Asset Management:
what it is and do we still need-it?

Andrej Volchkov

avolchkov@volchkov.ch

www.volchkov.ch

September 2019

ISACA®

3rd ISACA Belgrade Chapter Day – 50th Anniversary

Objectives

Information, like any other asset has to be managed and protected accordingly.

The objectives of the session are:

1. Reminder of what Information Asset Management is all about.
2. Give some insights on pragmatic Asset Management.
3. Bring some ideas on how to compile an Asset Inventory.

But first: take a look at Past, Present and Future

Past Present Future

Example 1: Client – Service relationship (ex: Travel industry)

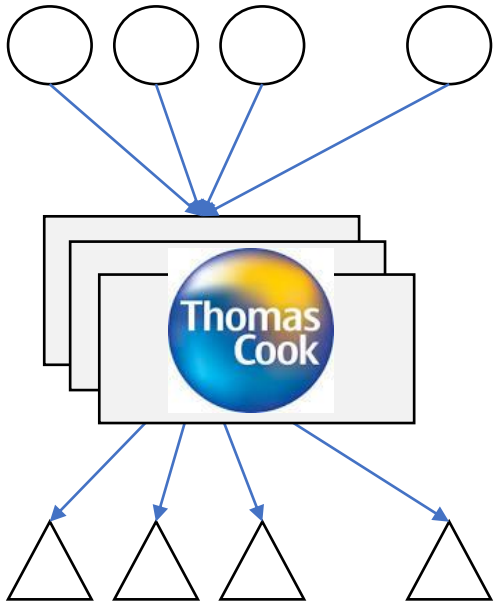
Agency

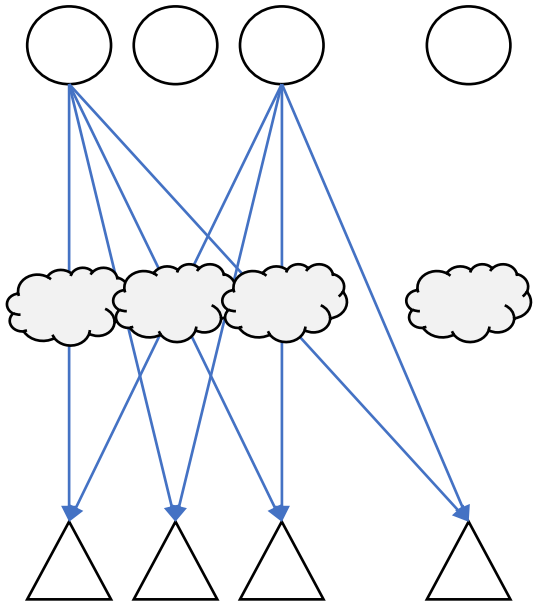
Intermediary

Self provisioning

Client

Service provider





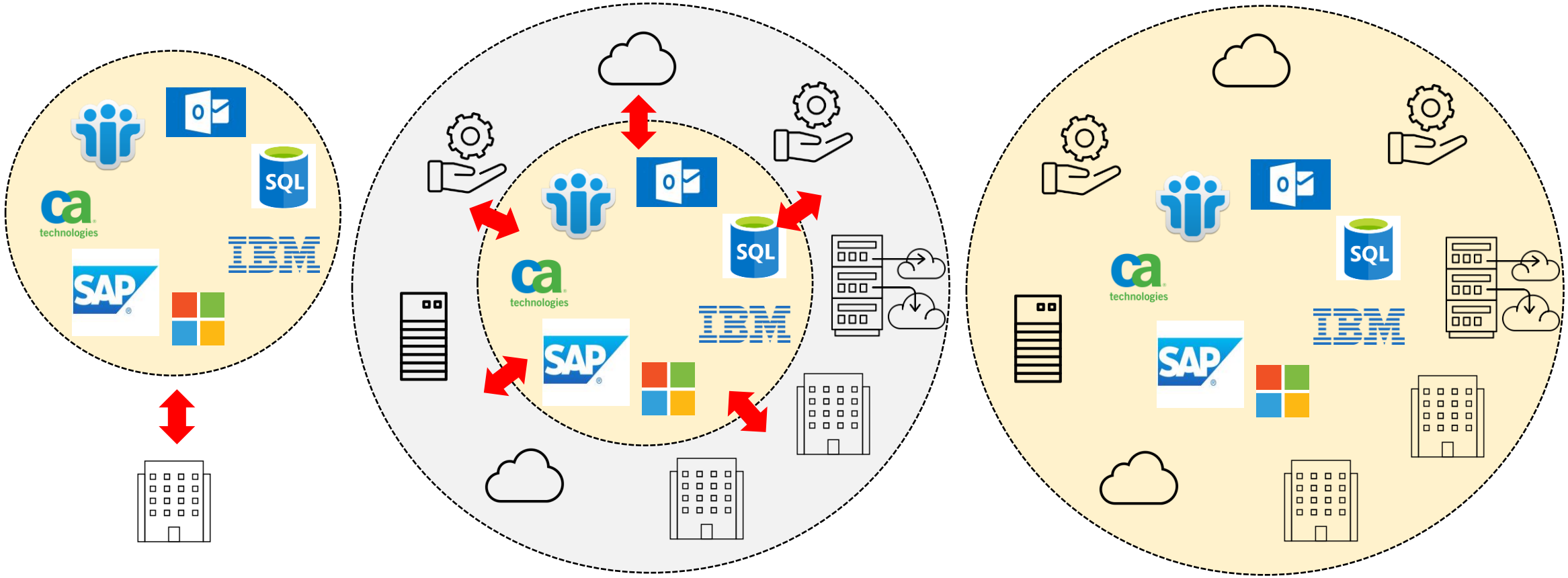
Blockchain (integrity)
Digital Receipts

