Networks • Services • People

Security Baseline for NRENS

Michael Schmidt
On behalf of GN4-3 WP8 T2

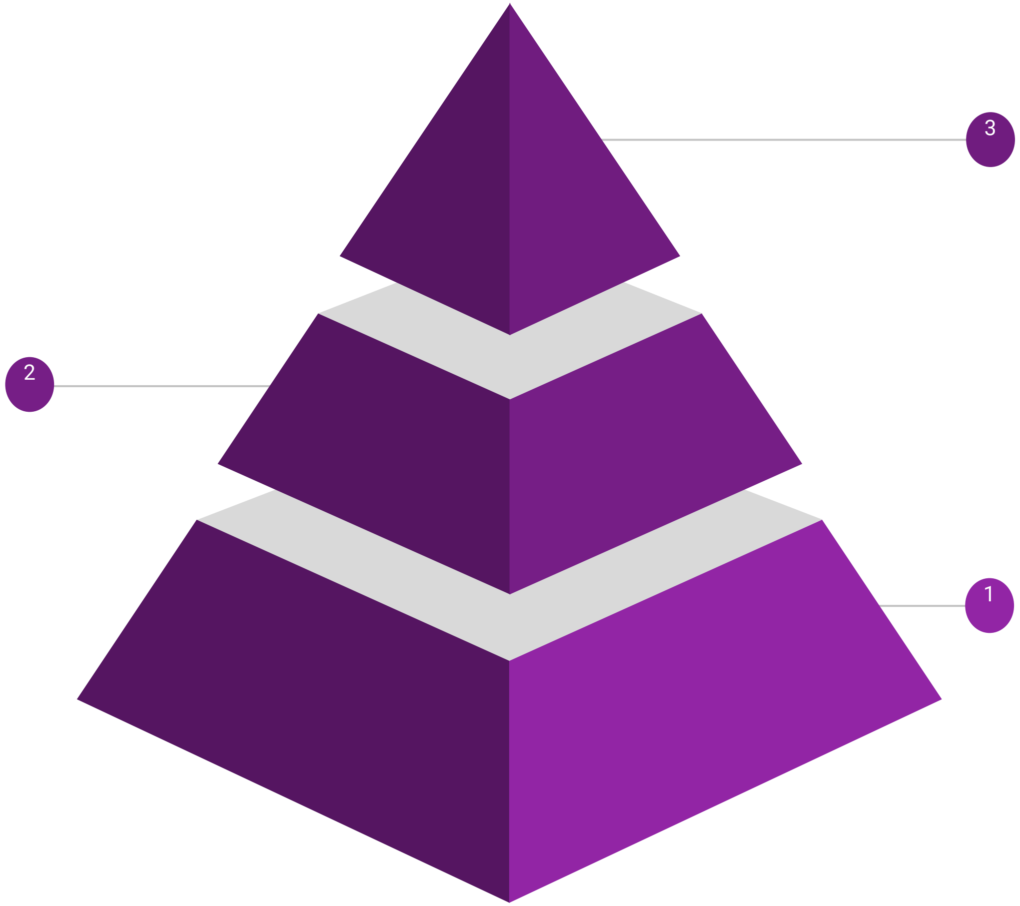
SIG-ISM Workshop, Online, 29.10.2020

Public

How to define a baseline

- Common security standard across GÉANT
- Defined and comparable security levels
- A framework specifically adjusted to NRENS
- Don’t reinvent the wheel

Towards the next maturity level



Expert

10% of NRENS

Sophisticated security program. Only a few NRENS are already compliant. This is the long term goal to achieve.

