Analysing the EUCS requirements
Executive Summary

François DUTHILLEUL
Red Hat representative in Sylva WG03

EARLY DRAFT
FOR DISCUSSION

Red Hat

ABOUT THIS DECK

- Sylva WG03 analysed the EUCS requirements from the ENISA EUCS draft from December 2020 [1]
- Each EUCS requirement has been analysed to check whether it was related to the Sylva software stack or not
- For each relevant requirement, one (or more) Sylva feature was (were) identified
- During the F2F meeting, we agreed to release a blog post to share the main outcome of this analysis
- This deck is trying to summarise this outcome

[1] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

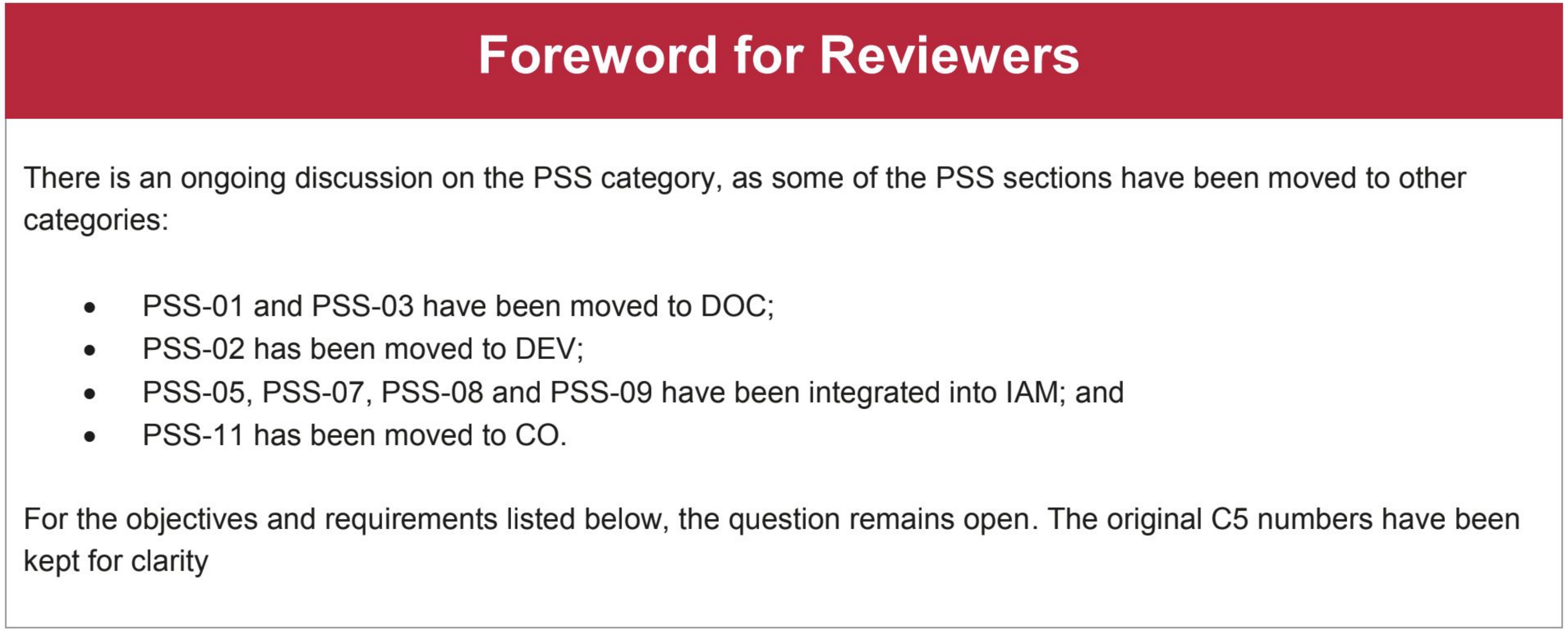
EXECUTIVE SUMMARY - OUTCOME BY THE NUMBERS

- **534 requirements reviewed**
- **109 requirements where one or more Sylva features identified**
  - 85 requirements with a single feature identified
  - 24 requirements with multiple features identified
- **61 features identified**
  - 39 unique features covering the 85 requirements
  - 43 unique features covering the 24 requirements
  - 21 common features

EUCS Requirements

EUCS REQUIREMENTS

- WG03 analysed also the category 20 even if there is a note that some of the PSS requirements have been moved to other categories
- We should decide if we report our analysis for 19 or 20 categories



Foreword for Reviewers

There is an ongoing discussion on the PSS category, as some of the PSS sections have been moved to other categories:

- PSS-01 and PSS-03 have been moved to DOC;
- PSS-02 has been moved to DEV;
- PSS-05, PSS-07, PSS-08 and PSS-09 have been integrated into IAM; and
- PSS-11 has been moved to CO.

