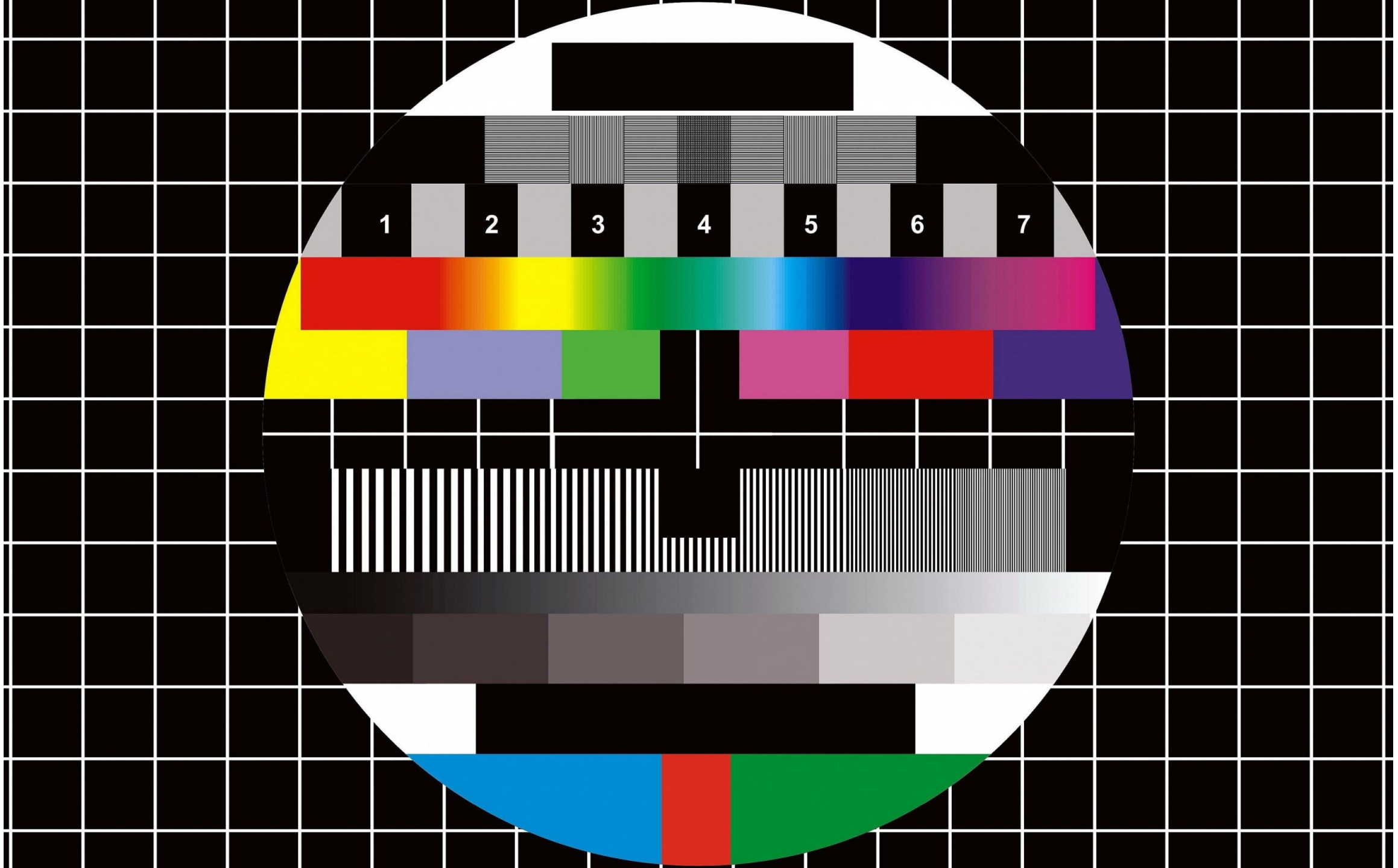
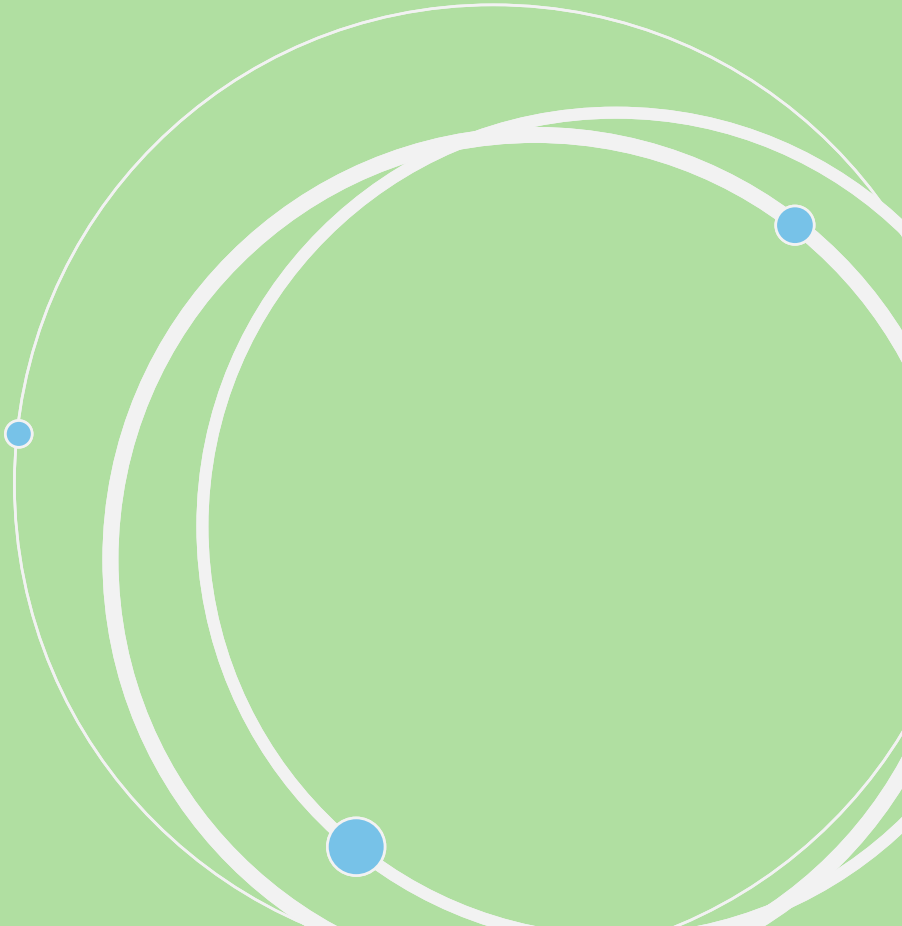

1
2
3
4
5
6
7

Making Security Decisions Like a Boss

Ron Parker
http://www.secretchipmunk.com
@scmunk



A typical day in security

We had lunch with a thought-leading vendor, and they said we could replace everything with an AI-centric quantum blockchain-verified precognitive edge service.

For ***less money*** than you are spending now!

SOAR
Ethereum…
S.A.S.E…
iSOC
ZT
Ransomware Prevention
UEBA…
XDR++
NFT…

Security Leadership

Those questions and decisions pile up*

- What technologies and implementations do we have for security?
- Don't we have something that will do that already?
- We are covering the important stuff, right?
- Is there anything we can DROP?
- Which way should we grow or improve?
- What happens when this services goes out of support?
- How do I plan the work for next year?
- I know we just moved to the cloud but I though we already implemented that security thing.
- How does this fit with the long-term road map?
- How does that new security product fit in?
- How does all this relate to our security controls?
- Is our organization organized correctly?
- Where are we spending our money?