Advanced

30% of NRENS

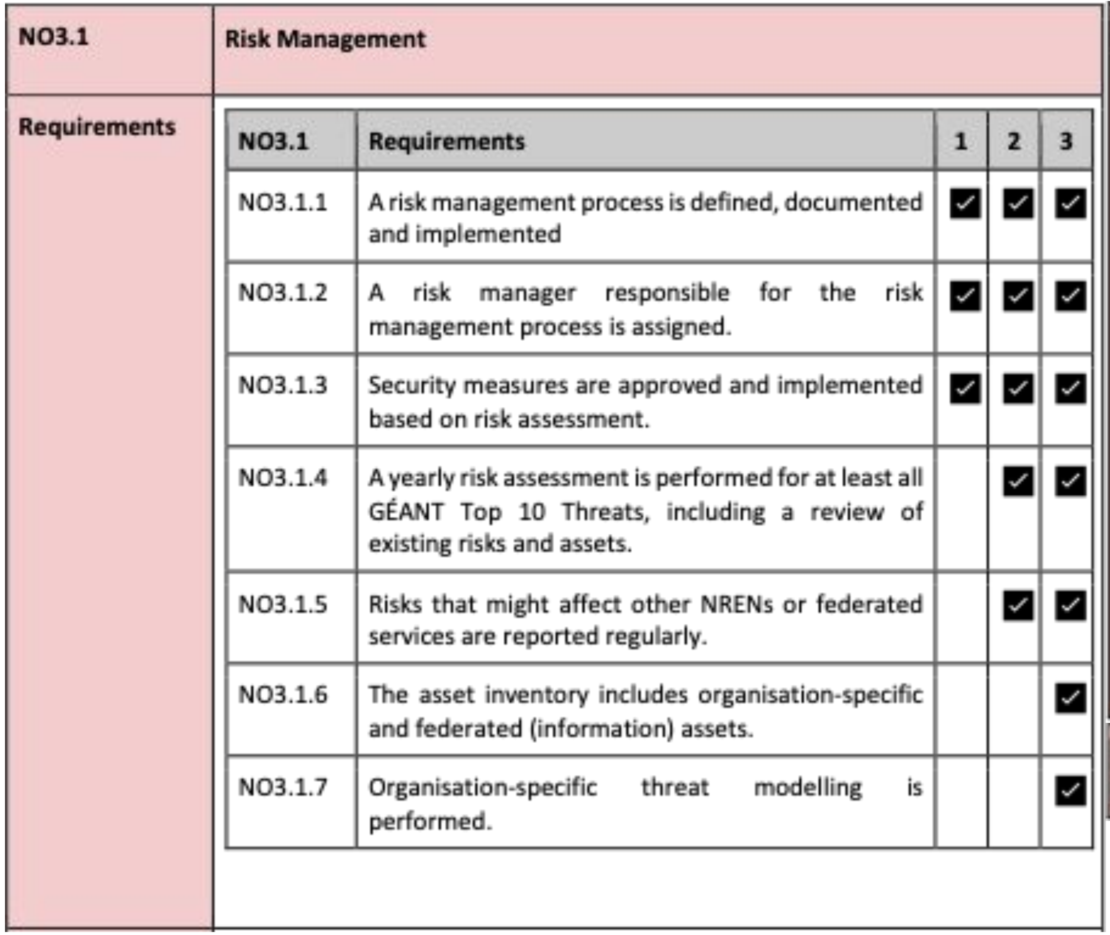
Solid security practices. A minor part of NRENS is already compliant, most implement just individual requirements.

Baseline

80% of NRENS

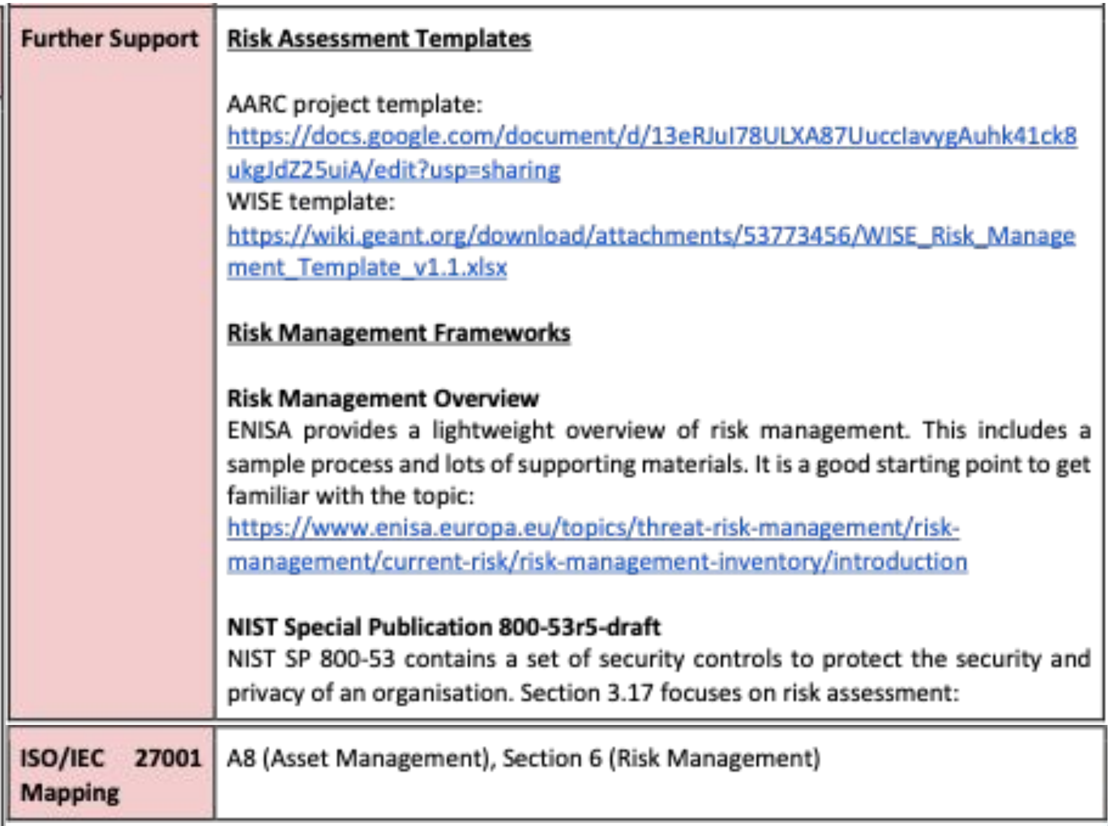
Entry level security. The majority of NRENS is already compliant.