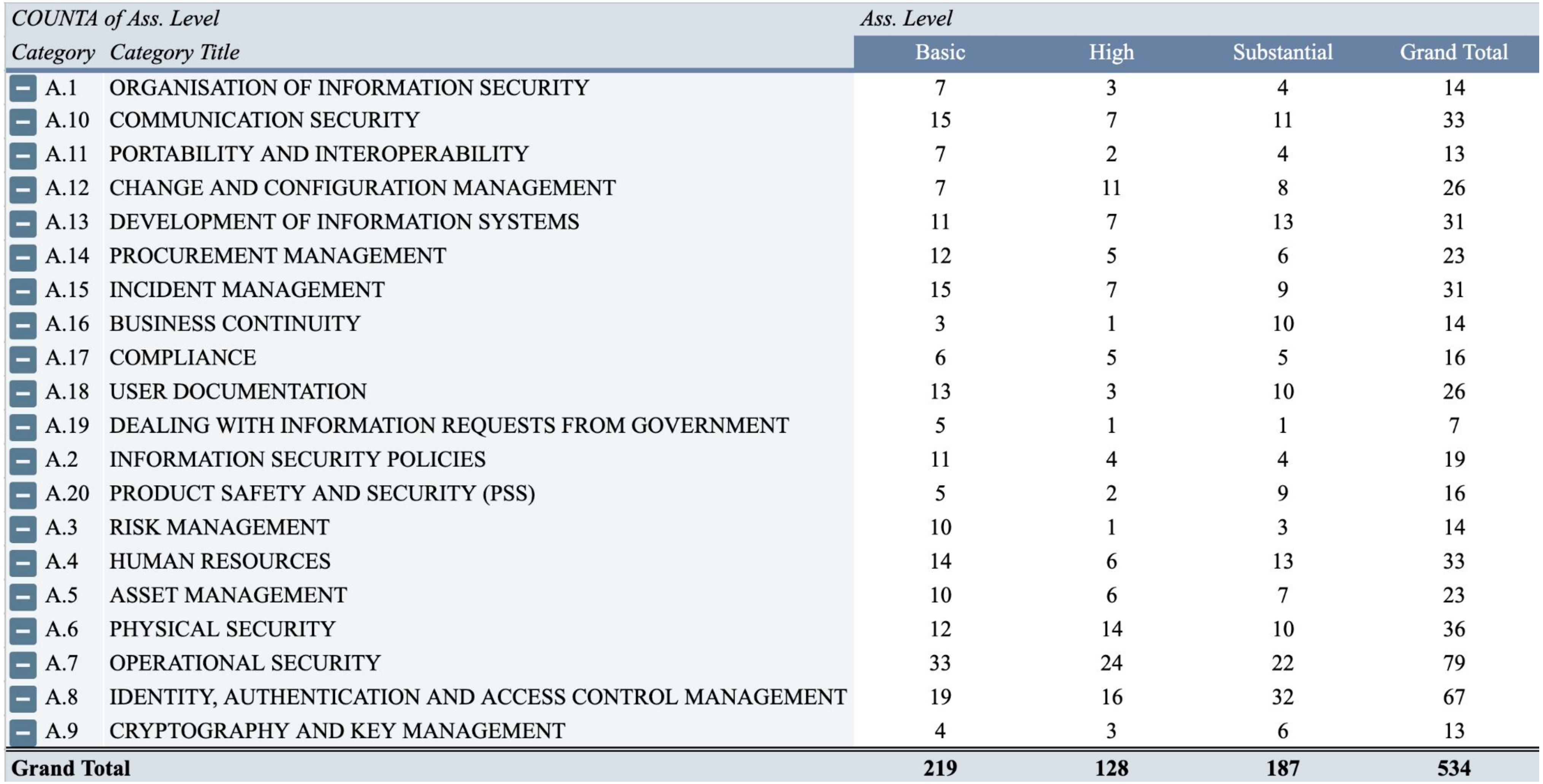
For the objectives and requirements listed below, the question remains open. The original C5 numbers have been kept for clarity

