

“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!

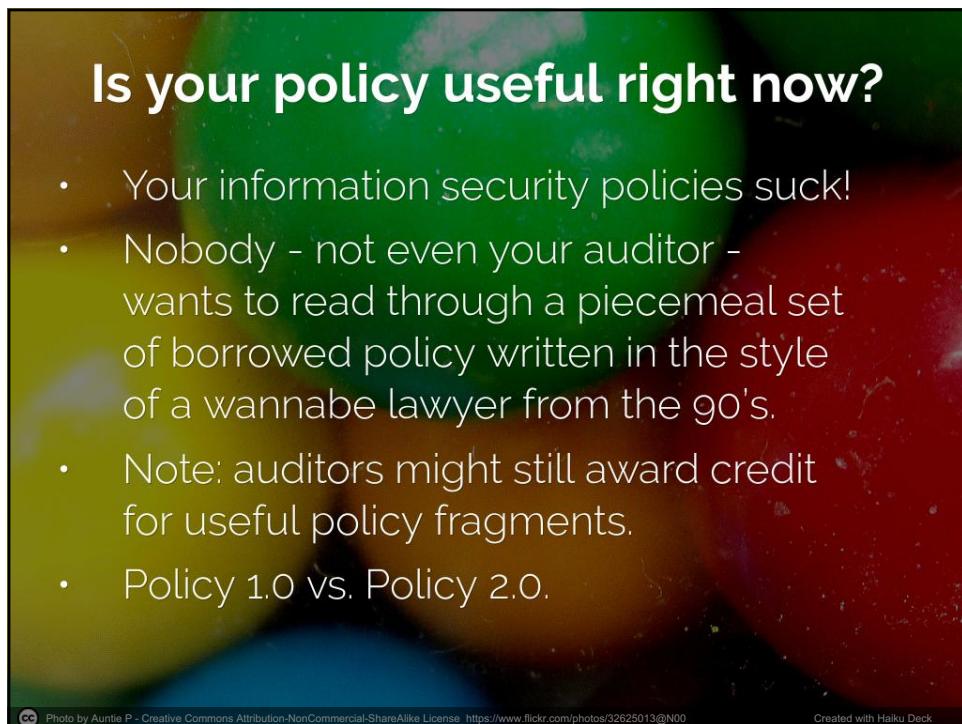
- \$1.3M upgrade project/s.
- 4 days' lost business.
- 3000 PCs & 5800 staff.
- 3 audits.



4



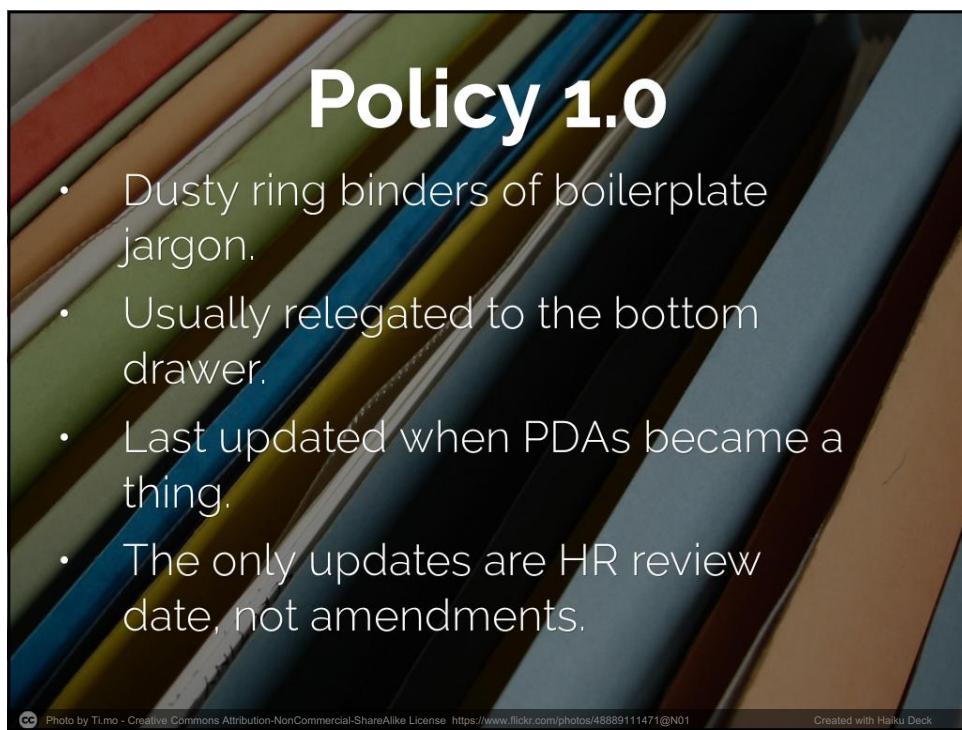
5



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/@frenchieeye?utm_source=haikudeck&utm_medium=referral&utm_campaign=HaikuDeck