Security Module Example



NO3.1	Risk Management
Requirements	

NO3.1	Requirements	1	2	3
NO3.1.1	A risk management process is defined, documented and implemented	☑	☑	☑
NO3.1.2	A risk manager responsible for the risk management process is assigned.	☑	☑	☑
NO3.1.3	Security measures are approved and implemented based on risk assessment.	☑	☑	☑
NO3.1.4	A yearly risk assessment is performed for at least all GÉANT Top 10 Threats, including a review of existing risks and assets.		☑	☑
NO3.1.5	Risks that might affect other NRENs or federated services are reported regularly.		☑	☑
NO3.1.6	The asset inventory includes organisation-specific and federated (information) assets.			☑
NO3.1.7	Organisation-specific threat modelling is performed.			☑



Further Support	**Risk Assessment Templates** AARC project template: https://docs.google.com/document/d/13eRJuI78ULXA87UucclavygAuhk41ck8ukgJdZ25uiA/edit?usp=sharing WISE template: https://wiki.geant.org/download/attachments/53773456/WISE_Risk_Management_Template_v1.1.xlsx **Risk Management Frameworks** **Risk Management Overview** ENISA provides a lightweight overview of risk management. This includes a sample process and lots of supporting materials. It is a good starting point to get familiar with the topic: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/introduction **NIST Special Publication 800-53r5-draft** NIST SP 800-53 contains a set of security controls to protect the security and privacy of an organisation. Section 3.17 focuses on risk assessment:
ISO/IEC 27001 Mapping	A8 (Asset Management), Section 6 (Risk Management)

Security from every angle

01 Policy

- Management Commitment and Mandate
- Internal Security Policy
- Acceptable Use Policy
- Regulatory and Privacy

