policy bureaucracy is holding us back."
- "Your documents are smothering our enthusiasm and our innovation."
- "Your policies have little we need ... and nothing we want."

Photo by manoftaste.de - Creative Commons Attribution License <https://www.flickr.com/photos/96913861@N04> Created with Haiku Deck

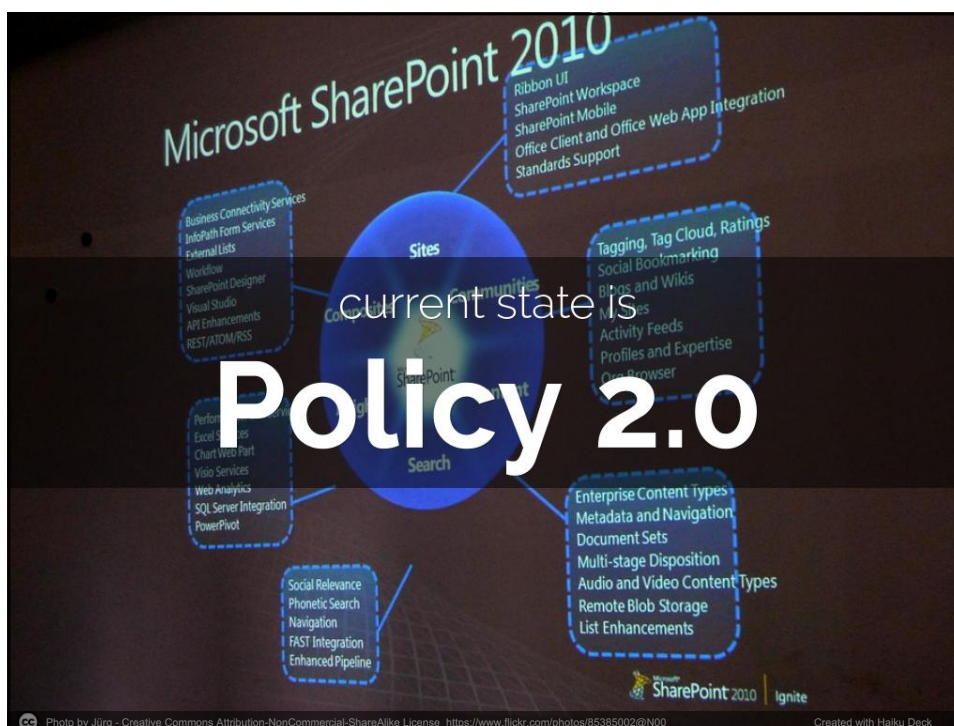
10

Making Policy 1.0 useful

- Use it as a fire starter.
- If it's large, as a paper weight.
- Make origami.
- Papier mâché bowls or animals.
- Paper hats for the whole office.
- Packing material.
- [Hat tip to Aura's Nick Malcolm.]

Photo by Meritt Thomas - Creative Commons No known copyright restrictions. https://unsplash.com/@merittthomas?utm_source=haikudeck&utm_medium=referral&utm_campaign=haikudeck

11



12

Policy 2.0

- Now a cluster of standalone Word documents, probably in a folder on the corporate intranet.
- SharePoint 2010 or 365?

Photo by Jürg - Creative Commons Attribution-NonCommercial-ShareAlike License <https://www.flickr.com/photos/85385002@N00> Created with Haiku Deck

13

Laudable Policy 2.0 aims

- Behaviour, behaviour, behaviour, ...
- Keeping management promises.
- User behaviour.
- Protecting our technical staff.
- Reinforcing a "culture of security".