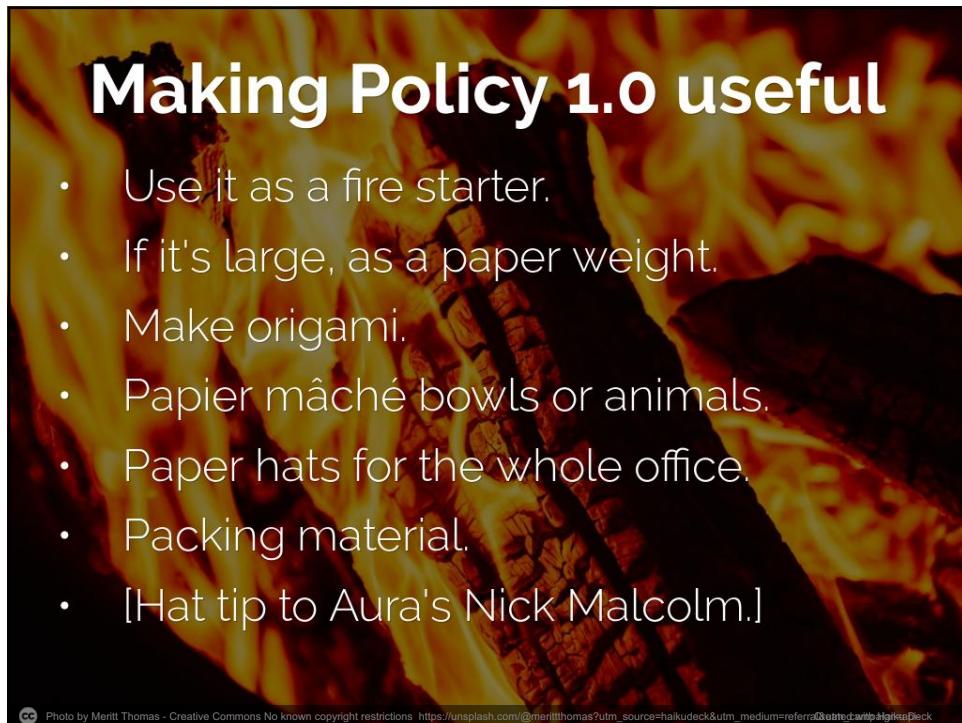
9

Policy 1.0 remorse

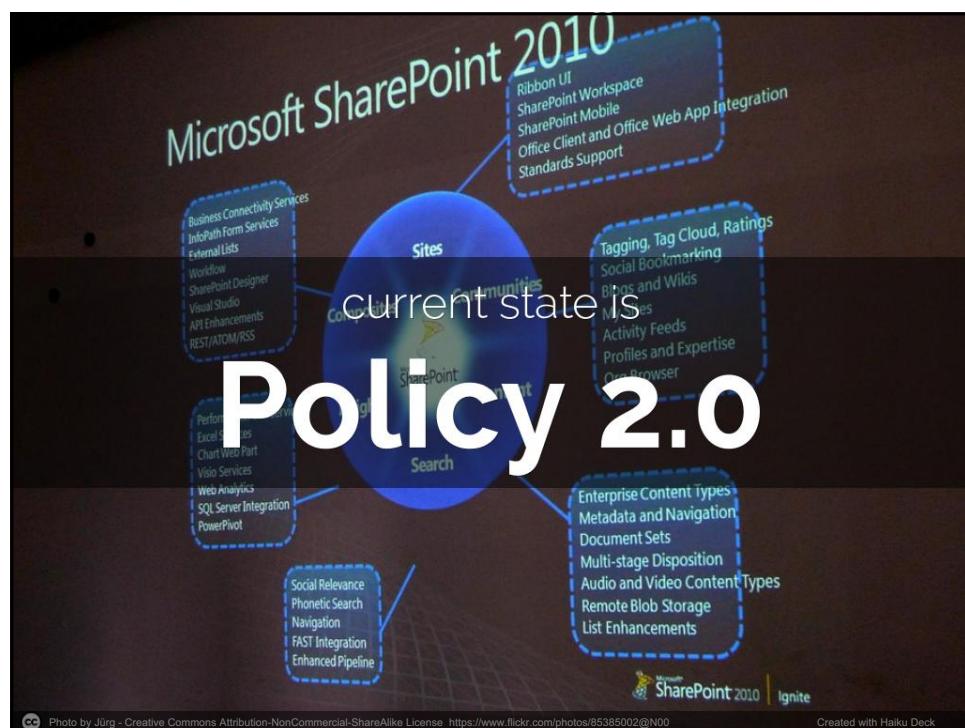
- "We needed your security expertise to enable the business, but policy bureaucracy is holding us back."
- "Your documents are smothering our enthusiasm and our innovation."
- "Your policies have little we need ... and nothing we want."