02 People

- Training and Awareness
- Personnel Management
- Supplier Management

03 Threats

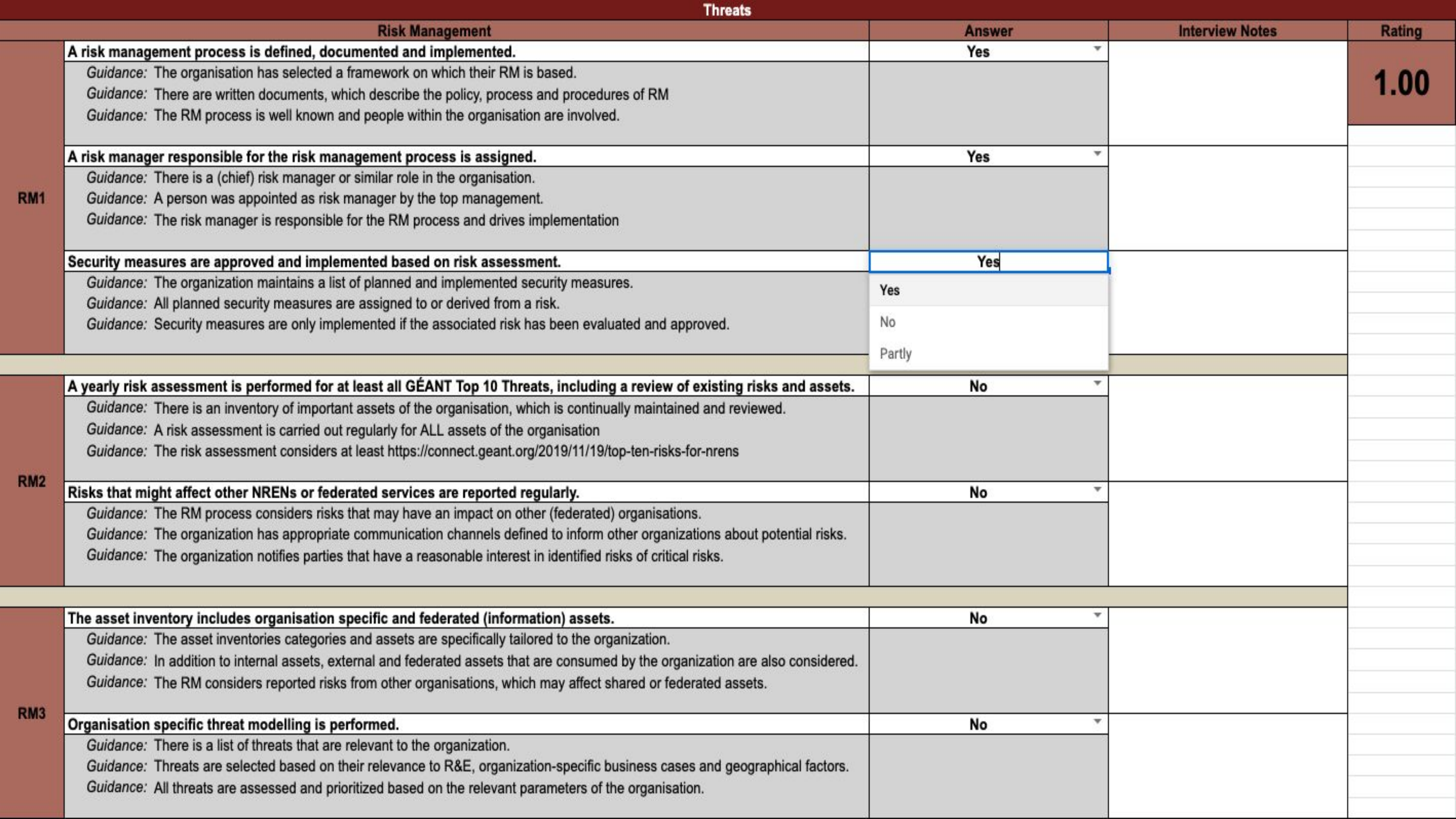
- Risk Management
- Incident Management
- Business Continuity Management

04 Operations

- Tools
- Cryptography
- Access Management
- Patch Management
- Vulnerability Management