Example 2: Business environment

Controlled ICT

Extended enterprise

Integrated / Virtual



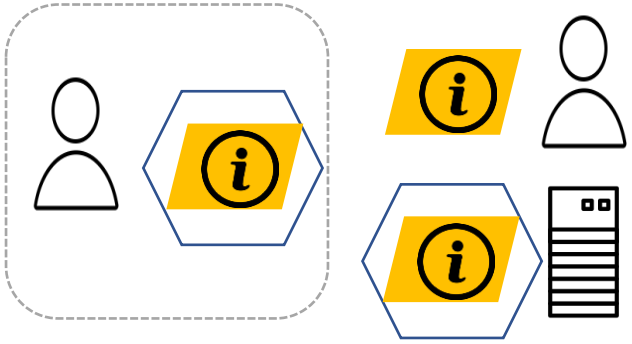
Example 3: Asset management / Data protection

Perimeter protection

- Mainframe, central DB
- Limited visibility
- Perimeter protection
- Access Rights within the enterprise

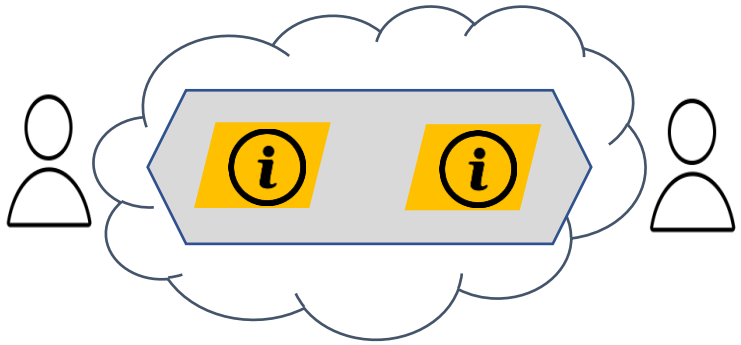
In-depth Data Protection

- Process and data sharing
- Close Data Protection
- Rule based protection
- Privacy regulations



Life-cycle Data Protection

- Self-regulated extensive information availability
- Big data / info market
- Privacy as fundamental right (digital trust)



Back to our subject: main topics

1. What is Information Asset Management (AM)?
2. Categories of Assets.
3. Asset Classification.
4. Roles and responsibilities in Asset Management.
5. Asset Inventory and how to build it?
6. Conclusion / Take-aways.