Photo by stockcatalog - Creative Commons Attribution License <https://www.flickr.com/photos/151691693@N02> Created with Haiku Deck

14

Positive Policy 2.0 outcomes

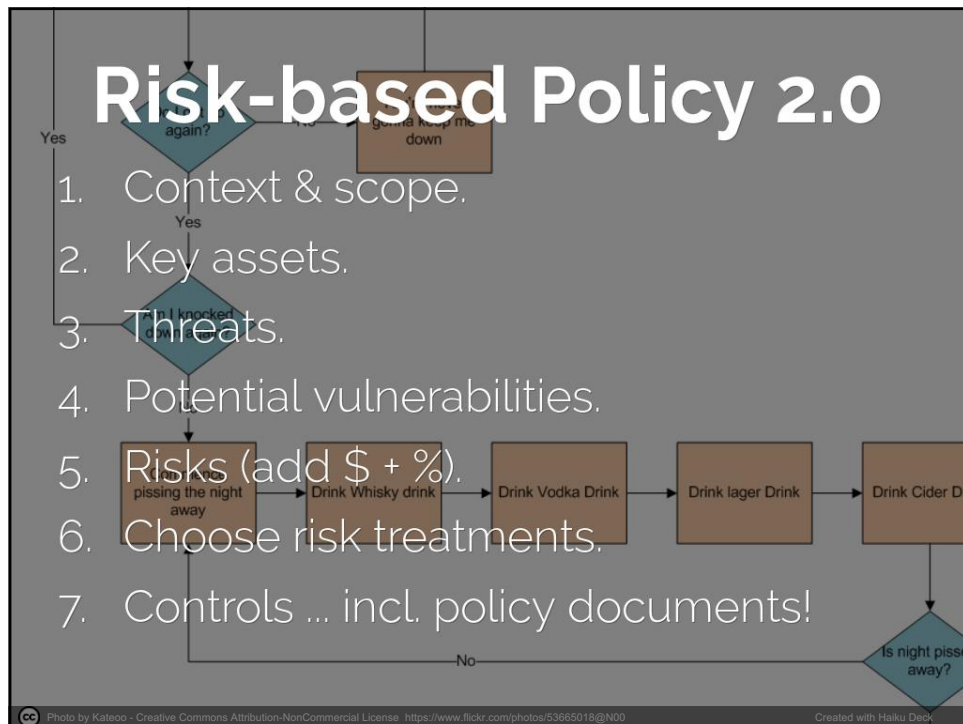
- Fit (right-sized & risk-based).
- Readable (find, search, read, good style/tone, musts & penalties).
- Authoritative (current & signed-off).
- Correct & actionable.
- Contact info (for clarification & advice).
- Measurable (success criteria).

15

Policy 2.0 is shaped by ...

- Drivers (business model, mission, vision, strategies).
- Risks (business & information security).
- Imperatives (overriding legislation, regulation, contracts, certification).

16



17



18

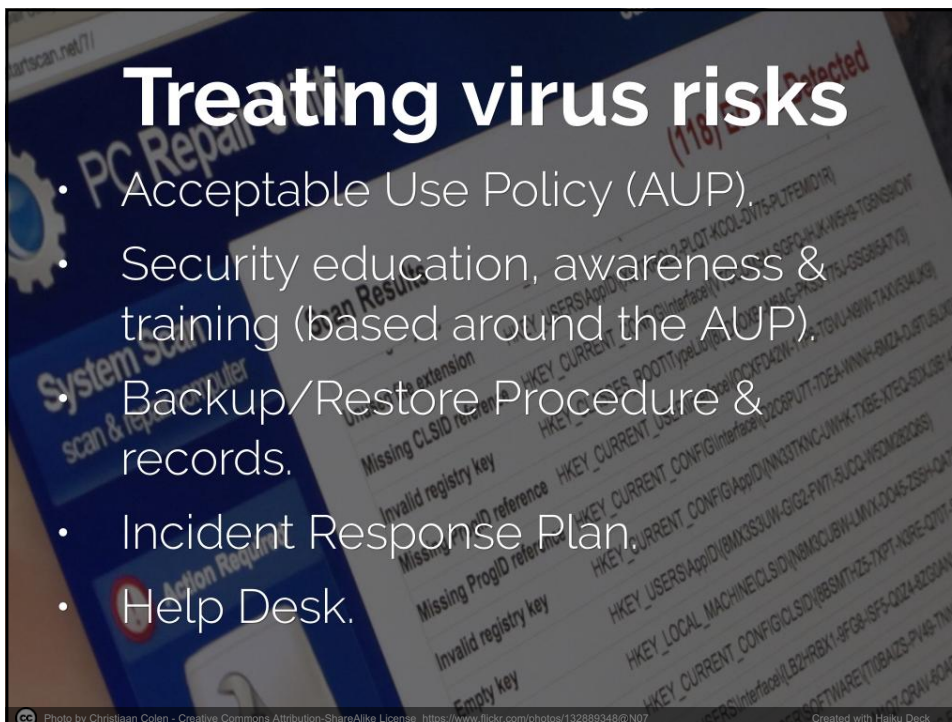


Treating virus risks?