* This is a good example of a bad slide

How do we make security decisions like a boss?

First, what makes a good decision?

Good decisions are:

Consistent – Your method can be depended upon

Traceable – You can show the factors the result is based upon

Valuable – Your answers are useful for your business and you

Transparent – The process is open

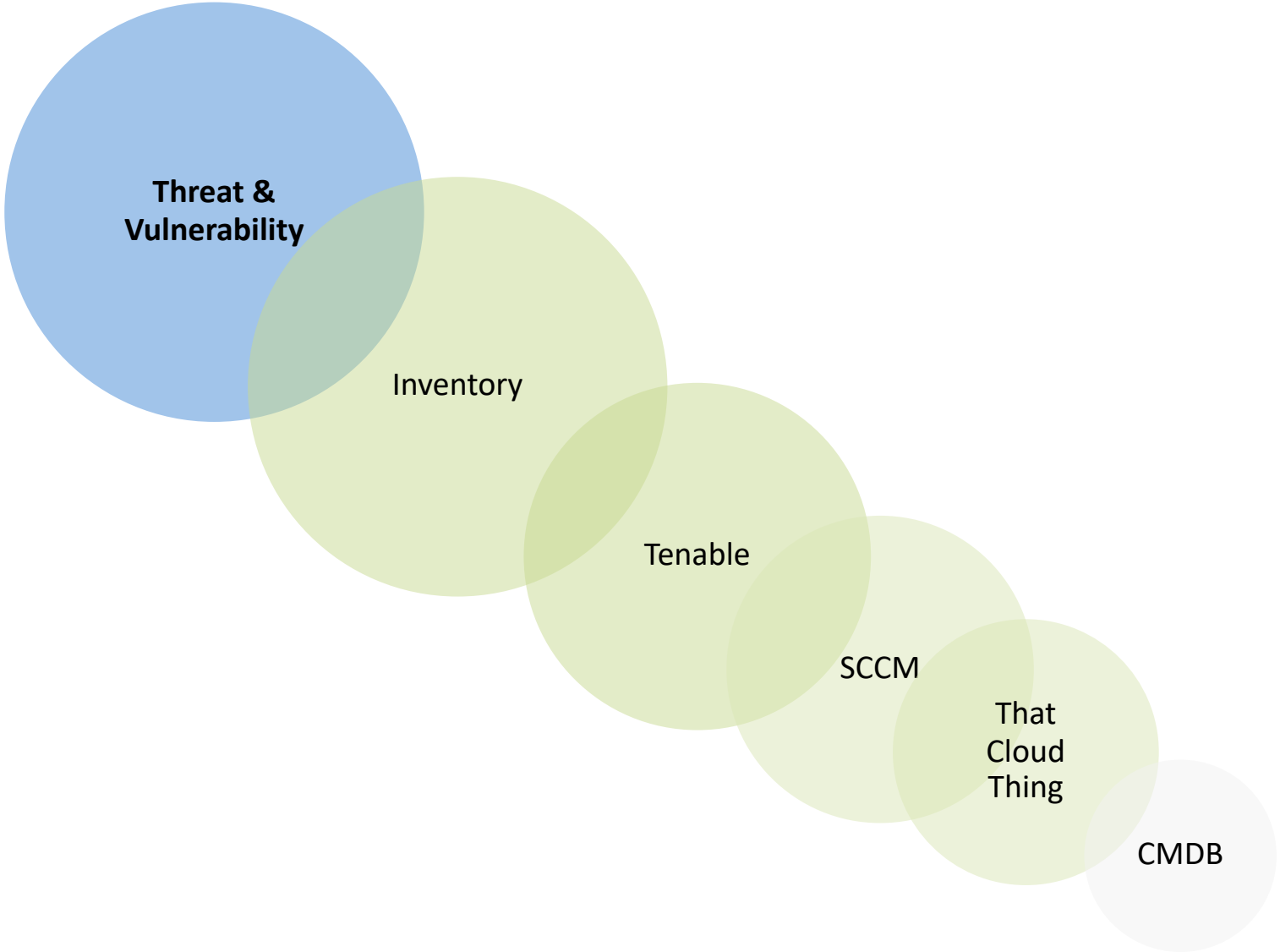
Deliberate – There is no guessing (ok, maybe some)

Looking at typical security

- Network Operations*
- Application Security
- Identity & Access Management
- Security Compliance
- Architecture & Engineering
- Threat Intel & Research
- Threat & Vulnerability
- Security Program
- Security Operations

Each area does a lot

Behind each activity lies more



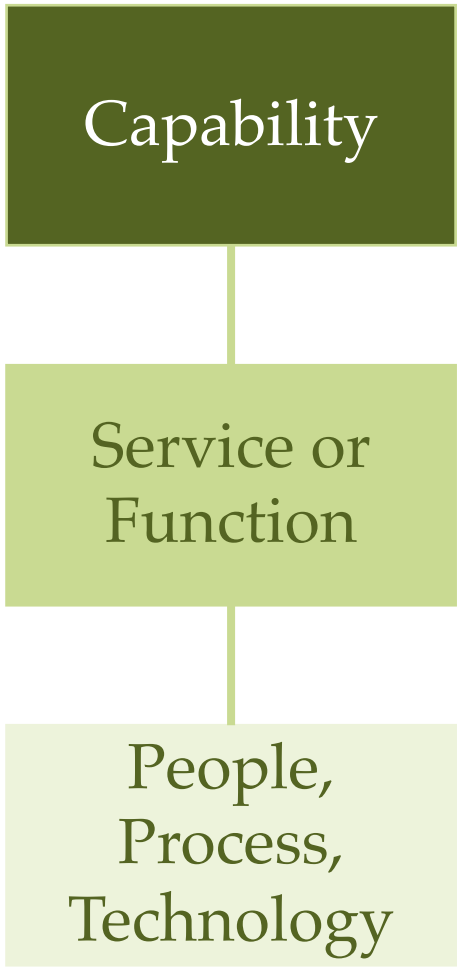
How do we organize this a bit?