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

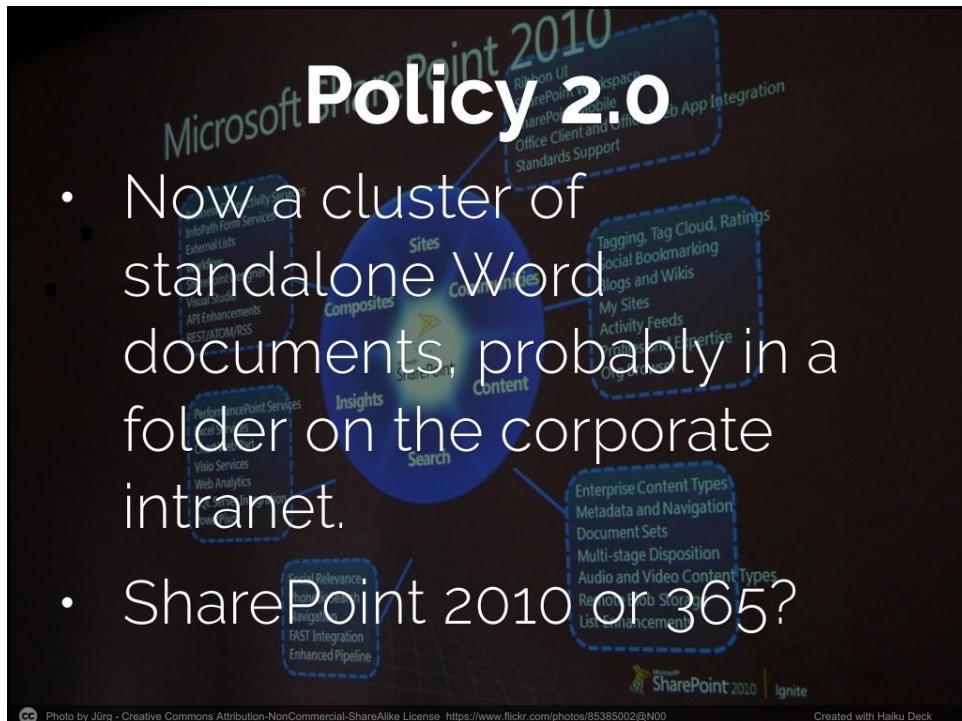
10



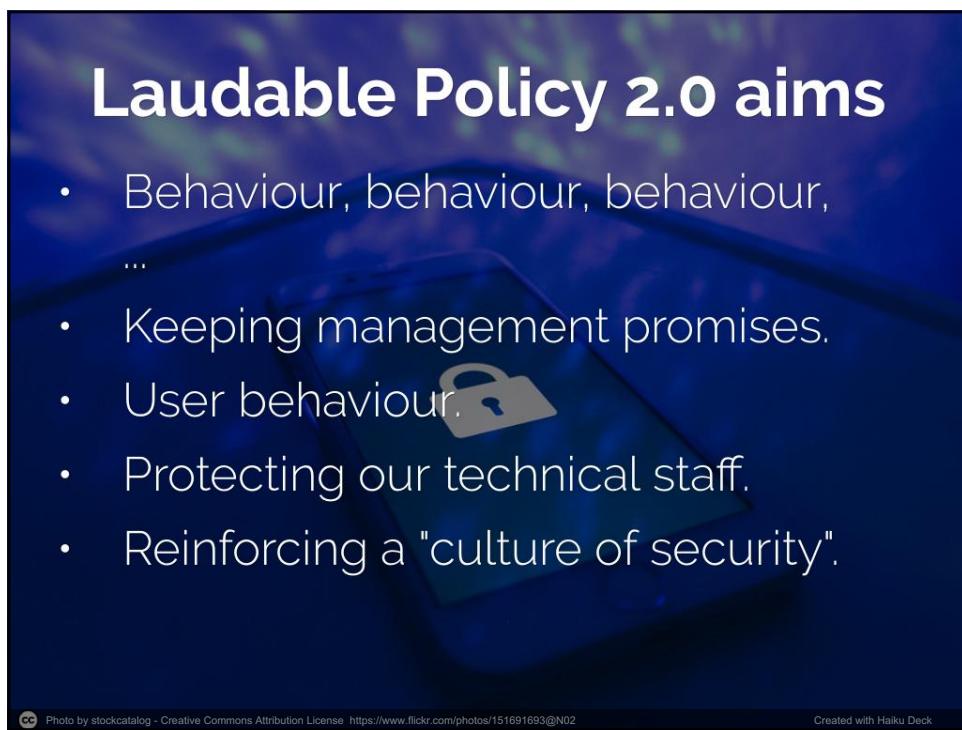
11



12



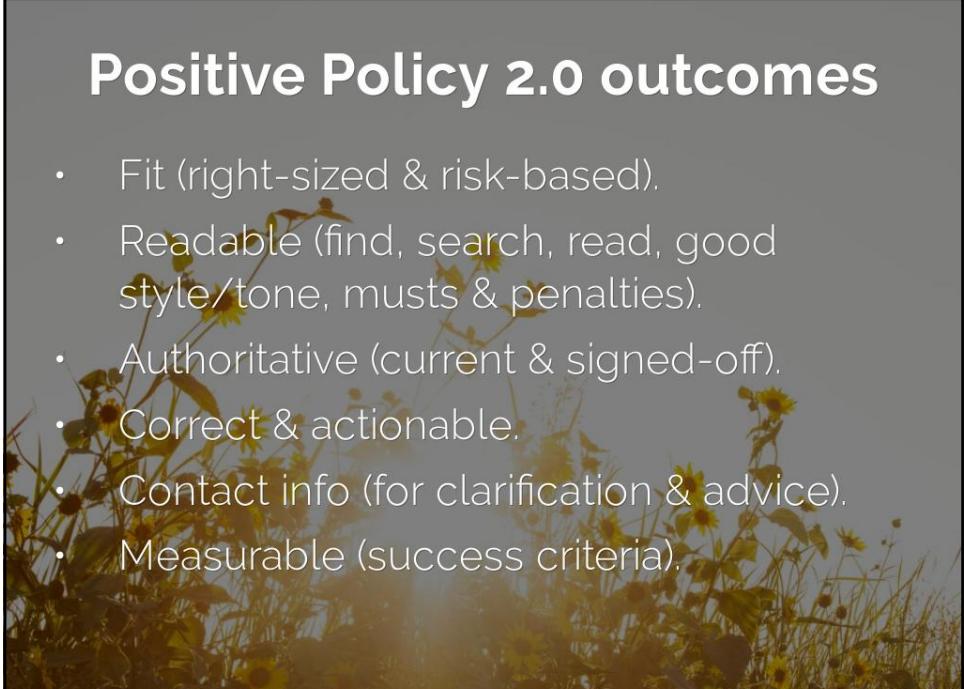
13



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).