1. Anti-malware for endpoints + portable media.
2. Anti-malware at web & email gateways.

Photo by Christiaan Colen - Creative Commons Attribution-ShareAlike License. <https://www.flickr.com/photos/132889348@N07>
Created with Haiku Deck

19



Treating virus risks

- Acceptable Use Policy (AUP).
- Security education, awareness & training (based around the AUP).
- Backup/Restore Procedure & records.
- Incident Response Plan.
- Help Desk.

Photo by Christiaan Colen - Creative Commons Attribution-ShareAlike License. <https://www.flickr.com/photos/132889348@N07>
Created with Haiku Deck

20



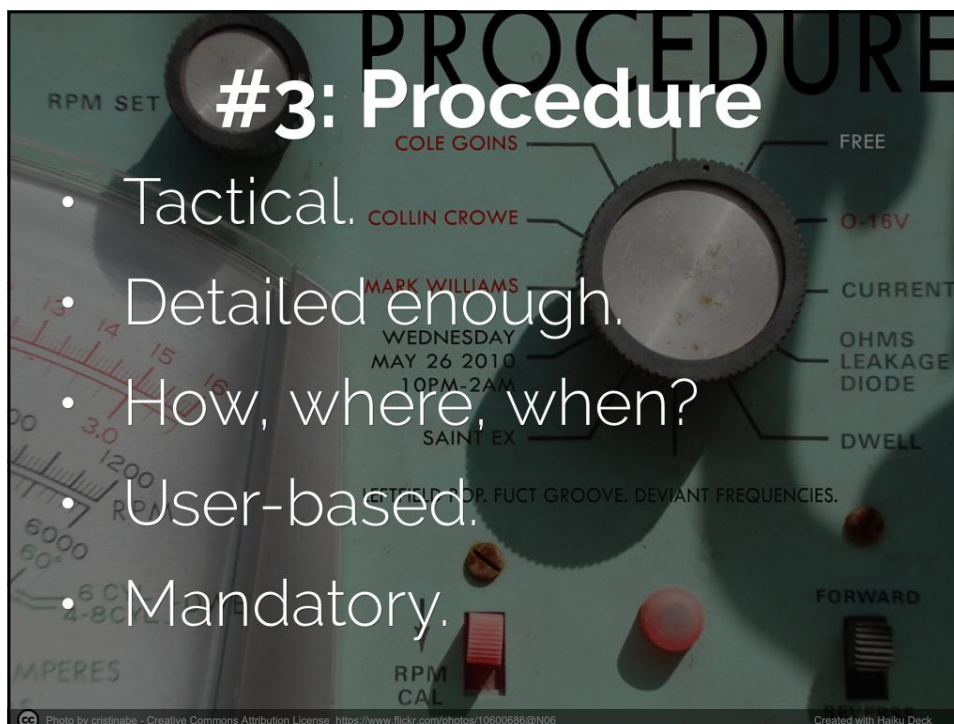
21



22



23



24

#4: Guideline

- User-based.
- Advice & guidance.
- To help comply with mandatory rules.

CC Photo by toby - Creative Commons Attribution-NonCommercial License <https://www.flickr.com/photos/8178188@N04>

Created with Haiku Deck

25

Document focus

1. Generic/organisational.
2. Issue-specific (marketing & new websites).
3. System-specific (SAP CRM system).

CC Photo by WanderingtheWorld (www.ChrisFord.com) - Creative Commons Attribution-NonCommercial License <https://www.flickr.com/photos/44028103@N07>

Created with Haiku Deck

26

Workload & responsibility

- How much of this policy stuff is new, and how much is an extension of "existing" (?) IT, HR, Privacy, Procurement work?
- Why should corporate risk management be an information security thing?
- As per NZ PSR, share with IT, HR, H&S, Physical Security, Risk.
- Consider 3rd parties (MSP, CSP, outsourced development).