A capability model for clarity

A Capability is the management of an ability

A Capability can be broken down into its parts

Those parts are implemented



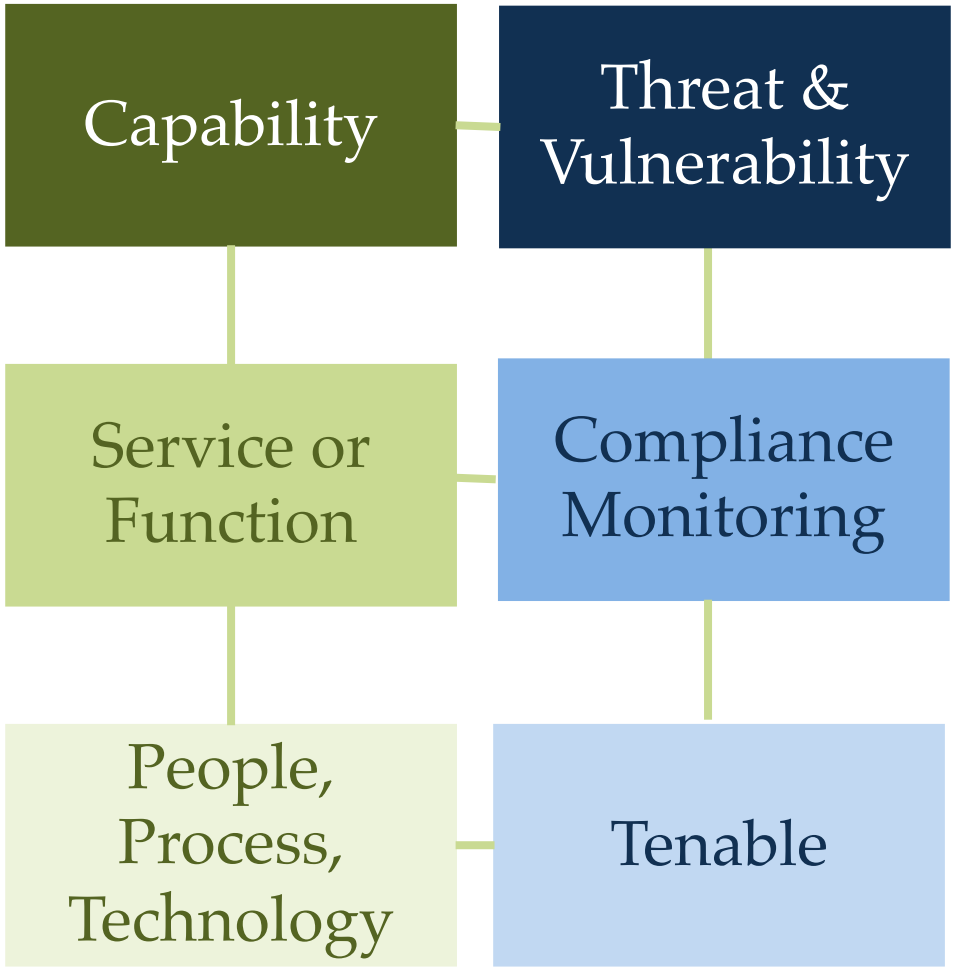

DANGER

The model connects to reality

A Capability is the management of an ability

A Capability can be broken down into its parts

Those parts are implemented



T&V is an area that must be managed

Compliance is a service, and has many functions

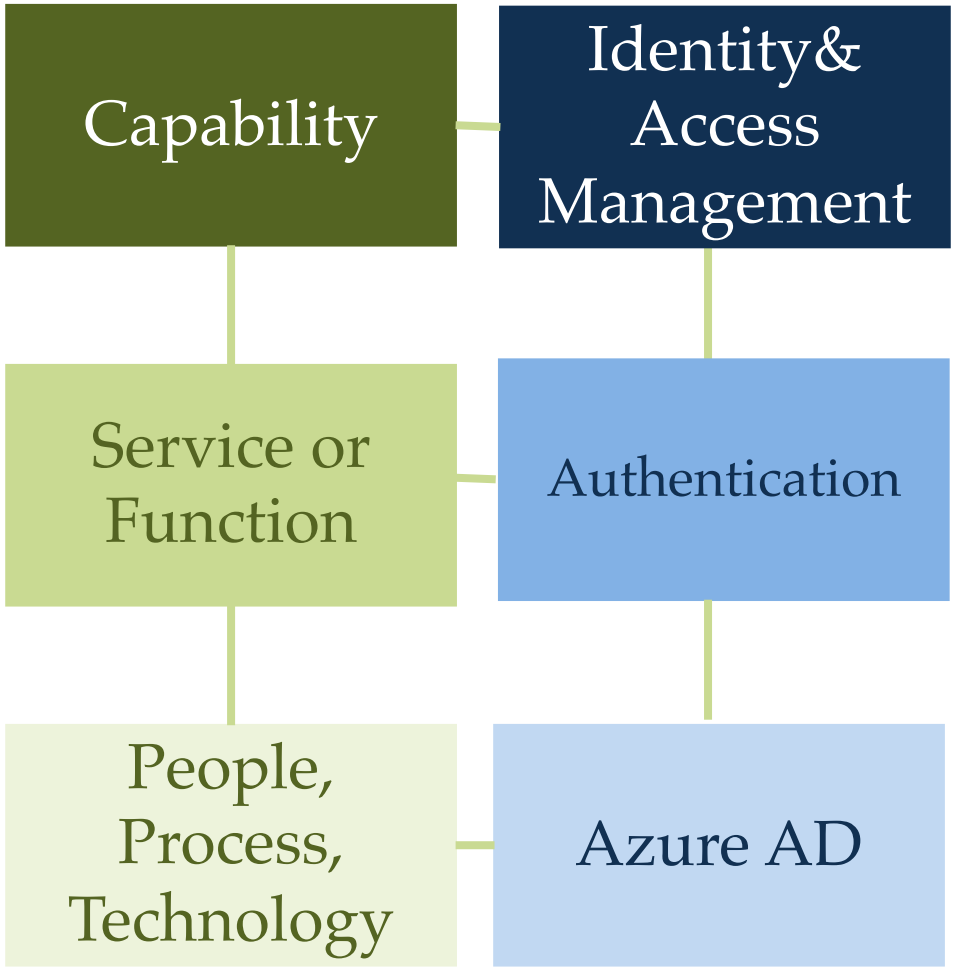
A technology that implements compliance

Another example

A Capability is the management of an ability

A Capability can be broken down into its parts

Those parts are implemented



IAM is an area that must be managed

Authentication is a service, and has many functions

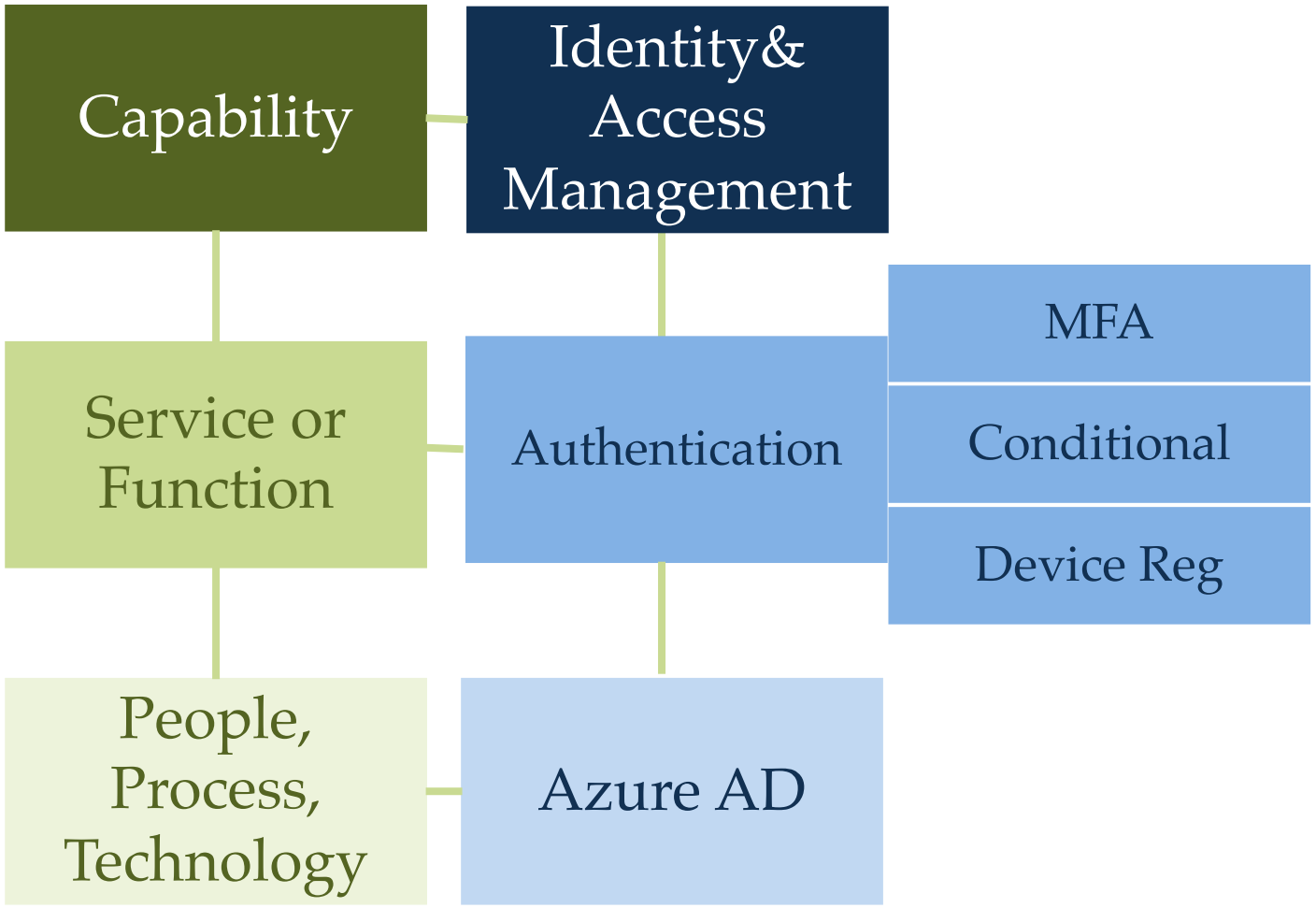
A technology that implements Authentication