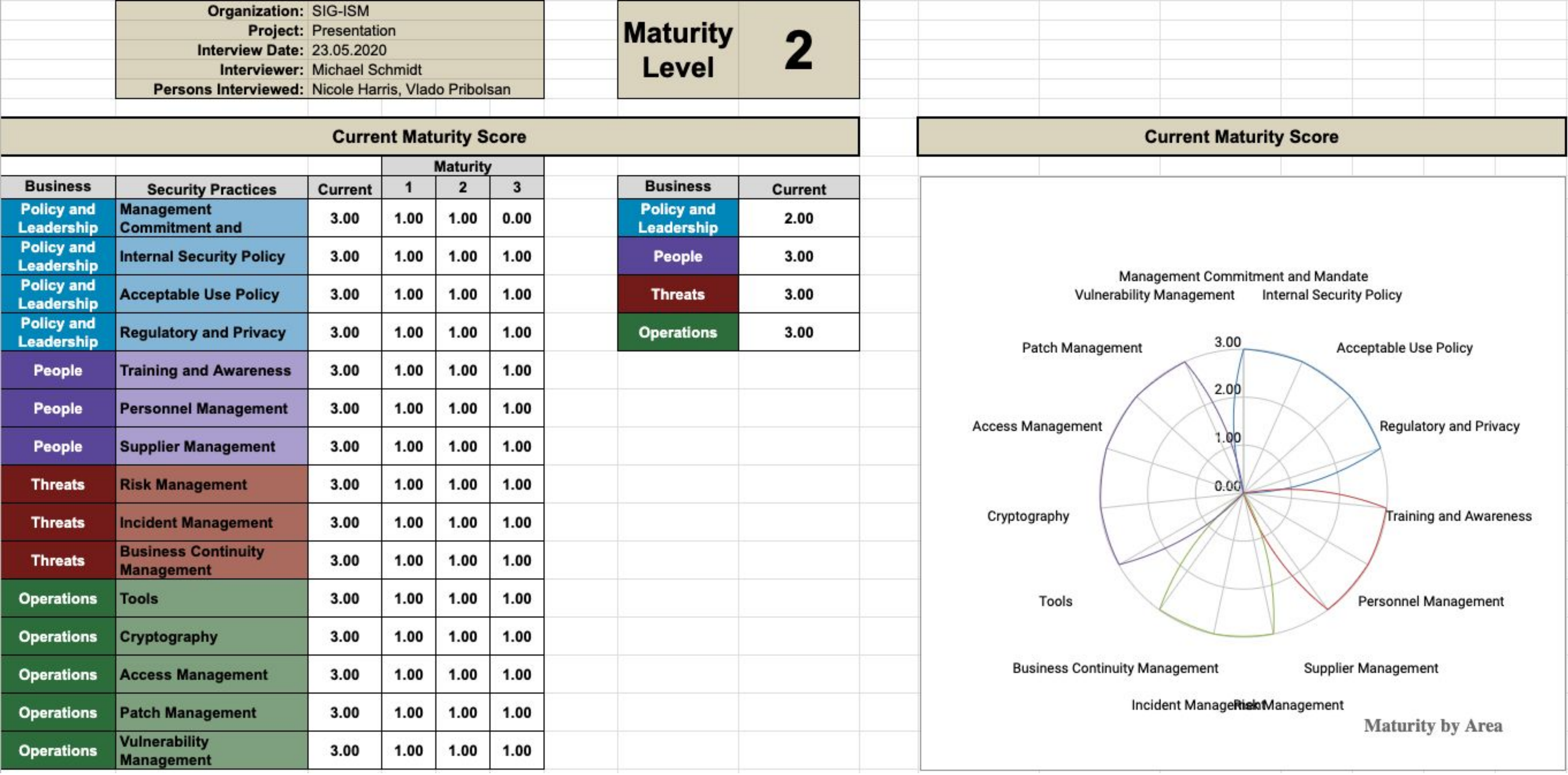
Assessment Sheet

- Support organizations to conduct a (self) assessment
- Helps to better understand the requirements of the security baseline
- Makes the maturity level and requirements fulfillment of an organisation visible
- Enables us to create statistics to identify the security level of our community



Threats

Risk Management		Answer	Interview Notes	Rating
RM1	**A risk management process is defined, documented and implemented.**	Yes		1.00
	Guidance: The organisation has selected a framework on which their RM is based. *Guidance:* There are written documents, which describe the policy, process and procedures of RM *Guidance:* The RM process is well known and people within the organisation are involved.			
	A risk manager responsible for the risk management process is assigned.	Yes		
	Guidance: There is a (chief) risk manager or similar role in the organisation. *Guidance:* A person was appointed as risk manager by the top management. *Guidance:* The risk manager is responsible for the RM process and drives implementation			
	Security measures are approved and implemented based on risk assessment.	Yes		
	Guidance: The organization maintains a list of planned and implemented security measures. *Guidance:* All planned security measures are assigned to or derived from a risk. *Guidance:* Security measures are only implemented if the associated risk has been evaluated and approved.			
RM2	**A yearly risk assessment is performed for at least all GÉANT Top 10 Threats, including a review of existing risks and assets.**	No		
	Guidance: There is an inventory of important assets of the organisation, which is continually maintained and reviewed. *Guidance:* A risk assessment is carried out regularly for ALL assets of the organisation *Guidance:* The risk assessment considers at least https://connect.geant.org/2019/11/19/top-ten-risks-for-nrens			
	Risks that might affect other NRENs or federated services are reported regularly.	No		
	Guidance: The RM process considers risks that may have an impact on other (federated) organisations. *Guidance:* The organization has appropriate communication channels defined to inform other organizations about potential risks. *Guidance:* The organization notifies parties that have a reasonable interest in identified risks of critical risks.			
RM3	**The asset inventory includes organisation specific and federated (information) assets.**	No		
	Guidance: The asset inventories categories and assets are specifically tailored to the organization. *Guidance:* In addition to internal assets, external and federated assets that are consumed by the organization are also considered. *Guidance:* The RM considers reported risks from other organisations, which may affect shared or federated assets.			
	Organisation specific threat modelling is performed.	No		
	Guidance: There is a list of threats that are relevant to the organization. *Guidance:* Threats are selected based on their relevance to R&E, organization-specific business cases and geographical factors. *Guidance:* All threats are assessed and prioritized based on the relevant parameters of the organisation.			