27

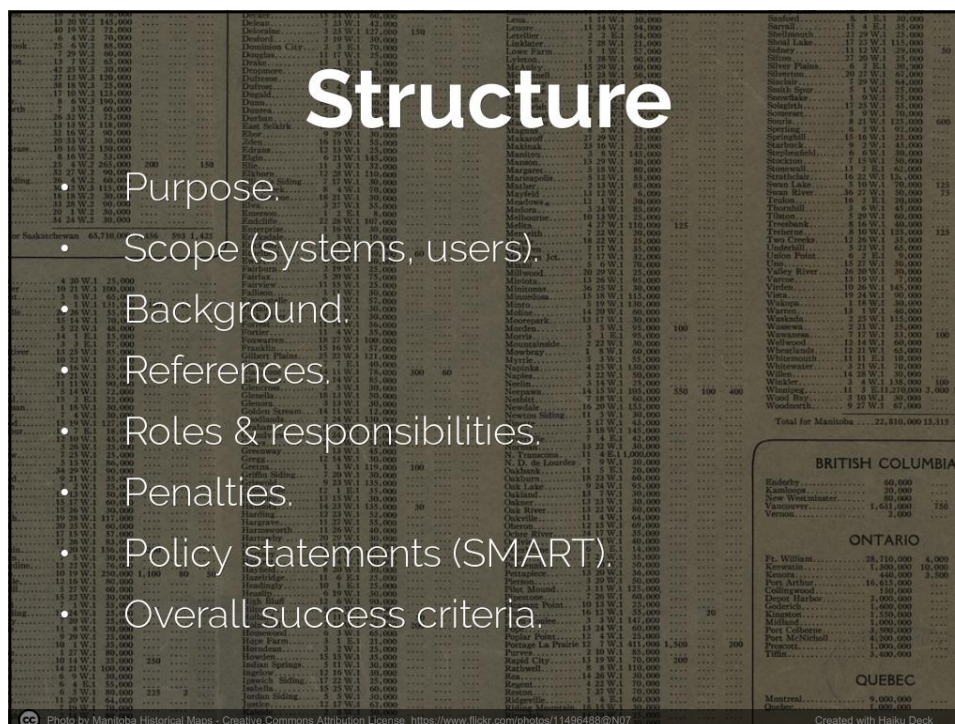
Policy 2.0 construction

- Boilerplate.
- Structure.
- Wording options (x3).
- Consistency implies style guide or "Policy Standard".