More detail

A Capability is the management of an ability

A Capability can be broken down into its parts

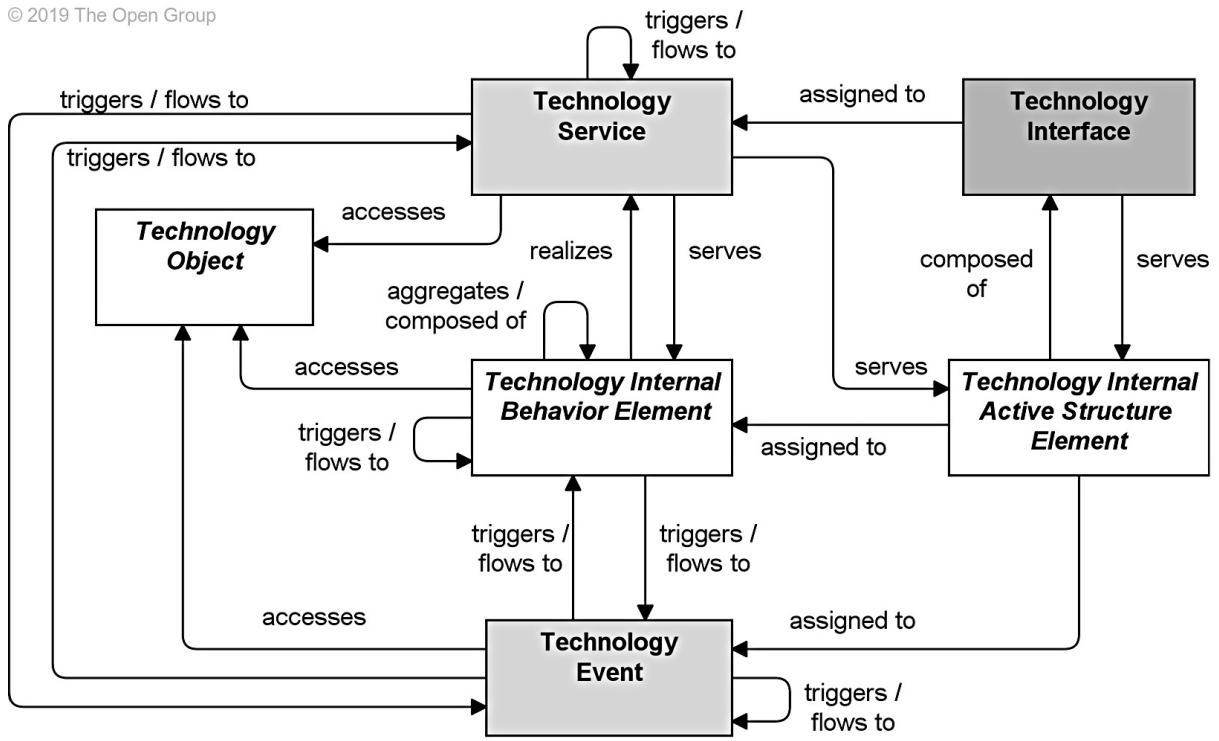
Those parts are implemented



Geeky note

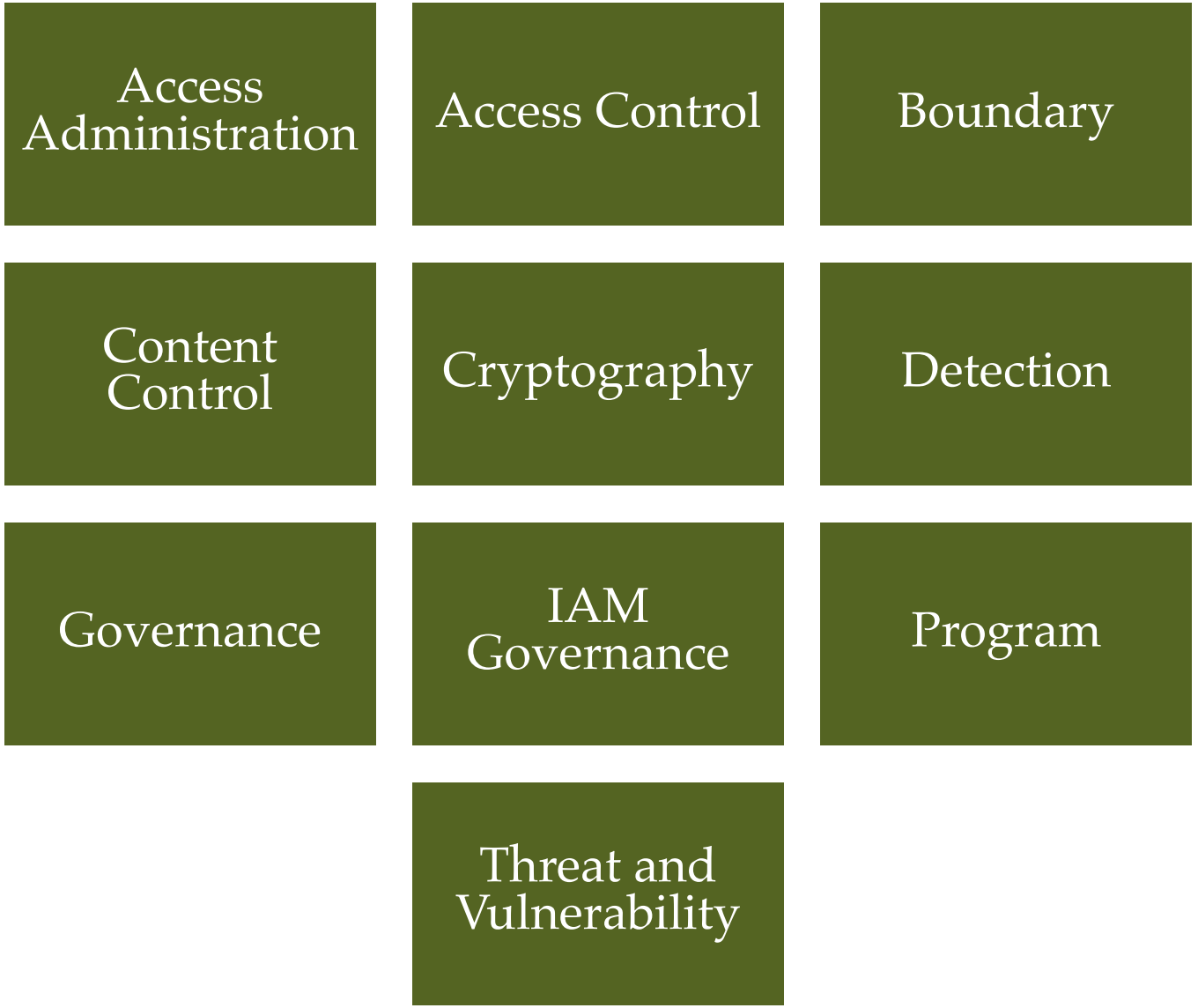
There is a logical SERVICE like "Compliance Monitoring"