1. What is Information Asset Management (AM)?

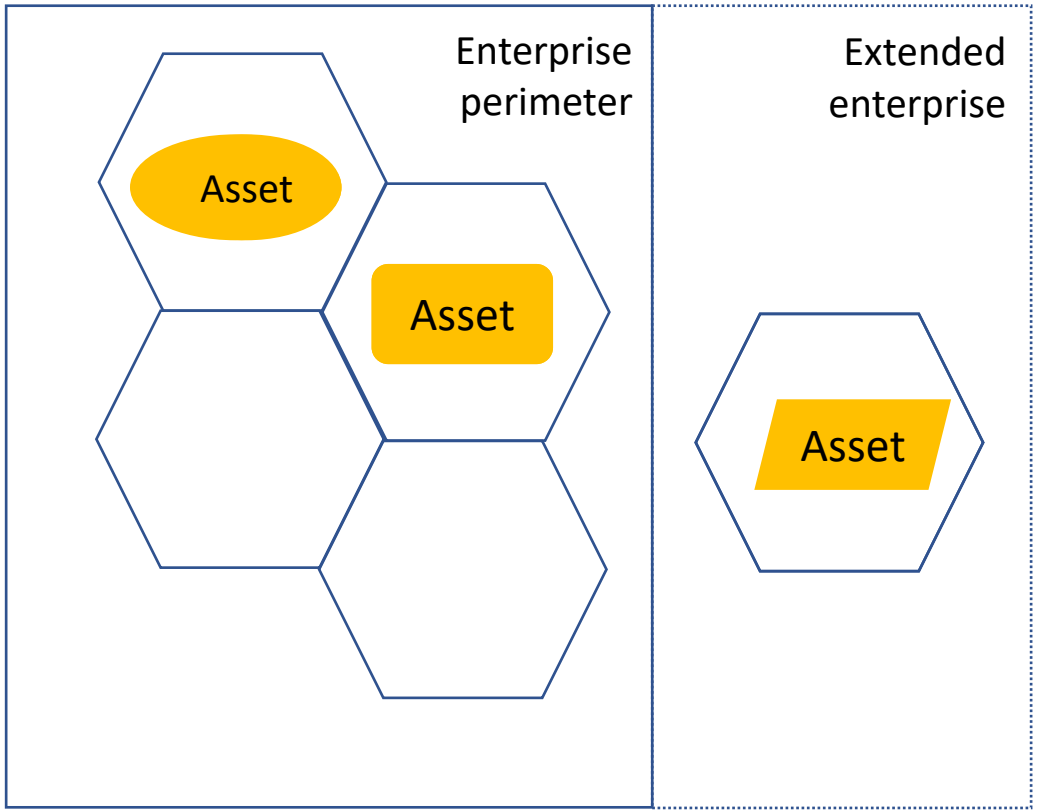
- "*…an asset is an “item, thing or entity that has potential or actual value to an organization*" (*ISO 55000 - Asset management)*.
- AM encompasses a series of core activities along with accountability in the management and governance of asset protection.
- AM is not only about data, but also about data usage and means of accessing information (applications, storage, network).
- Implementing security controls without knowing "what" and "how" (to what extend) to protect would be either too costly or inefficient.
- AM is a prerequisite to risk management (threats and vulnerabilities).
- Recommended by all standards and regulatory frameworks.
- Essential concepts: Classification, Protection rules and Accountability (ownership).