Organization:	SIG-ISM
Project:	Presentation
Interview Date:	23.05.2020
Interviewer:	Michael Schmidt
Persons Interviewed:	Nicole Harris, Vlado Pribolsan

Maturity Level **2**

Current Maturity Score

			Maturity		
Business	**Security Practices**	**Current**	**1**	**2**	**3**
Policy and Leadership	Management Commitment and	3.00	1.00	1.00	0.00
Policy and Leadership	Internal Security Policy	3.00	1.00	1.00	1.00
Policy and Leadership	Acceptable Use Policy	3.00	1.00	1.00	1.00
Policy and Leadership	Regulatory and Privacy	3.00	1.00	1.00	1.00
People	Training and Awareness	3.00	1.00	1.00	1.00
People	Personnel Management	3.00	1.00	1.00	1.00
People	Supplier Management	3.00	1.00	1.00	1.00
Threats	Risk Management	3.00	1.00	1.00	1.00
Threats	Incident Management	3.00	1.00	1.00	1.00
Threats	Business Continuity Management	3.00	1.00	1.00	1.00
Operations	Tools	3.00	1.00	1.00	1.00
Operations	Cryptography	3.00	1.00	1.00	1.00
Operations	Access Management	3.00	1.00	1.00	1.00
Operations	Patch Management	3.00	1.00	1.00	1.00
Operations	Vulnerability Management	3.00	1.00	1.00	1.00

Business	Current
Policy and Leadership	2.00
People	3.00
Threats	3.00
Operations	3.00