 CC Photo by Matti Johnson - Creative Commons No known copyright restrictions https://unsplash.com/@matti_johnson?utm_source=haikudeck&utm_medium=referred_by_haiku_deck

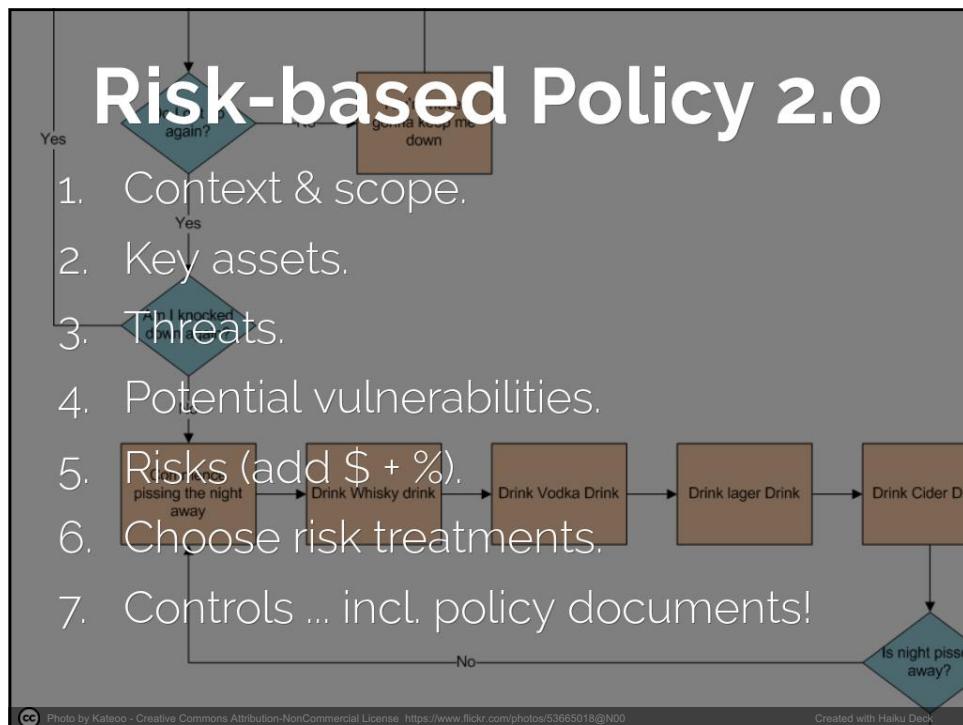
15

Policy 2.0 is shaped by ...

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

 CC Photo by qmponic - Creative Commons Attribution License <https://www.flickr.com/photos/58578431@N00> Created with Haiku Deck