EUCS ASSURANCE LEVELS

- EUCS assurance levels are described on page 82

- Requirements labelled **Basic** apply to all assurance levels
- Requirements labelled **Substantial** apply to levels Substantial and High
- Requirements labelled **High** only apply to level High

EUCS CATEGORIES & EUCS REQUIREMENTS PER ASSURANCE LEVEL



COUNTA of Ass. Level		*Ass. Level*			
Category	*Category Title*	Basic	High	Substantial	Grand Total
⊟ A.1	ORGANISATION OF INFORMATION SECURITY	7	3	4	14
⊟ A.10	COMMUNICATION SECURITY	15	7	11	33
⊟ A.11	PORTABILITY AND INTEROPERABILITY	7	2	4	13
⊟ A.12	CHANGE AND CONFIGURATION MANAGEMENT	7	11	8	26
⊟ A.13	DEVELOPMENT OF INFORMATION SYSTEMS	11	7	13	31
⊟ A.14	PROCUREMENT MANAGEMENT	12	5	6	23
⊟ A.15	INCIDENT MANAGEMENT	15	7	9	31
⊟ A.16	BUSINESS CONTINUITY	3	1	10	14
⊟ A.17	COMPLIANCE	6	5	5	16
⊟ A.18	USER DOCUMENTATION	13	3	10	26
⊟ A.19	DEALING WITH INFORMATION REQUESTS FROM GOVERNMENT	5	1	1	7
⊟ A.2	INFORMATION SECURITY POLICIES	11	4	4	19
⊟ A.20	PRODUCT SAFETY AND SECURITY (PSS)	5	2	9	16
⊟ A.3	RISK MANAGEMENT	10	1	3	14
⊟ A.4	HUMAN RESOURCES	14	6	13	33
⊟ A.5	ASSET MANAGEMENT	10	6	7	23
⊟ A.6	PHYSICAL SECURITY	12	14	10	36
⊟ A.7	OPERATIONAL SECURITY	33	24	22	79
⊟ A.8	IDENTITY, AUTHENTICATION AND ACCESS CONTROL MANAGEMENT	19	16	32	67
⊟ A.9	CRYPTOGRAPHY AND KEY MANAGEMENT	4	3	6	13
Grand Total		**219**	**128**	**187**	**534**

EUCS REQUIREMENTS PER ASSURANCE LEVEL

20 CATEGORIES

Assurance Level	# Requirements	%	Cumulative Requirements	%
Basic	219	41%	219	41%
Substantial	128	24%	347	65%
High	187	35%	534	100%
Total	**534**	100%	N/A	N/A