Current Maturity Score

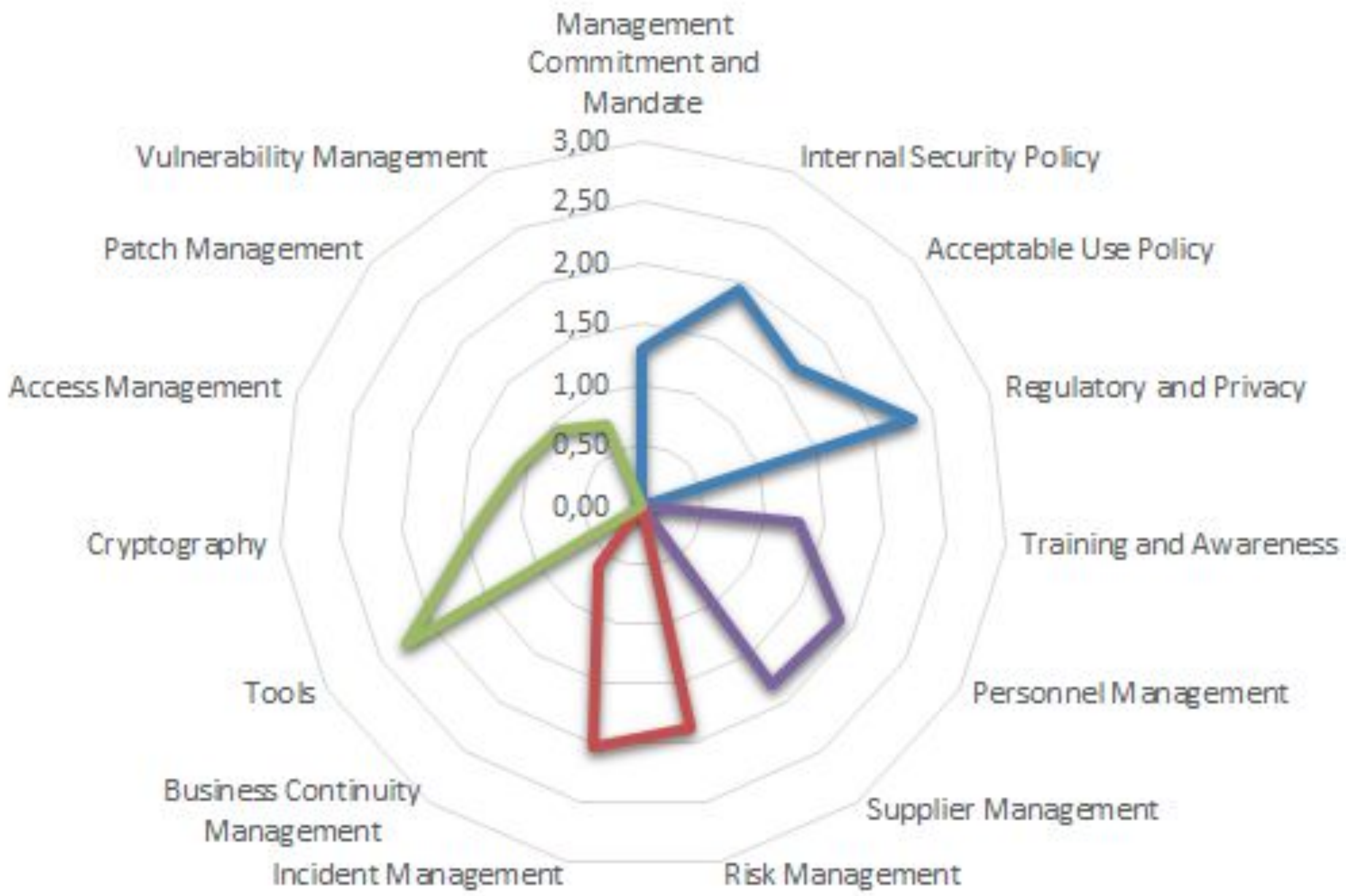
Maturity by Area

Lessons Learned

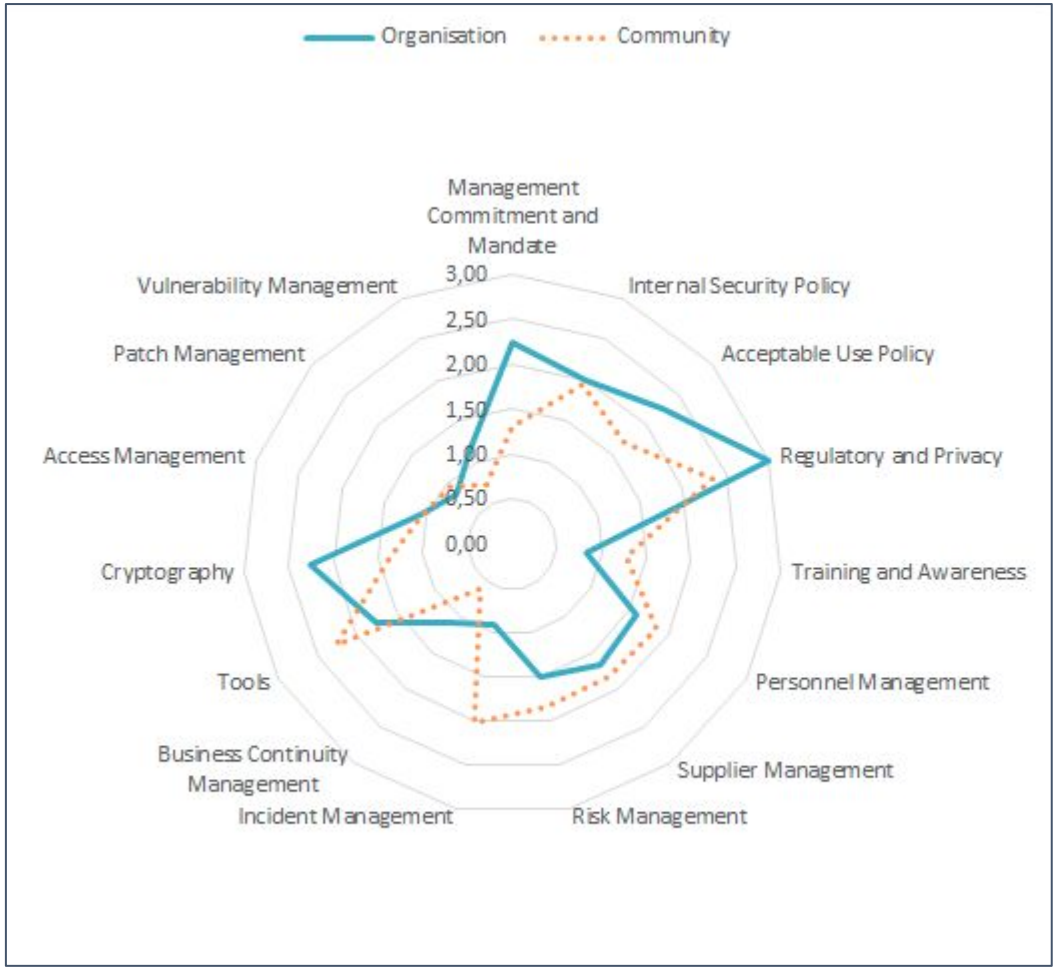
	✓	💡
Publications	● Security Baseline ● Security Assessment Sheet	● Received almost no feedback ● Feedback we did receive was positive
Presentations	● GÉANT Symposium February ● SIG-ISM April ● Cloud Security Workshop June	● Many of the planned presentations could not be held ● Little follow-up from these meetings
Assessment	● Self Assessment Pilot ● 3 Organisations	● Requirements are more difficult than expected ● Questions updated