16



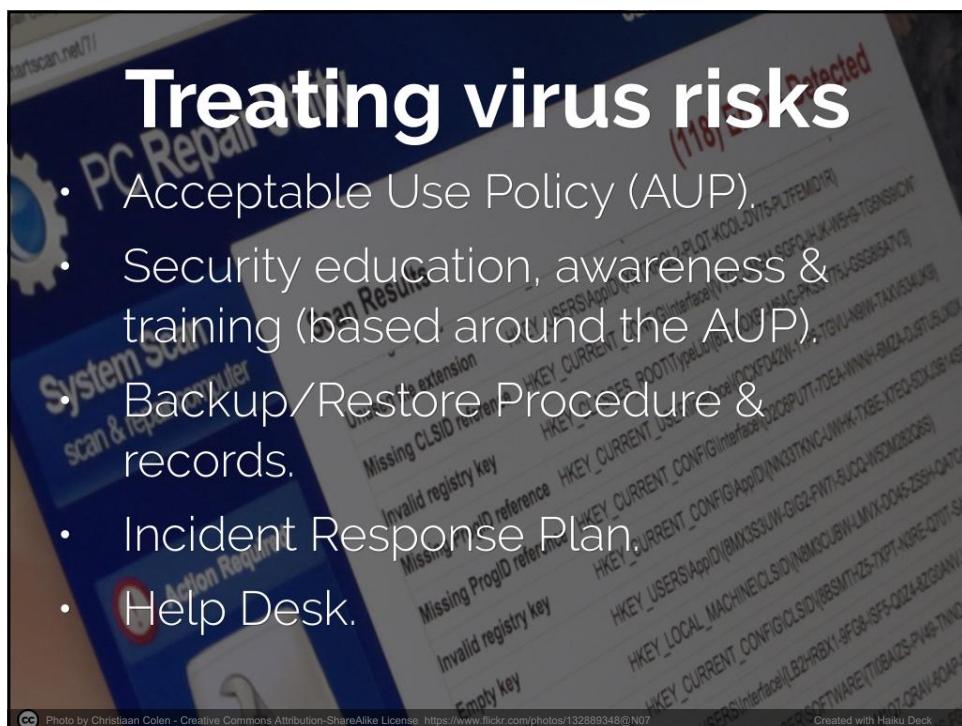
17



18



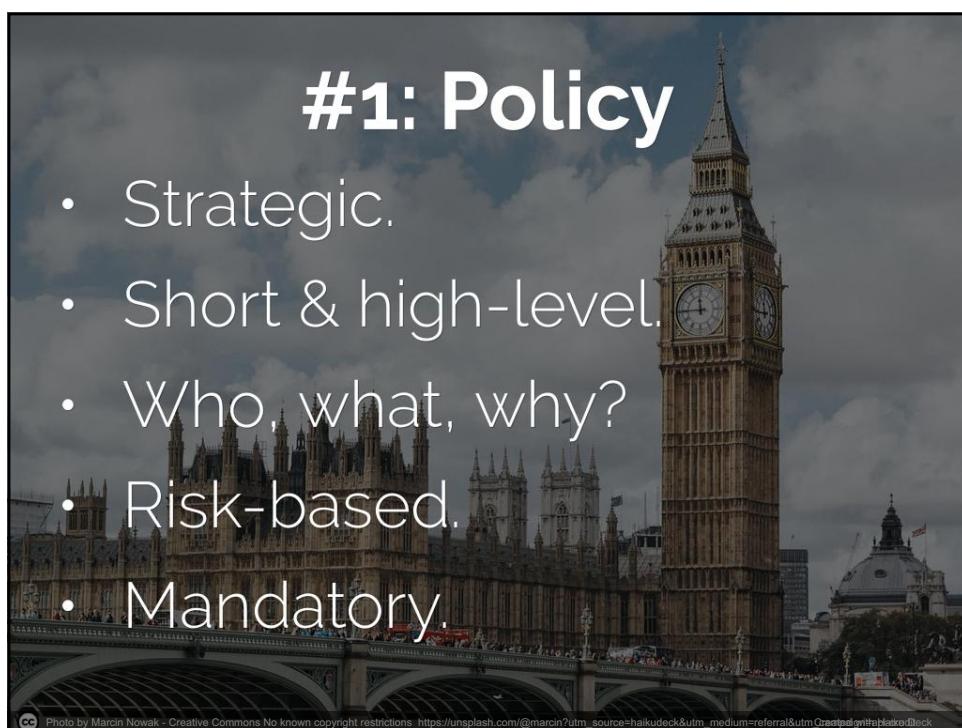
19



20



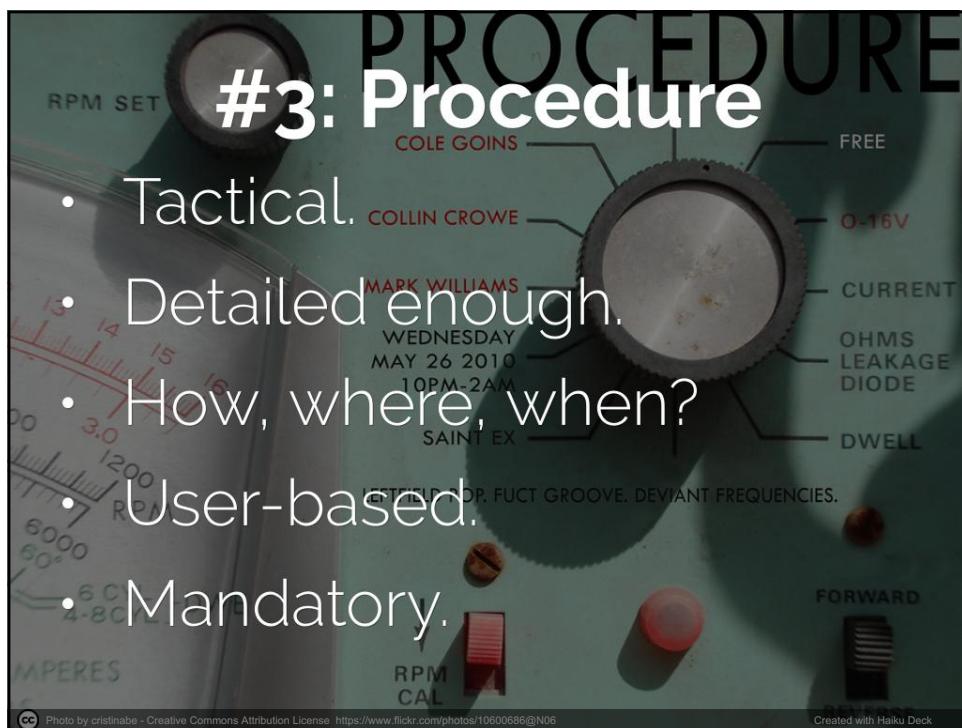
21



22



23



24

#4: Guideline

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

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

25

Document focus

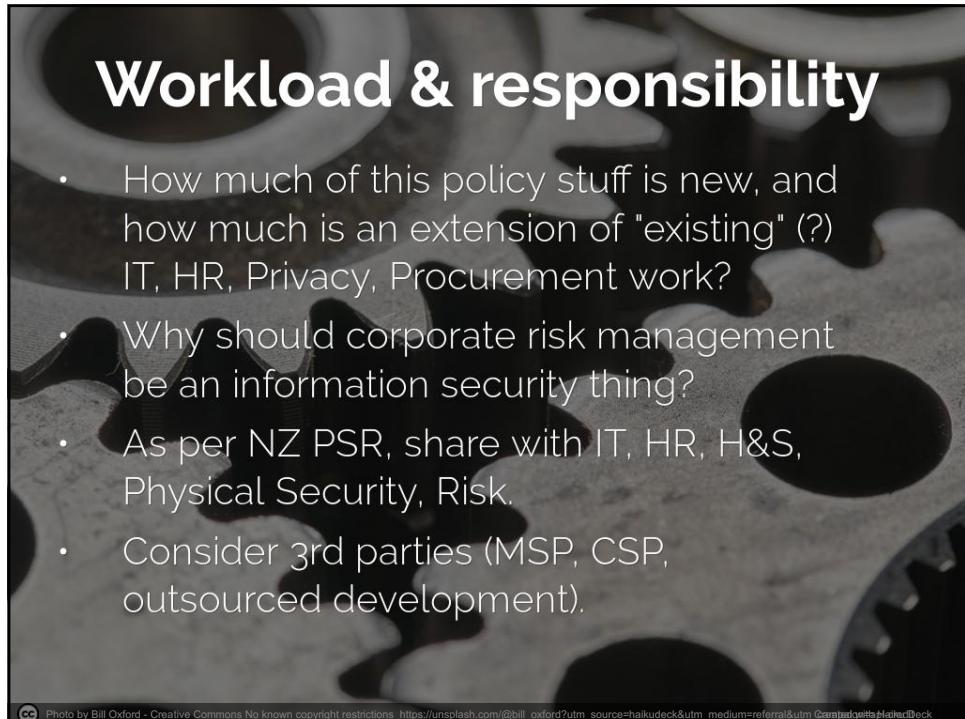
1. Generic/organisational.
2. Issue-specific (marketing & new websites).
3. System-specific (SAP CRM system).

 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

	<i>Boilermakers</i>	
1. 30,000	Adams	16 15 W-1
2. 150,000	Edmunds	12 15 W-1