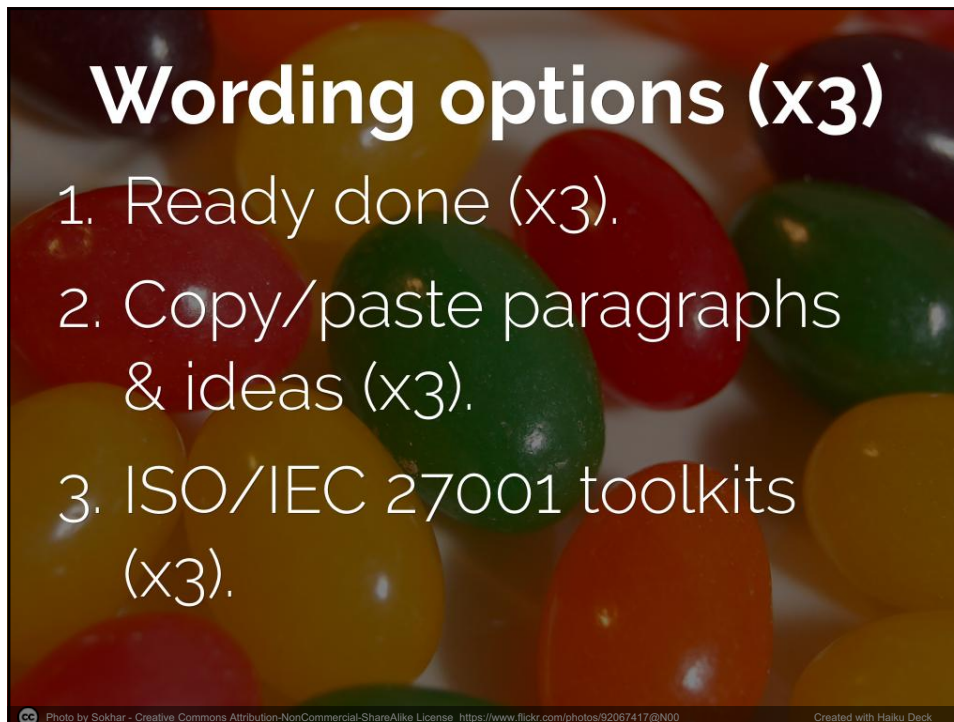
28



29



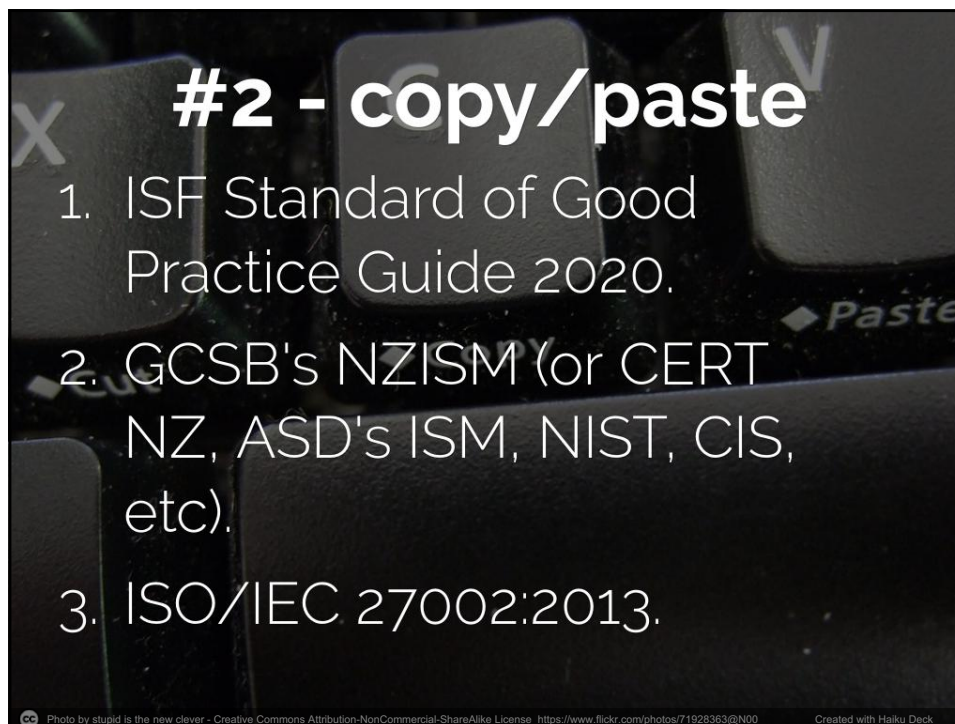
30



31



32



33



34



35

So, what changed?

1. Desktop & phone => Google & Microsoft.
2. DIY code & servers => AWS & Azure.
3. Big-box apps => SaaS.
4. Remote access & VPN => cloud & MFA.
5. BYO/WFH (phone, laptop, Wi-Fi, desk).
6. ... more demand-side People & Process, less supply-side Technology operations.
7. NZ redefined "small" & "remote" ...

Photo by Chris Lawton - Creative Commons No known copyright restrictions. https://unsplash.com/@chrislawton?utm_source=haikudeck&utm_medium=referral&utm_campaign=haiku-deck

36

NZ business sizes

- L (50+ FTE): 1% or ~5,000.
- M (20-49 FTE): 2% or ~10,000.
- S (6-19 FTE): 7.5% or ~40,000.
- ... size of their IT & security teams?
- ... audience for writing, updating & consuming Policy 2.0?