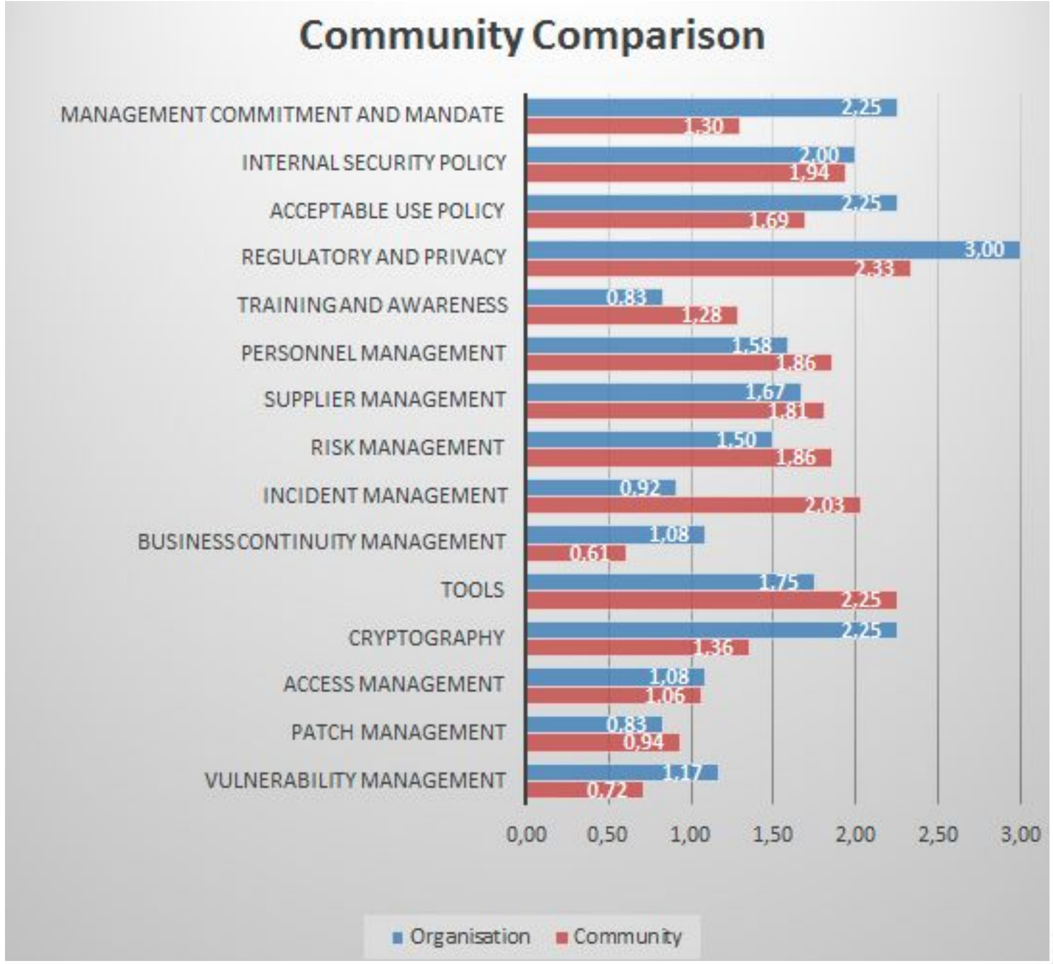
Community Average

Business Functions	Current
Policy and Leadership	1,82
People	1,65
Threats	1,50
Operations	1,27



Compare your Organisation





Questions 1

Have you heard of the Security Baseline before?

Questions 2

Did you use the Baseline or Assessment Sheet already?

Questions 3

Are you interested in being a pilot partner?

Questions 4

Which additional resources (guidelines, templates, examples) do you need to implement the Baseline?

Questions 5

Are there any other areas to be covered in the baseline?

Thank you

Any questions?

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 3 project (GN4-3).
The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Resources & References

- GÉANT Security Baseline
  https://wiki.geant.org/x/iDH5Bw

- Baseline Assessment Sheet
  https://wiki.geant.org/x/bwGMC