3. 53,000	Elgin	6 21 W-1 145,000
4. 25,000	Erie	11 3 W-1
5. 90,000	Fairmont	12 20 W-1 110,000
6. 60,000	Elliott's Salina	7 1 W-1
7. 115,000	Gardiner	8 4 10 W-1

Structure

• Wording options (x3)

- Consistency implies style guide or "Policy Standard"

Policy 2.0 construction

• Boilerplate.

• Structure.

• Wording options (x3).

• Consistency implies style guide or "Policy Standard".

Boilerplate

- Name.
 - Reference number.
 - Classification.
 - Dates (approval, next review).
 - Authoriser/s.
 - Version.

 Photo by Omid Kashmari - Creative Commons No known copyright restrictions https://unsplash.com/@omidkashmari?utm_source=halkudek&utm_medium=referral&utm_campaign=yoitnhdq1gn

29

3	23 W.	127,000	150	Lesterill,	2	E. E.	54,000
10	W.	30,000	25	Lintonl.	7	28 W.	21,000
11	W.	25,000	25	Lowe Farm,	5	I.W.L.	57,000
11	1 E.	4,000	—	Lyleton,	1	28 W.	9,000
11	1 E.	5,000	—	McAuley,	15	29 W.	60,000
11	1 E.	6,000	—	McAllister,	15	28 W.	36,000
4	2	30,000	—	McGillivray,	15	28 W.	36,000

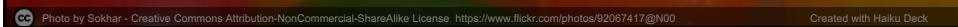
• Policy statements (SMART)

12 22 W.1	76,000						
10 19 W.1	250,000	1,100	80	50			Hayside..
.12 16 W.1	80,000						Hazelridge.
.5 27 W.1	60,000						Headingly..
.15 27 W.1	30,000						Heslip..