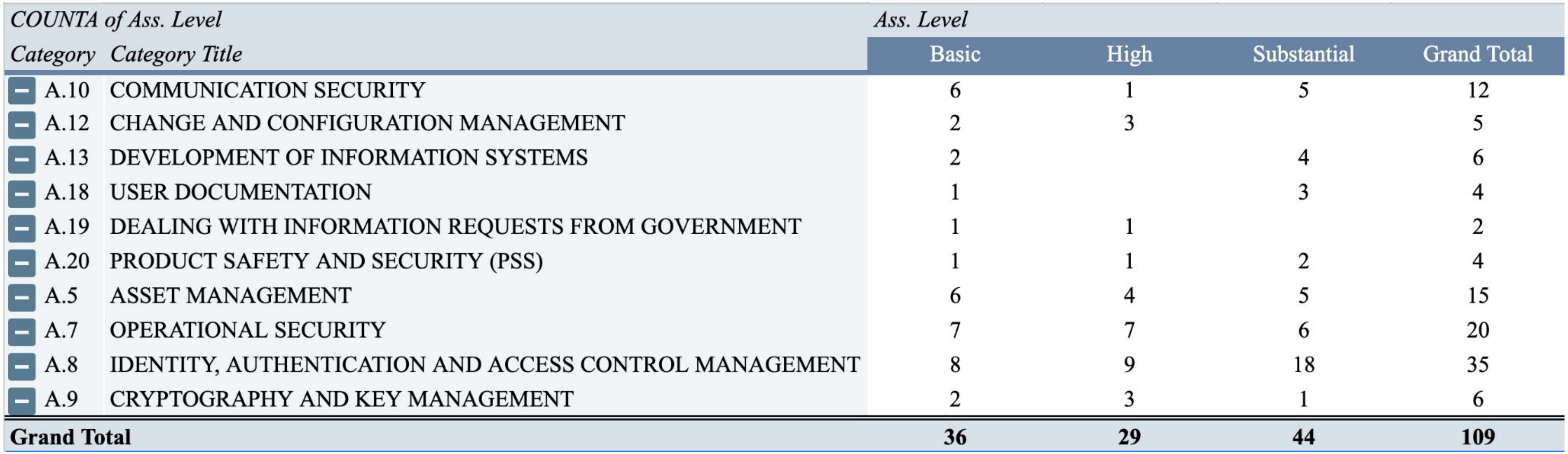
EUCS REQUIREMENTS PER ASSURANCE LEVEL

19 CATEGORIES

Assurance Level	# Requirements	%	Cumulative Requirements	%
Basic	214	41,3%	214	41,3%