There is also an implementation of that LOGICAL SERVICE that the industry also may call a SERVICE. We purchase services that are a service, and you can have cloud service providers.



Archimate is an example of a modeling language used to clear up these types of description

Common InfoSec capabilities



The Capability

The Service or Function

Access Admin
Administration
Directory
Identity
Provisioning
Synchronization

Access Control
Risk-Based Authentication
Authentication
Authorization
Federation
Policy-based Access
SSO
Federation
Multi/2Factor Authentication

Boundary
Firewall
Network Access Control
Proxy
Segmentation
System 2 System
User Connectivity
VPN
WAF

Content Control
Anti-Spam
Anti-Virus/malware
Data Encryption
Data Loss
Drive/Vol Encryption
Email Behavior Analysis
Email URL Protection
Phishing Education
Phishing Protection
Sandboxing
URL Filtering/Listing

Cryptography
Digital Signatures
Encryption
Key Management
Public Keys/Asymmetric
Secret Orchestration

Detection
Anomoly Detection
Endpoint Detection
Host Detection
Logging
Managed Security Provider
Network Detection
Security Event
Wireless Detection

Governance
Assurance
Awareness
Incident
Training

IAM Governance
Access Certification
Cloud Access
IAM Forensics
Privileged Access

Program
Arch & Engineering
Capacity
Planning
Policy
Strategy

Threat & Vulnerability
Asset Control
Compliance Monitoring
Mobile Application
Mobile Device
Patching
Research/Intelligence
Vulnerability
DAST
SAST/CAS

Capabilities and high-level services

MANAGEMENT CAPABILITY
SERVICE or FUNCTION

Capability examples

Access Admin
Administration
Directory
Identity
Provisioning
Synchronization

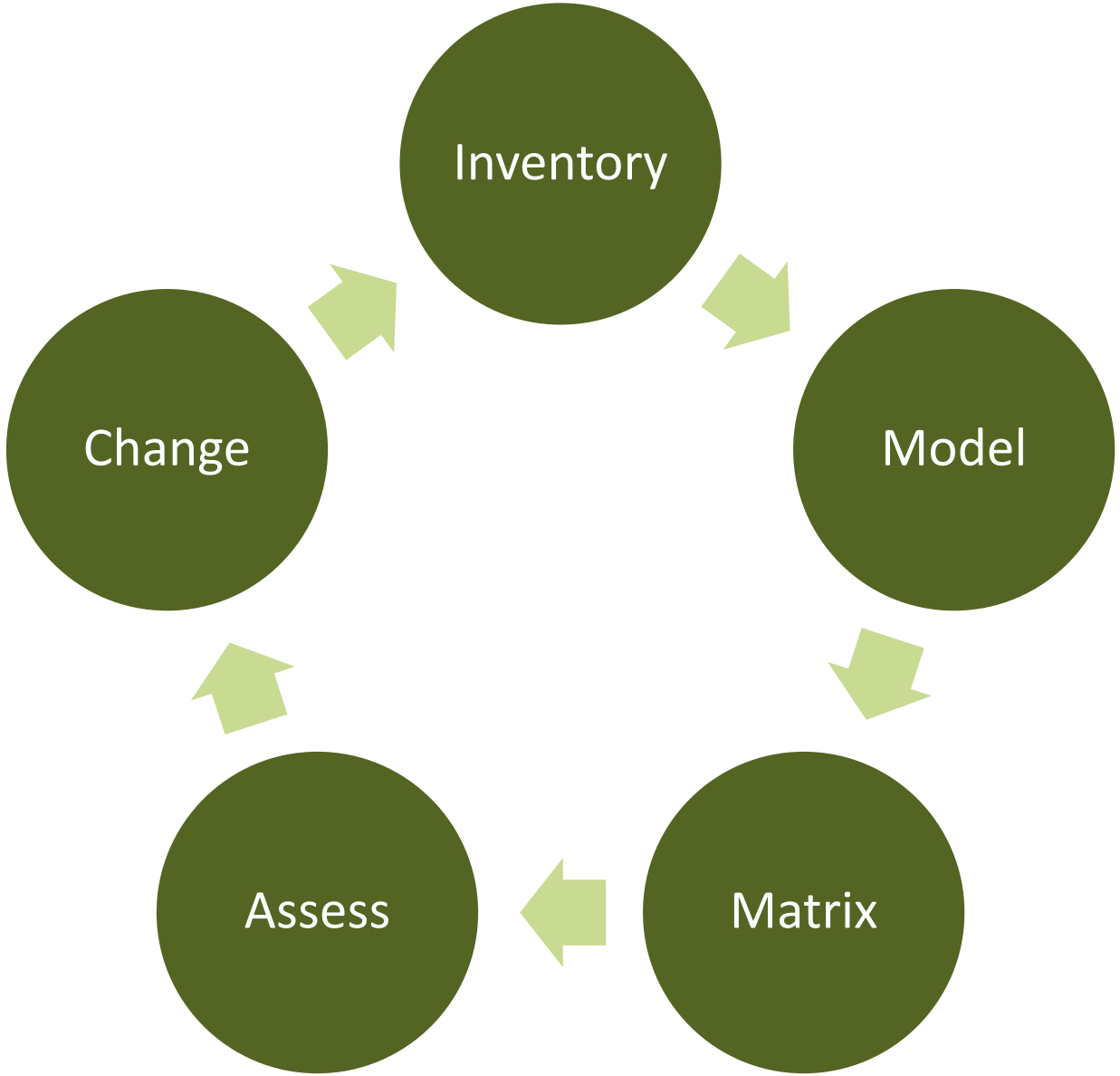
Access Control
Risk-Based Authentication
Authentication
Authorization
Federation
Policy-based Access
SSO
Federation
Multi/2Factor Authentication

Boundary
Firewall
Network Access Control
Proxy
Segmentation
System 2 System
User Connectivity
VPN
WAF

This is a catalog of capabilities, not necessarily the capabilities you have.

Great to know but are we there yet?

