From:	Lieven Van Uytfanghe
To:	cyberframework
Subject:	CSF 2.0 Draft / Comment - Page 36 - Identity Management, Authentication, and Access Control (PR.AA)
Date:	Thursday, November 2, 2023 7:43:32 AM
Attachments:	image.png image.png Outlook-1480441769.png

Dear,

As a practitioner in Enterprise Cybersecurity Architecture, I regularly employ this framework in my interactions with various stakeholders on a daily basis Please find my feedback and suggestion regarding the specified topic with this mail

For me identity management belongs to the identify function/pilar   The authentication and authorization part of identity and access management definitely belong to the protect function/pilar

It would also be more consistent with the ideas, concepts and text of page 33 where you identify people under asset management   People asset management relate to identity managment

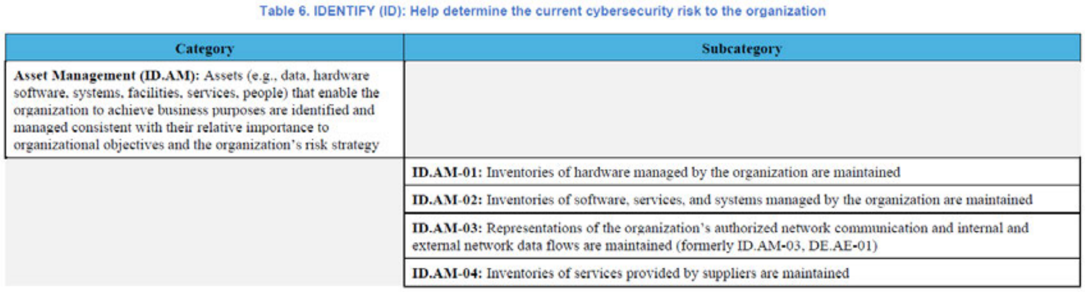
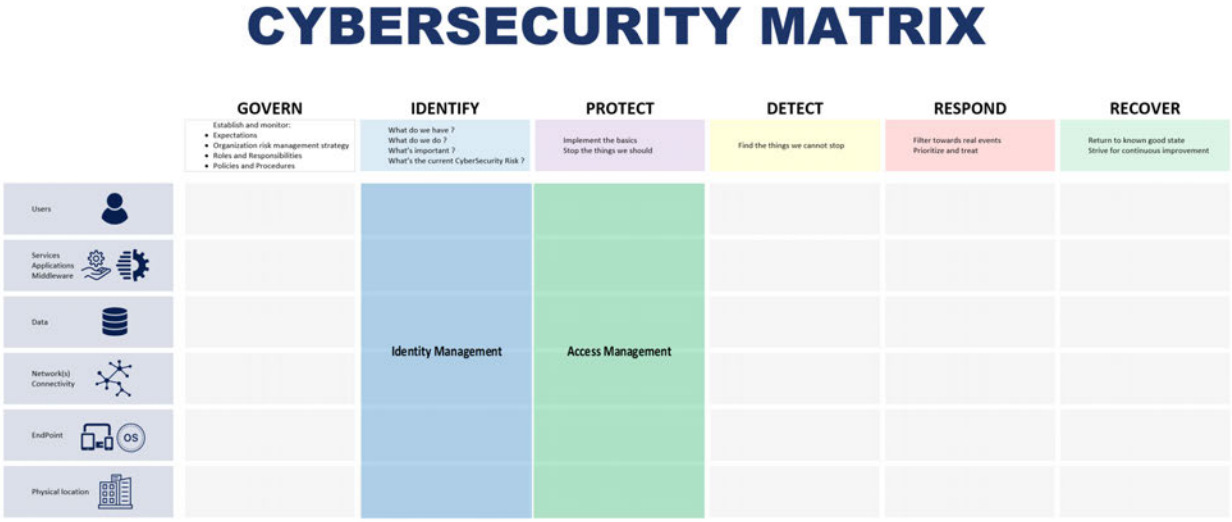


Table 6. IDENTIFY (ID): Help determine the current cybersecurity risk to the organization

Category	Subcategory
Asset Management (ID.AM): Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	
	ID.AM-01: Inventories of hardware managed by the organization are maintained
	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained
	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained (formerly ID.AM-03, DE.AE-01)
	ID.AM-04: Inventories of services provided by suppliers are maintained

This is how I coach people IdAM



CYBERSECURITY MATRIX

	GOVERN	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
	Establish and monitor: • Expectations • Organization risk management strategy • Roles and Responsibilities • Policies and Procedures	What do we have ? What do we do ? What's important ? What's the current CyberSecurity Risk ?	Implement the basics Stop the things we should	Find the things we cannot stop	Filter towards real events Prioritize and treat	Return to known good state Strive for continuous improvement
Users		Identity Management	Access Management			
Services Applications Middleware						
Data						
Network(s) Connectivity						
EndPoint						
Physical location						

The govern function needs to be perhaps also horizontally depicted Still reflecting and experimenting with it

Best Regards,

Lieven Van Uytfanghe
Consultant

www.ict-security.be

ICT SECURITY
[redacted]
[redacted]

This message should on y be read by those persons to whom it is addressed and may contain confident al information. If you have received this message n error please not fy ict-security and delete the message from your system.