Substantial	126	24,3%	340	65.6%
High	178	34,4%	518	100%
Total	**518**	100%	N/A	N/A

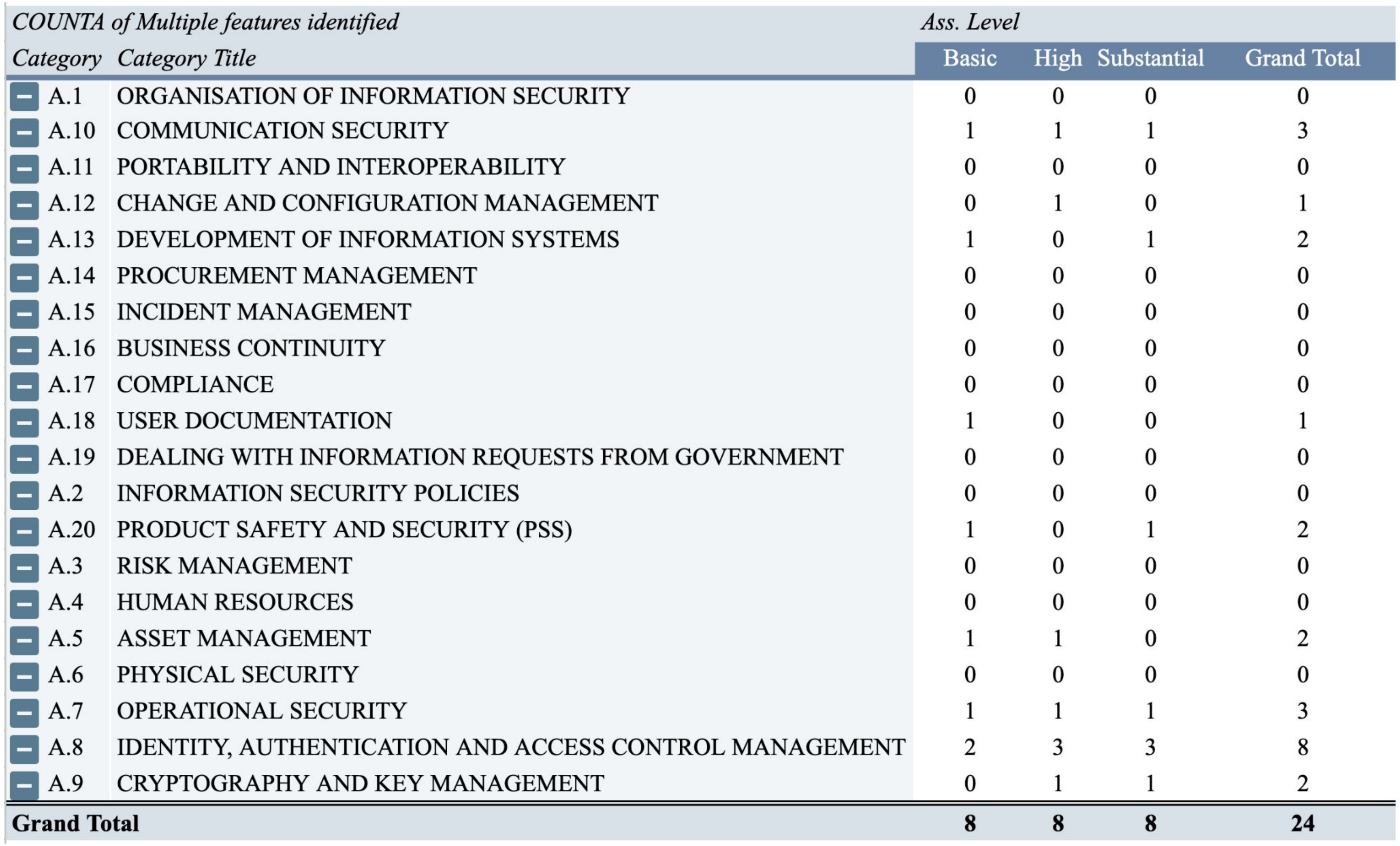
Sylva Features identified from EUCS Analysis