Three Level Control Framework (Sec. Governance)

Policies	Strategy	Organization	Strategic
Risks	Program	Reporting	Tactical
Assets	Compliance	Metrics	
	Operations		Operational

Asset Management helps:

1. Optimize protection system (IDS, network partitioning, Data Loss prevention, etc.)
2. Build more efficient protections closer to the data (in-depth protection).
3. Protect assets in Extended enterprises.
4. Develop security policies based on asset classification.
5. Risk identification: start from asset, then identify threats and vulnerabilities.

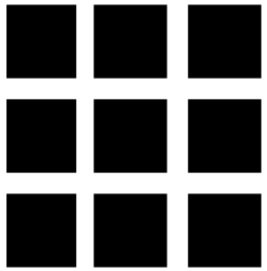


2. Categories of Assets

1. Data on all media (database, paper, office file, etc.)
2. Applications or software
3. Hardware and equipment (laptops, servers, mobile devices, USB)
4. Network as a support for information flows
5. Infrastructure (as a means for information availability)
6. People (knowledge of employees and third parties)
7. Digital footprint (outside the enterprise)

3. Asset Classification

1. By Confidentiality (different categories of asset visibility or accessibility).
2. By Criticality (availability and integrity).
3. "Highly confidential" might not be considered "highly critical" and vice versa.
4. The number of classification levels depends on risk appetite or the willingness to apply differentiated protections according to the class and type of asset.
5. The need for specific protection is an indicator for a "new" class. If everything has to be protected the same way, then one class is enough.



Protective measures should be defined for each asset class and context of usage

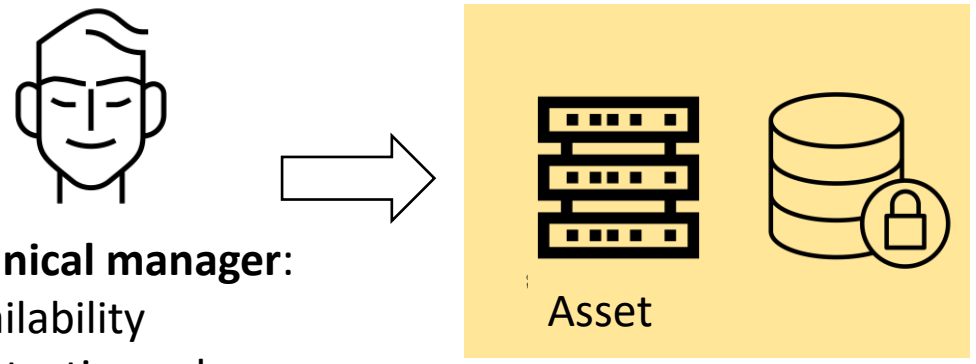
1. Data Hiding - make data unusable in case of loss or theft
2. Access control - limit the exposure of assets solely to those who need to access them
3. Disposal of assets - limit the area exposed to incidents and reduce complaints and legal accountability
4. Supervision - to identify inappropriate patterns of use (usage monitoring..)
5. Availability and integrity assurance - backups, availability, disaster recovery, business continuity, recovery

Type of asset		Application	Office document	Database	Removable Media
Class		A	B	C	D
Confidential	1	Rule A.1	Rule B.1	Rule C.1	Rule D.1
Internal use	2	Rule A.2	Rule B.2	Rule C.2	Rule D.2
Public	3	N/A	Rule B.3	N/A	N/A

Rule B.1: *Office documents classified as "confidential" must be systematically encrypted or filed in protected folders. They cannot be consulted while outside the company.*

4. Roles and responsibilities in asset management

1. Formal responsibility for assets is a guarantee of good risk management and adequate controls.
2. Functional vs Technical responsibility.
3. Data owners or application owners have semantic knowledge of the assets.
4. Central data accountability function: Chief Data Officer (CDO), Data Protection Officer (DPO), Data Architect, …
5. "Asset owners" help CISOs, governing bodies and business executives in the more effective asset management.