The approach



Making a list

Inventory

- Make a list of your people/roles, processes, and technologies
- Look for where you have implemented security
- Group similar things together

Capability Area	Service/Function	Description	Notes
Access Administration		Creation and maintenance of elements necessary for runtime access control.	
Access Control		Runtime authentication and authorization services.	
Boundary		and across physical and logical areas specifically where the security policy/ownership varies.	
Content Control		Protecting data to keep its original intent, provide confidentiality, integrity, and potentially limit the types of contents being interacted with.	
Cryptography		Secure communications and storage techniques. This is often a horizontal or shared services and used across other capabilities.	
Detection			
Governance		General oversight and associated horizontal activities.	
IAM Governance		Oversight specifically related to identity and access management.	
Program		The overall security program.	
Threat and Vulnerability			
Access Admin	Administration		
Access Admin	Directory		

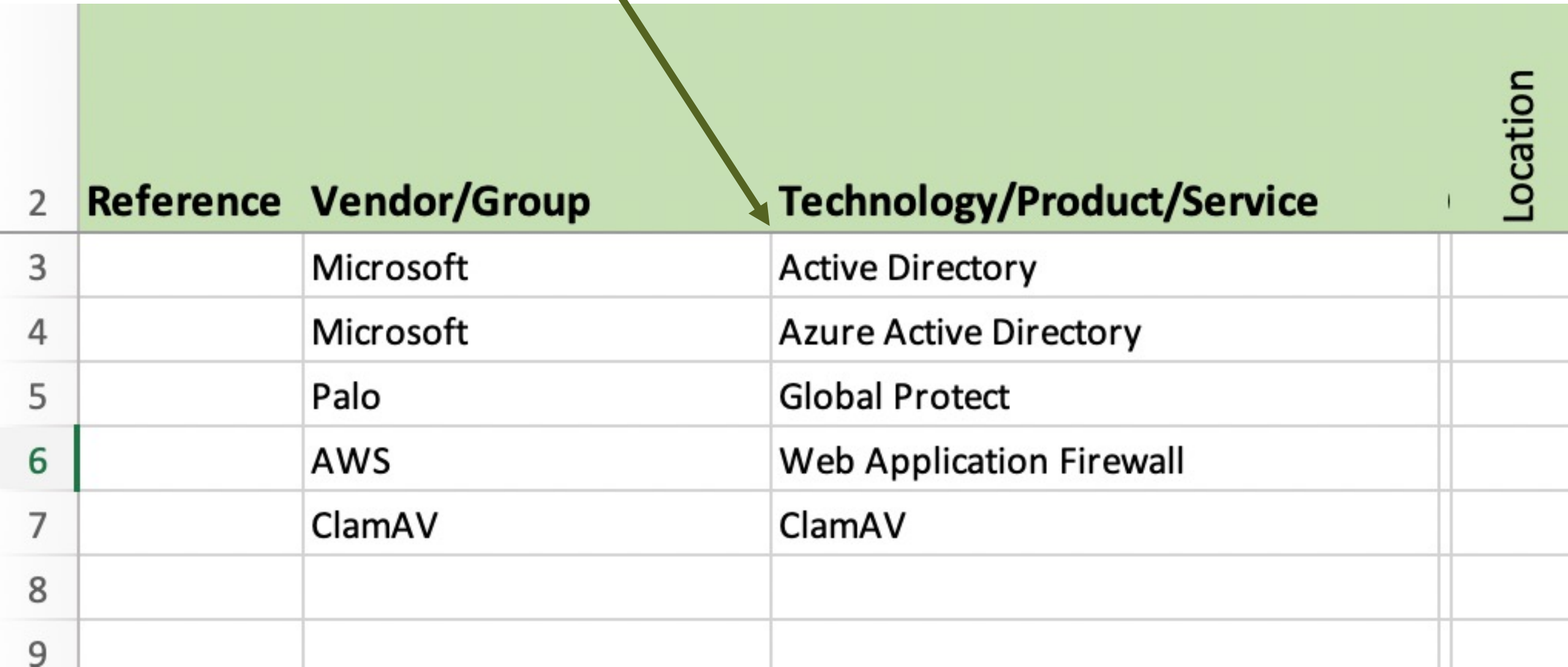
Model and Matrix

Model & Matrix

- Compare you list to the capability model
- Add your implementations to the Matrix

						AA	AA	AA	AA	AA	AA	AC	AC	A
Reference	Vendor/Group	Technology/Product/Service	Location	Technology/Service Meets	Technology/Service Partial	Administration	Directory	Entitlement	Identity	Provisioning	Synchronization	Adaptive Risk	Authentication	
	Microsoft	Active Directory		3	3		M	P	M				M	
	Microsoft	Azure Active Directory		12	1	M	M	M	M	M	M	M	M	
	Palo	Global Protect		1	0									
	AWS	Web Application Firewall		1	0									

The implementation of security



	Reference	Vendor/Group	Technology/Product/Service	Location
3		Microsoft	Active Directory	
4		Microsoft	Azure Active Directory	
5		Palo	Global Protect	
6		AWS	Web Application Firewall	
7		ClamAV	ClamAV	
8				
9				

Technology/Product/Service	Location	Technology/Service Meets	Technology/Service Partial	Administration	Directory	Entitlement	Identity	Provisioning	Synchronization	Adaptive Risk	Authentication	Authorization	Federation
Active Directory		3	3		M	P	M				M	P	P
Azure Active Directory		12	1	M	M	M	M	M	M	M	M	M	M

The number of Services/Functions that are implemented with this technology

The Service/Function being implemented

Technology/Product/Service	Location	Technology/Service	Technology/Service	Administration	Directory	Entitlement	Identity	Provisioning	Synchronization	Adaptive Risk	Authentication	Authorization	Federation	Policy Based Access	SSO
Active Directory		3	3		M	P	M				M	P	P		
Azure Active Directory		12	1	M	M	M	M	M	M	M	M	M	M	M	M
Global Protect		1	0												
Web Application Firewall		1	0												
ClamAV		0	1												
OpenLDAP		4	2	M	M	P	M				M	P			
		0	0												
		0	0												
			Meets	2	3	1	3	1	1	1	3	1	1	1	1
			Partial	0	0	2	0	0	0	0	0	2	1	0	0
			Target State	2	3	2	2	1	1						
			Current State	3	2	2	2	2	2						
			Maturity State	1	-1	0	0	1	1	0	0	0	0	0	0

Maturity assessment using the matrix

Assess

Technology/Product/Service	Location	Technology/Service	Technology/Service	Administration	Directory	Entitlement	Identity	Provisioning	Synchronization
Active Directory		3	3		M	P	M		
Azure Active Directory		12	1	M	M	M	M	M	M
Global Protect		1	0						
Web Application Firewall		1	0						
ClamAV		0	1						
OpenLDAP		4	2	M	M	P	M		
		0	0						
		0	0						
			Meets	2	3	1	3	1	
			Partial	0	0	2	0	0	
		Target State		2	3	2	2	1	
		Current State		3	2	2	2	2	
		Maturity State		1	-1	0	0	1	

By setting a target state and evaluating your current functionality you can get some idea of your general maturity.

You can't necessarily judge the maturity of a capability by the number of technologies that meet a capability. There may be other circumstances that have to be considered.