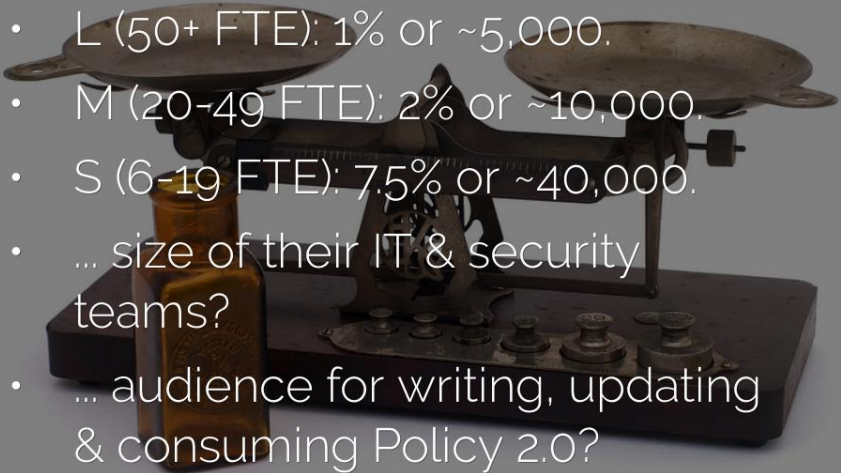


Photo by Carol Kodak - Creative Commons Attribution-NonCommercial License <https://www.flickr.com/photos/35114754@N00> Created with Haiku Deck

37

Policy 3.0

- Make our policies risk-based, referenced, well-structured, visually attractive, and in plain language?
- Switch Guidelines and “Acceptable Use Policies” to pull, rather than push or broadcast.

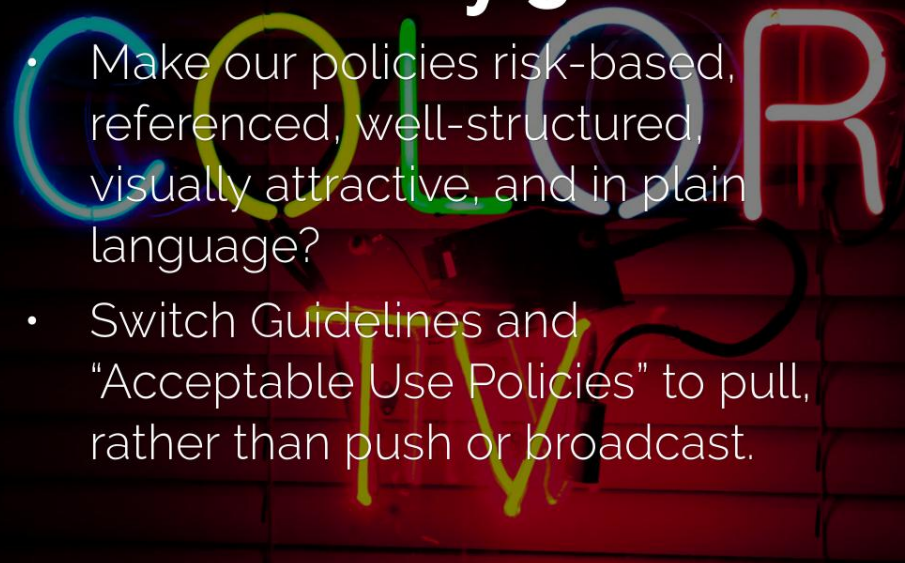
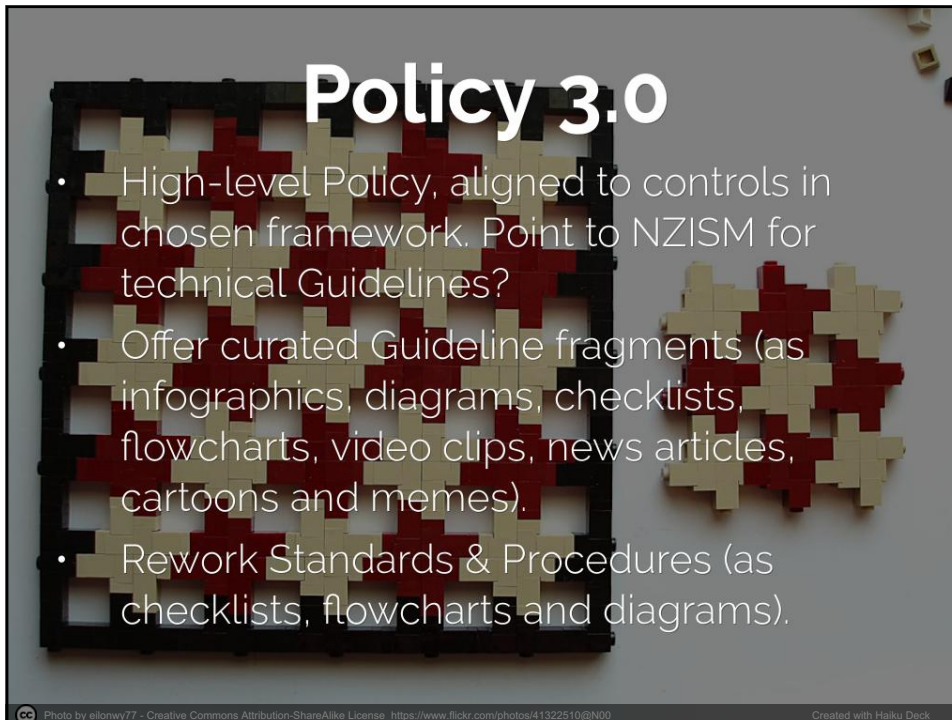