EUCS REQUIREMENTS WITH AT LEAST ONE SYLVA FEATURE WAS IDENTIFIED



COUNTA of Ass. Level		*Ass. Level*			
Category	*Category Title*	Basic	High	Substantial	Grand Total
A.10	COMMUNICATION SECURITY	6	1	5	12
A.12	CHANGE AND CONFIGURATION MANAGEMENT	2	3		5
A.13	DEVELOPMENT OF INFORMATION SYSTEMS	2		4	6
A.18	USER DOCUMENTATION	1		3	4
A.19	DEALING WITH INFORMATION REQUESTS FROM GOVERNMENT	1	1		2
A.20	PRODUCT SAFETY AND SECURITY (PSS)	1	1	2	4
A.5	ASSET MANAGEMENT	6	4	5	15
A.7	OPERATIONAL SECURITY	7	7	6	20
A.8	IDENTITY, AUTHENTICATION AND ACCESS CONTROL MANAGEMENT	8	9	18	35
A.9	CRYPTOGRAPHY AND KEY MANAGEMENT	2	3	1	6
Grand Total		**36**	**29**	**44**	**109**

EUCS REQUIREMENTS WITH MULTIPLE SYLVA FEATURES IDENTIFIED

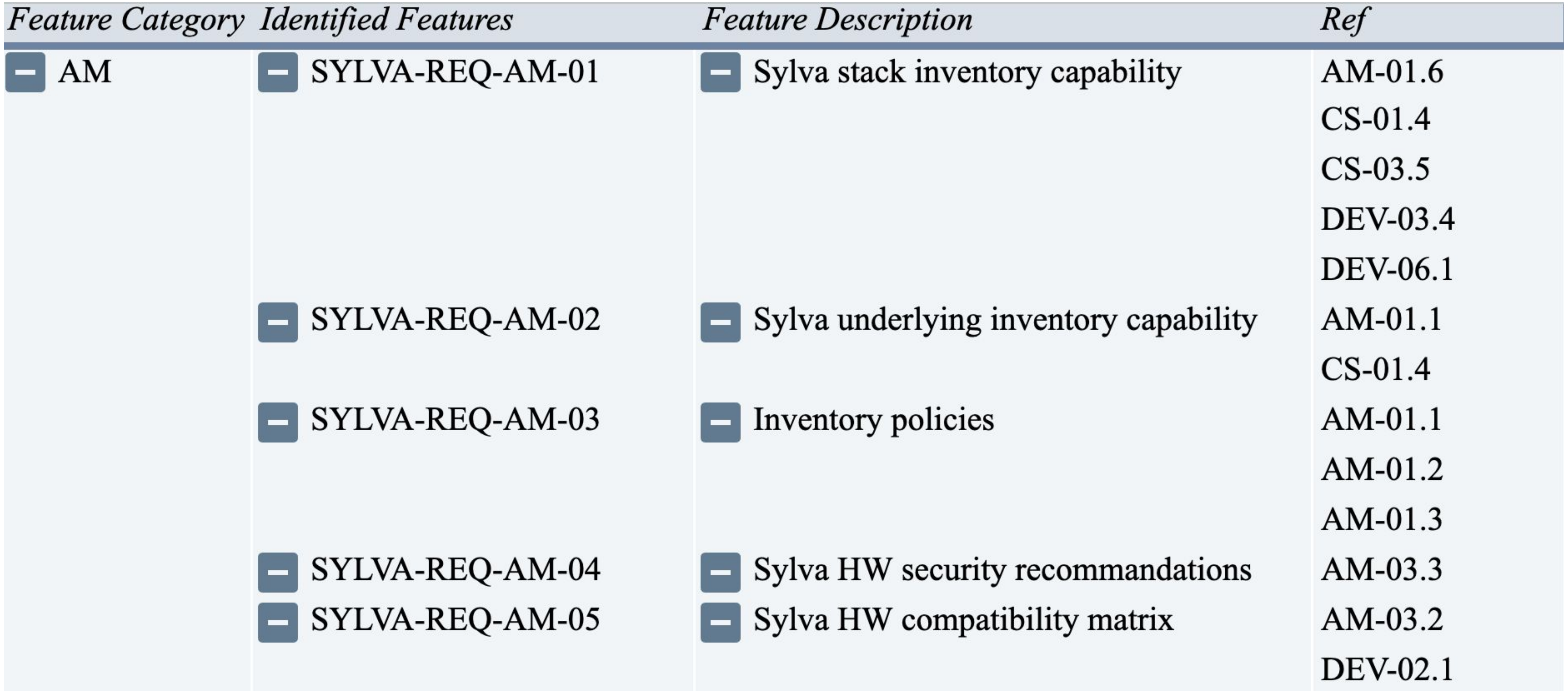


COUNTA of Multiple features identified		*Ass. Level*			
Category	*Category Title*	Basic	High	Substantial	Grand Total
⊟ A.1	ORGANISATION OF INFORMATION SECURITY	0	0	0	0
⊟ A.10	COMMUNICATION SECURITY	1	1	1	3
⊟ A.11	PORTABILITY AND INTEROPERABILITY	0	0	0	0
⊟ A.12	CHANGE AND CONFIGURATION MANAGEMENT	0	1	0	1
⊟ A.13	DEVELOPMENT OF INFORMATION SYSTEMS	1	0	1	2
⊟ A.14	PROCUREMENT MANAGEMENT	0	0	0	0
⊟ A.15	INCIDENT MANAGEMENT	0	0	0	0
⊟ A.16	BUSINESS CONTINUITY	0	0	0	0
⊟ A.17	COMPLIANCE	0	0	0	0
⊟ A.18	USER DOCUMENTATION	1	0	0	1
⊟ A.19	DEALING WITH INFORMATION REQUESTS FROM GOVERNMENT	0	0	0	0
⊟ A.2	INFORMATION SECURITY POLICIES	0	0	0	0
⊟ A.20	PRODUCT SAFETY AND SECURITY (PSS)	1	0	1	2
⊟ A.3	RISK MANAGEMENT	0	0	0	0
⊟ A.4	HUMAN RESOURCES	0	0	0	0
⊟ A.5	ASSET MANAGEMENT	1	1	0	2
⊟ A.6	PHYSICAL SECURITY	0	0	0	0
⊟ A.7	OPERATIONAL SECURITY	1	1	1	3
⊟ A.8	IDENTITY, AUTHENTICATION AND ACCESS CONTROL MANAGEMENT	2	3	3	8
⊟ A.9	CRYPTOGRAPHY AND KEY MANAGEMENT	0	1	1	2
Grand Total		**8**	**8**	**8**	**24**