30

Wording options (x3)

1. Ready done (x3).
2. Copy/paste paragraphs & ideas (x3).
3. ISO/IEC 27001 toolkits (x3).

 CC Photo by Sokhar - Creative Commons Attribution-NonCommercial-ShareAlike License https://www.flickr.com/photos/92067417@N00

Created with Haiku Deck

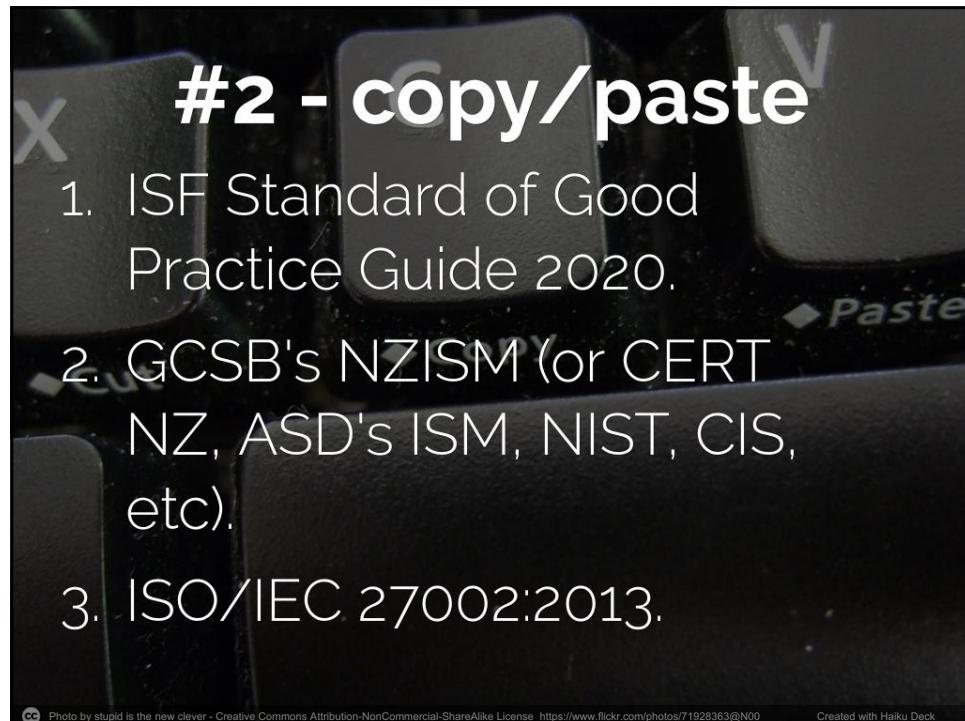
31

#1 - ready done

1. InstantSecurityPolicy.com.
2. Information Security Policies Made Easy v14 (book/CD).
3. SANS Institute's Policy Project.

 CC Photo by Lance Grandahl - Creative Commons No known copyright restrictions https://unsplash.com/@lg17?utm_source=haikudeck&utm_medium=referral&utm_campaign=withHaikuDeck

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%20Deck

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 Capt 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/51035555243@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 ellonwy77 - Creative Commons Attribution-ShareAlike License https://www.flickr.com/photos/41322510@N00

Created with Haiku Deck

39

Enabling technologies

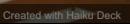
- Technology to produce content (engaging, fun, useful).
- Technology to engage with content (like, up-vote, comment, share, print).
- Catering for learning styles, preferences & personality types.
- Technology to produce
- Curation, search, AI, recommendations.

CC Photo by Kevin Ku - Creative Commons No known copyright restrictions https://unsplash.com/@ikukevk?utm_source=haikudeck&utm_medium=referral&utm_campaign=api%20deck

40

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).

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

41

Your questions & comments?



s.coates@aurainfosec.com

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

42