Photo by Thomas Hawk - Creative Commons Attribution-NonCommercial License <https://www.flickr.com/photos/5103555243@N01> Created with Haiku Deck

38

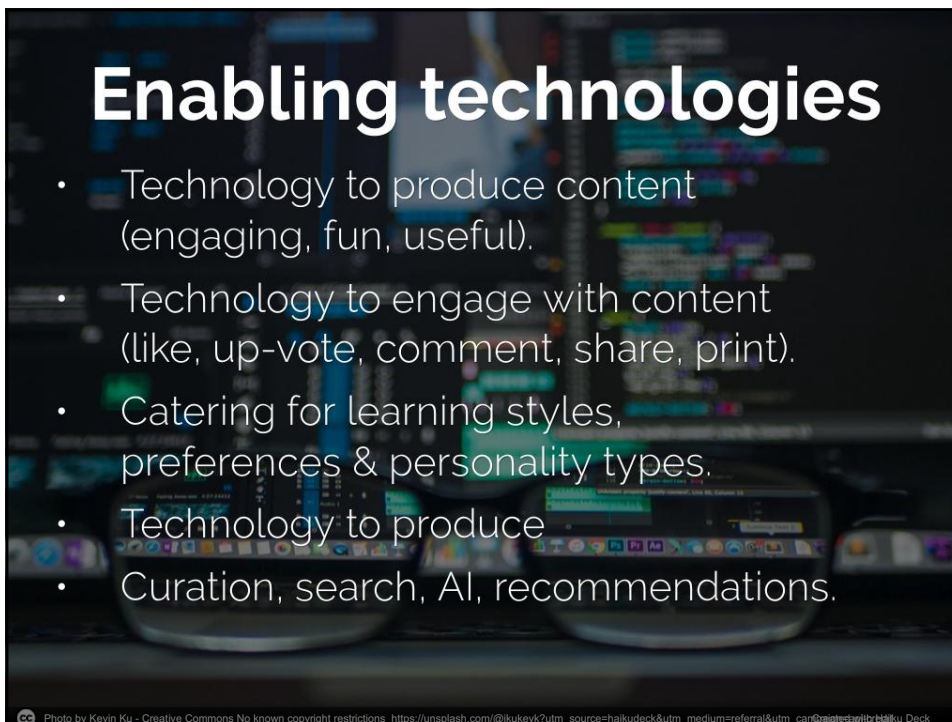


Policy 3.0

- High-level Policy, aligned to controls in chosen framework. Point to NZISM for technical Guidelines?
- Offer curated Guideline fragments (as infographics, diagrams, checklists, flowcharts, video clips, news articles, cartoons and memes).
- Rework Standards & Procedures (as checklists, flowcharts and diagrams).