EXECUTIVE SUMMARY - IDENTIFIED FEATURES

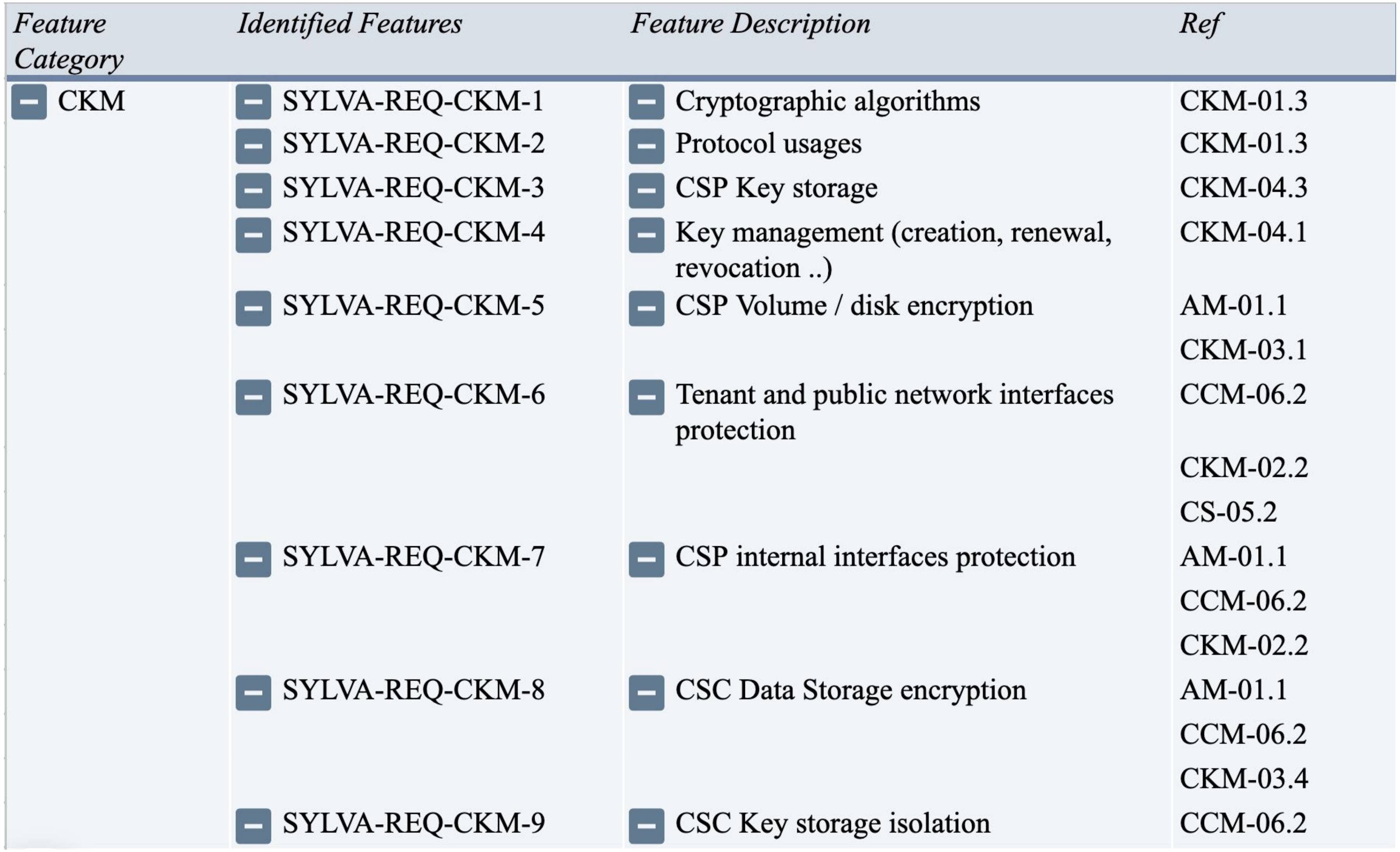
Feature Category	Feature Category Description	Amount of features identified	Amount of requirements covered by these features
AM	**Asset Management**	5	13
CKM	**Cryptography and Key Management**	9	16
DOC	**Documentation**	1	2
GEN	**Generic ?**	1	2
IAM	**Identity and Access Management**	13	47
OPS	**Operational Security**	30	73
SEG	**Segregation**	1	1
SIEM	**Security Information and Event Management**	1	3
	Total	**61**	**157**