Technical manager:
- availability
- protection rules

Functional manager (owner):
- confidentiality and integrity
- semantics and usage

5. Asset Inventory and how to build it

1. Asset inventory is seen as "costly", "inefficient" and even "not necessary".
2. A security program may exist even if the assets to be protected have not been formally identified. However… it would be either too expensive or ineffective.
3. Without knowing exactly "what" assets (class of…) and "how" to protect them, the security program could not be targeted and therefore not optimized.

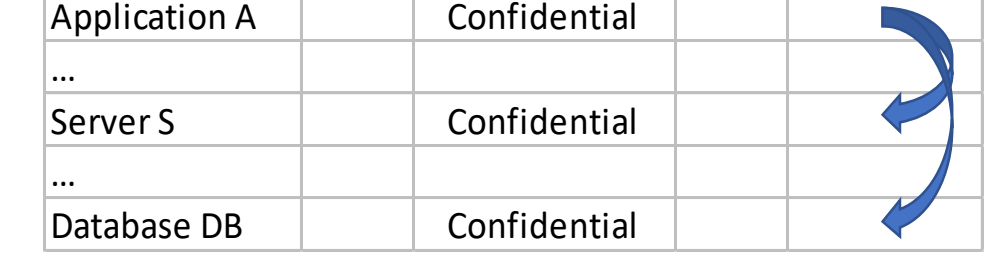
Example:

Grouping or virtualizing application servers of different criticality classes on the same physical servers does not facilitate the implementation of a differentiated recovery (DRP) strategy.

Essential attributes of Asset Inventory

1. Unique identifier,
2. Name,
3. Description,
4. Category or type - to be defined internally,
5. Confidentiality class,
6. Criticality class,
7. Owner or accountable (person or department),
8. Personal data (Y/N),
9. Other sensitive data (Y/N) - to be defined,
10. Location,
11. Used by third party (Y/N),
12. References to other related assets - dependency links.
13. Referencing business units and processes that use the asset.

Asset inventory				
Asset	…	Class	…	Link reference
Application A		Confidential		
…				
Server S		Confidential		
…				
Database DB		Confidential		



The inventory should contain dependency links between the assets.

How to build an Asset Inventory it in a pragmatic way

1. Most organizations already have some basic elements of an inventory: applications, classification.
2. ITAM (IT Asset Management) or Configuration Management Data Base (CMDB) could be a starting point.
3. Lists to be filled in by hand progressively as assets are identified, assigned to someone's responsibility.
4. Data mapping tools: questionnaire to identify applications, data or other resources used in business operations. It helps identify the assets, understand their usage and the data lifecycle.

Example

Article 30 of the GDPR (European General Data Protection Regulation) requires companies to establish "records of processing activities" in order to understand how personal data are actually processed. The goal is to be able to answer the questions "Why are these personal data collected?" and "What processes need these data?"