Assess

Technology/Se	Technology/Se	Administration	Directory	Entitlement	Identity	Provisioning	Synchronizatio	Adaptive Risk
	Meets	1	2	1	2	1	1	
	Partial	0	0	1	0	0	0	
Target State		2	3	2	2	1	1	
Current State		3	2	2	2	2	2	
Maturity State		1	-1	0	0	1	1	

0	N/A
1	Below Baseline
2	Baseline
3	Above Baseline

Visual assessment

Assess

Threat & Vulnerability	
Asset Control	B
Compliance Monitoring	-
Mobile Application	+
Mobile Device	N
Patching	B
Research/Intelligence	+
Vulnerability	B
DAST	B
SAST/CAS	+

- Below baseline

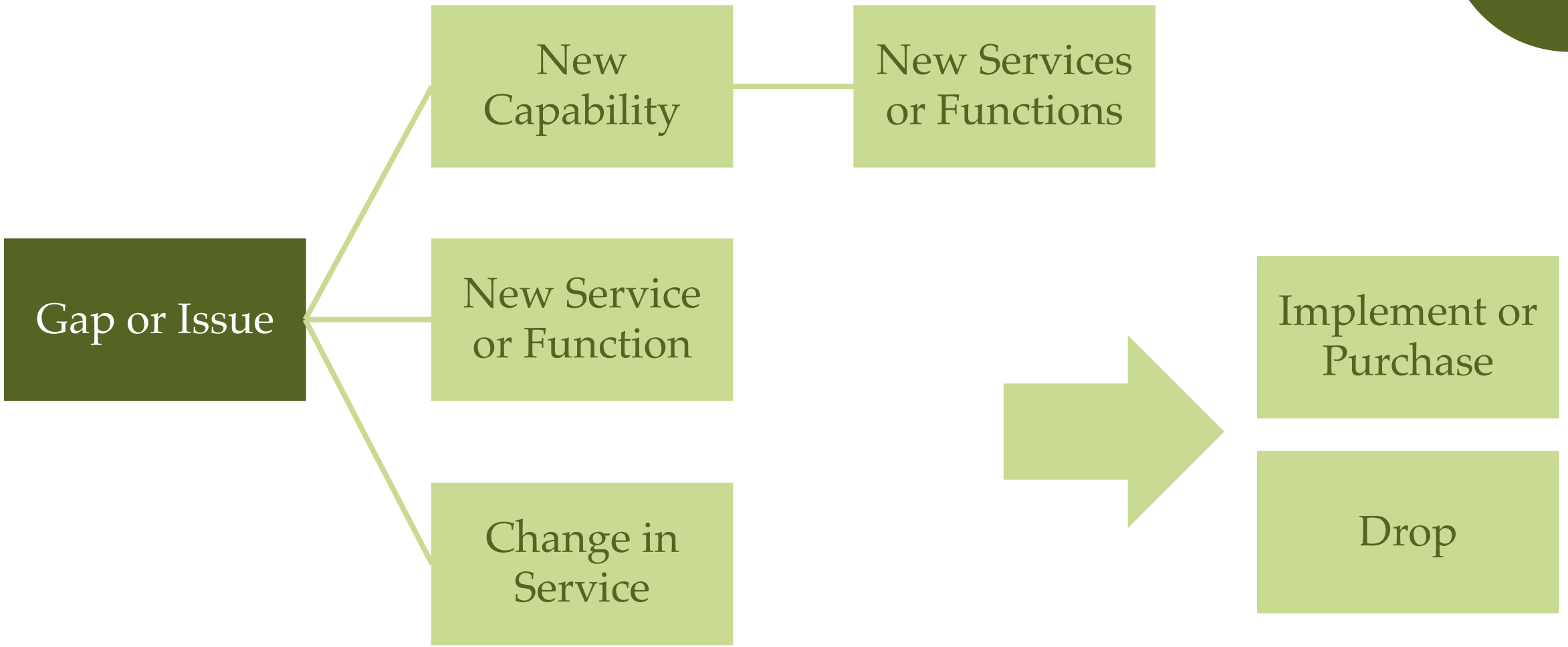
B Baseline

+ Above baseline

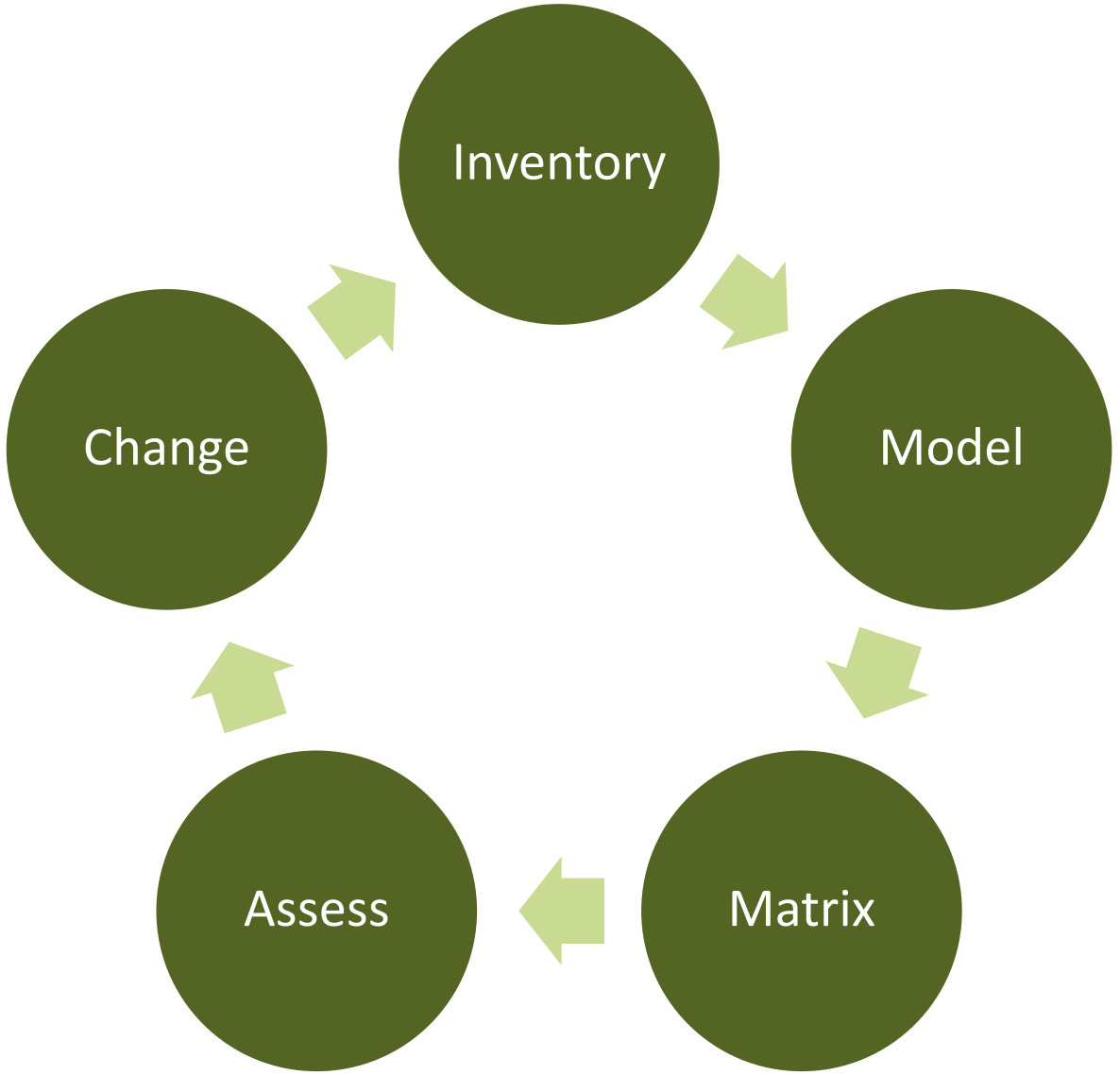
N Not applicable

What about changes

Change



Rinse and Repeat



Visual Mapping

Capability Mapping to the CyberSecurity Framework

Access Admin
Administration
Directory
Identity
Provisioning
Synchronization

Access Control	
Risk-Based Authentication	PR
Authentication	PR
Authorization	PR
Federation	PR
Policy-based Access	PR
SSO	PR
Federation	PR
Multi/2Factor Authentication	PR