CC Photo by eilonwy77 - Creative Commons Attribution-ShareAlike License <https://www.flickr.com/photos/41322510@N00> Created with Haiku Deck

39

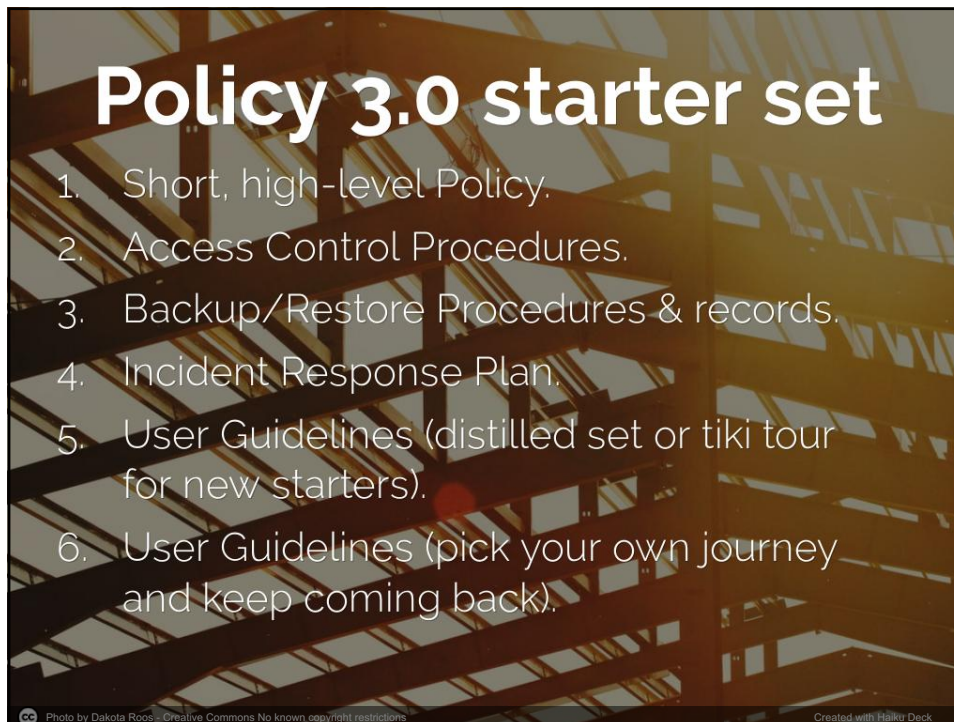


Enabling technologies

- Technology to produce content (engaging, fun, useful).
- Technology to engage with content (like, up-vote, comment, share, print).
- Catering for learning styles, preferences & personality types.
- Technology to produce
- Curation, search, AI, recommendations.

CC Photo by Kevin Ku - Creative Commons No known copyright restrictions https://unsplash.com/@kukevk?utm_source=haikudeck&utm_medium=referral&utm_campaign=tagged+with+haiku+deck

40

A presentation slide with a background image of a modern building's steel framework. The title "Policy 3.0 starter set" is in large white font. Below it is a numbered list of six items. At the bottom, there are two small Creative Commons license icons and text.

Policy 3.0 starter set

1. Short, high-level Policy.
2. Access Control Procedures.
3. Backup/Restore Procedures & records.
4. Incident Response Plan.
5. User Guidelines (distilled set or tiki tour for new starters).
6. User Guidelines (pick your own journey and keep coming back).

CC Photo by Dakota Ross - Creative Commons No known copyright restrictions Created with Haiku Deck

41

A presentation slide with a background image of a large black question mark hanging from a string above four black spheres on a surface. The title "Your questions & comments?" is in white font. At the bottom, the email address "s.coates@aurainfosec.com" is displayed in white. At the very bottom, there are two small Creative Commons license icons and text.

Your questions & comments?

s.coates@aurainfosec.com

CC Photo by Stefan Baudy - Creative Commons Attribution License https://www.flickr.com/photos/92454606@N00 Created with Haiku Deck

42