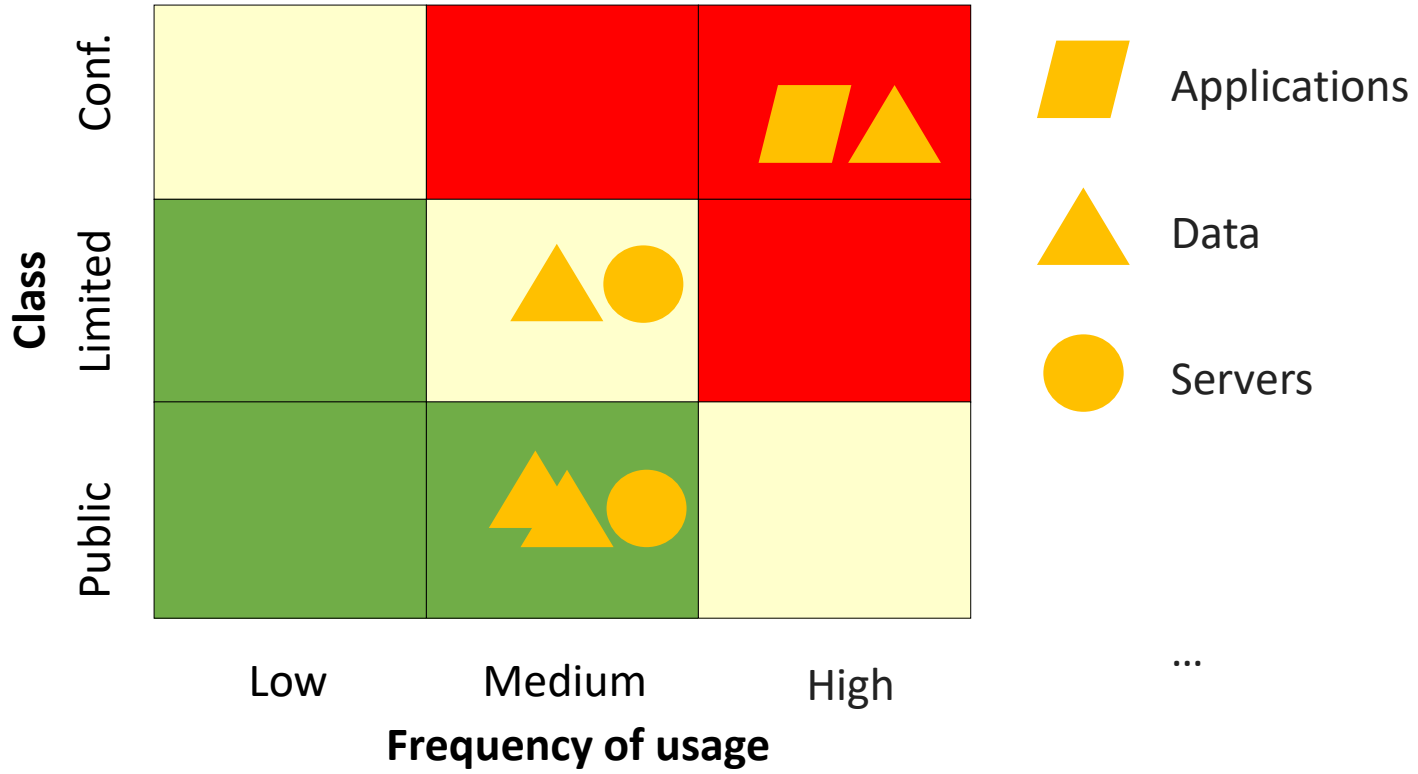
Functional mapping

- Show how applications (as assets) are used.
- This mapping can come from an asset inventory as long as the attributes of the applications contain a reference to the processes and business units that use them.

Function	Process	Business Unit 1	Business Unit 2	Business Unit 3	…	Business Unit n
Production	Purchase		A1			
	Controlling	A1				
	Stock mgmt			A1		
						A2
	Production		A2			A2
				A2		
Corporate functions	HR	A3	A3	A3	A3	A3
		A3				
	Risk	A4	A4	A4	A4	A4
	Finance			A2		
					A2	
			A2	A2		
	Legal & Compliance			A4	A4	
		A4	A4			
Relationship mgmt	CRM	A5		A5		A5
	Suppliers		A5	A5		
	Support				A5	
		A6	A6	A6	A6	A6
	Contracts	A2				
Sales	Marketing				A5	
			A5			
	Sales		A5	A5		
Etc.						

Example of usage to track the current level of asset protection

Insufficiently protected assets



6. Conclusion / Take-aways

1. AM is implicitly done in every organization but - be more formalized.
2. Establish the categories of assets and their classifications.
3. Build regulatory framework around asset classes (Class / Context / Protection rule).
4. Establish asset accountability (ownership) outside the technical team.
5. Build a pragmatic asset inventory starting with tools you already have.
6. Enrich your inventory gradually.

Than you for your attention

Andrej Volchkov

avolchkov@volchkov.ch

www.volchkov.ch

September 2019