Boundary		
Firewall		PR
Network Access Control		PR
Proxy	DE	PR
Segmentation		PR
System 2 System		PR
User Connectivity		PR
VPN		PR
WAF		PR

Content Control			
Anti-Spam			PR
Anti-Virus/malware			PR
Data Encryption			PR
Data Loss	DE	ID	PR
Drive/Vol Encryption			PR
Email Behavior Anal	DE		PR
Email URL Protection			PR
Phishing Education			PR
Phishing Protection			PR
Sandboxing	DE		PR
URL Filtering/Listing	DE		PR

Cryptography	
Digital Signatures	PR
Encryption	PR
Key Management	PR
Public Keys/Asymmetric	PR
Secret Orchestration	PR

Detection	
Anomoly Detection	DE
Endpoint Detection	DE
Host Detection	DE
Logging	DE
Managed Security Provide	DE
Network Detection	DE
Security Event	DE
Wireless Detection	DE

Governance		
Assurance		PR
Awareness		PR
Incident	RE	RS
Training		PR

IAM Governance	
Access Certification	PR
Cloud Access	PR
IAM Forensics	RS
Privileged Access	PR

Program
Arch & Engineering
Capacity
Planning
Policy
Strategy

Threat & Vulnerability			
Asset Control			ID
Compliance Monitoring			PR
Mobile Application	PR		ID
Mobile Device	PR		ID
Patching			PR
Research/Intelligence			ID
Vulnerability	DE	PR	ID
DAST			ID
SAST/CAS			ID
Endpoint Forensics			RS

CSF 1.1 Functions	
ID	Identify
PR	Protect
DE	Detect
RS	Respond
RE	Recover

MANAGEMENT CAPABILITY
SERVICE or FUNCTION

Cryptography	
Digital Signatures	PR
Encryption	PR
Key Management	PR
Public Keys/Asymmetric	PR
Secret Orchestration	PR

Detection	
Anomoly Detection	DE
Endpoint Detection	DE
Host Detection	DE
Logging	DE
Managed Security Provide	DE
Network Detection	DE
Security Event	DE
Wireless Detection	DE

Governance		
Assurance		PR
Awareness		PR
Incident	RE	RS
Training		PR

IAM Governance	
Access Certification	PR
Cloud Access	PR
IAM Forensics	RS
Privileged Access	PR

Program
Arch & Engineering
Capacity
Planning
Policy
Strategy

Threat & Vulnerability			
Asset Control			ID
Compliance Monitoring			PR
Mobile Application		PR	ID
Mobile Device		PR	ID
Patching			PR
Research/Intelligence			ID
Vulnerability	DE	PR	ID
DAST			ID
SAST/CAS			ID
Endpoint Forensics			RS

CSF 1.1 Functions	
ID	Identify
PR	Protect
DE	Detect
RS	Respond
RE	Recover

MANAGEMENT CAPABILITY
SERVICE or FUNCTION

Can we make decisions like a boss yet?

What technologies and implementations do we have for security?

You can now look at your Matrix for the specific area in question

Don't we have something that will do that already?

You can see what you have that overlaps, you may also use addition data (columns) to see what makes them different such as platform or location

We are covering the important stuff, right?

You can ask them what they think is important. It should be in your model. Maybe you need a discussion on what is important.

Is there anything we can DROP, stop supporting, cancel the contract?
What happens when this services goes out of support?

See what specific areas of security will be affected and if you have multiple implementations for that coverage.

Making decisions - Continued

Which way should we grow or improve?
How does this fit with the long-term road map?
How do I plan the work for next year?

Look at your Matrix and diagrams you can see obvious gaps or places that you don't have coverage that is needed. These discoveries should be turned into plans and projects.

I know we just moved to the cloud but I though we already implemented that security thing.

This may take more contextual diagrams or some extra columns in the Matrix to show what platforms apply but it can be answered.

Our security decisions should now be more:

Consistent – A reusable process

Traceable – You can follow you decision path

Valuable – Your answers are meaningful to you and not just guesses

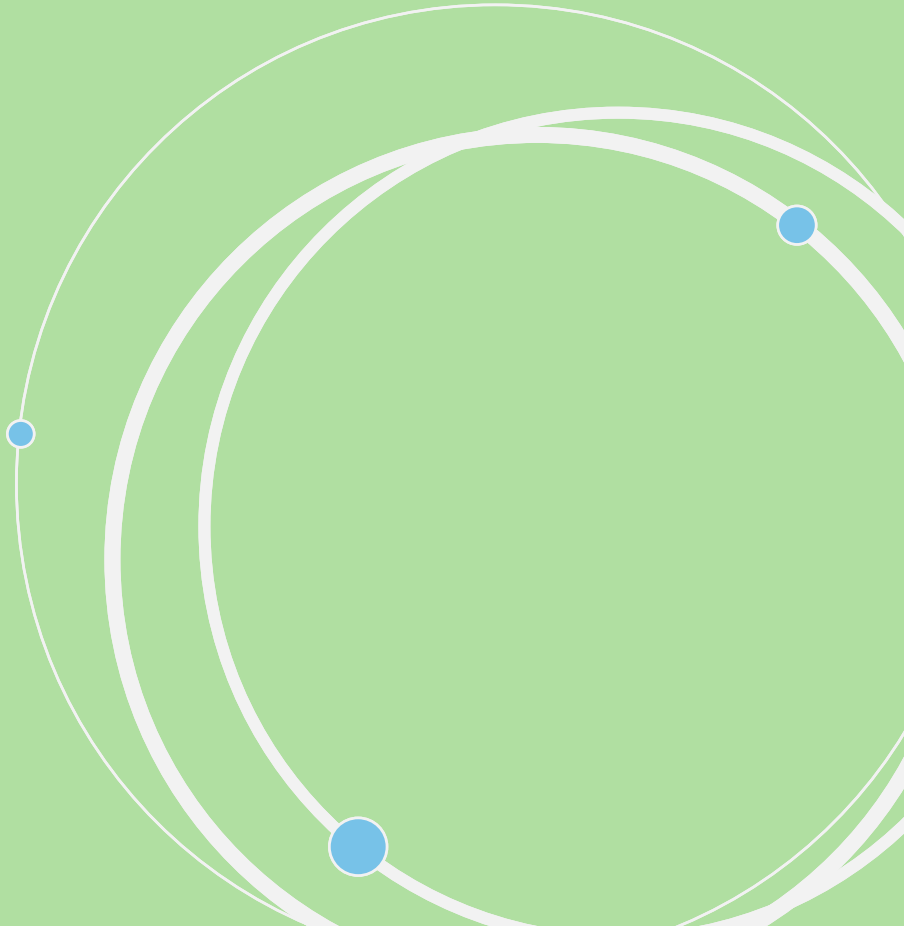
Transparent – The process is open and documented

Deliberate – For the most part

Making Security Decisions Like a Boss

Questions?

Ron Parker
https://github.com/scmunk/decisions
http://www.secretchipmunk.com
@scmunk



REFERENCES

Making Decisions Like a Boss Artifacts
https://github.com/scmunk/decisions

Archimate
https://pubs.opengroup.org/architecture/archimate3-doc/chap01.html#_Toc10045266

Archi – a modeling tool
https://www.archimatetool.com

Draw.io – a diagramming tool, there is an offline version too
https://app.diagrams.net