AM - ASSET MANAGEMENT FEATURES



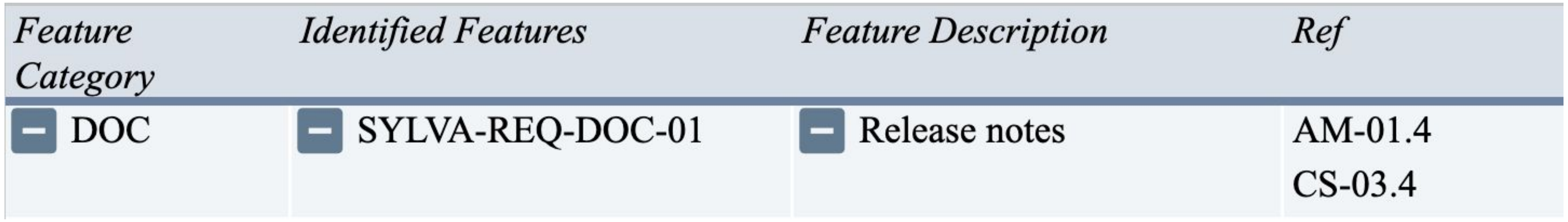
Feature Category	*Identified Features*	*Feature Description*	*Ref*
⊟ AM	⊟ SYLVA-REQ-AM-01	⊟ Sylva stack inventory capability	AM-01.6 CS-01.4 CS-03.5 DEV-03.4 DEV-06.1
	⊟ SYLVA-REQ-AM-02	⊟ Sylva underlying inventory capability	AM-01.1 CS-01.4
	⊟ SYLVA-REQ-AM-03	⊟ Inventory policies	AM-01.1 AM-01.2 AM-01.3
	⊟ SYLVA-REQ-AM-04	⊟ Sylva HW security recommandations	AM-03.3
	⊟ SYLVA-REQ-AM-05	⊟ Sylva HW compatibility matrix	AM-03.2 DEV-02.1

CKM – CRYPTO & KEY MANAGEMENT FEATURES



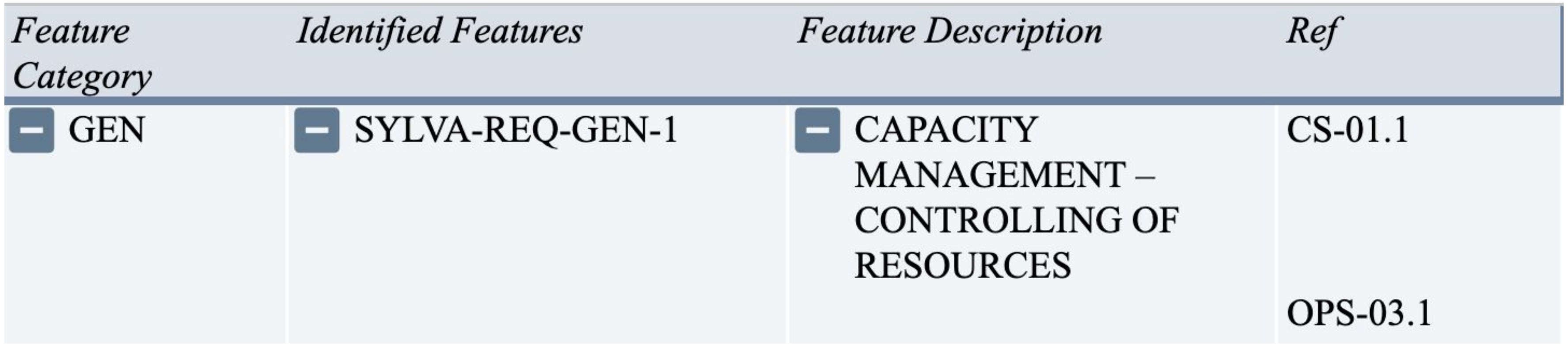
Feature Category	*Identified Features*	*Feature Description*	*Ref*
CKM	SYLVA-REQ-CKM-1	Cryptographic algorithms	CKM-01.3
	SYLVA-REQ-CKM-2	Protocol usages	CKM-01.3
	SYLVA-REQ-CKM-3	CSP Key storage	CKM-04.3
	SYLVA-REQ-CKM-4	Key management (creation, renewal, revocation ..)	CKM-04.1
	SYLVA-REQ-CKM-5	CSP Volume / disk encryption	AM-01.1 CKM-03.1
	SYLVA-REQ-CKM-6	Tenant and public network interfaces protection	CCM-06.2 CKM-02.2 CS-05.2
	SYLVA-REQ-CKM-7	CSP internal interfaces protection	AM-01.1 CCM-06.2 CKM-02.2
	SYLVA-REQ-CKM-8	CSC Data Storage encryption	AM-01.1 CCM-06.2 CKM-03.4
	SYLVA-REQ-CKM-9	CSC Key storage isolation	CCM-06.2

DOC – DOCUMENTATION FEATURES



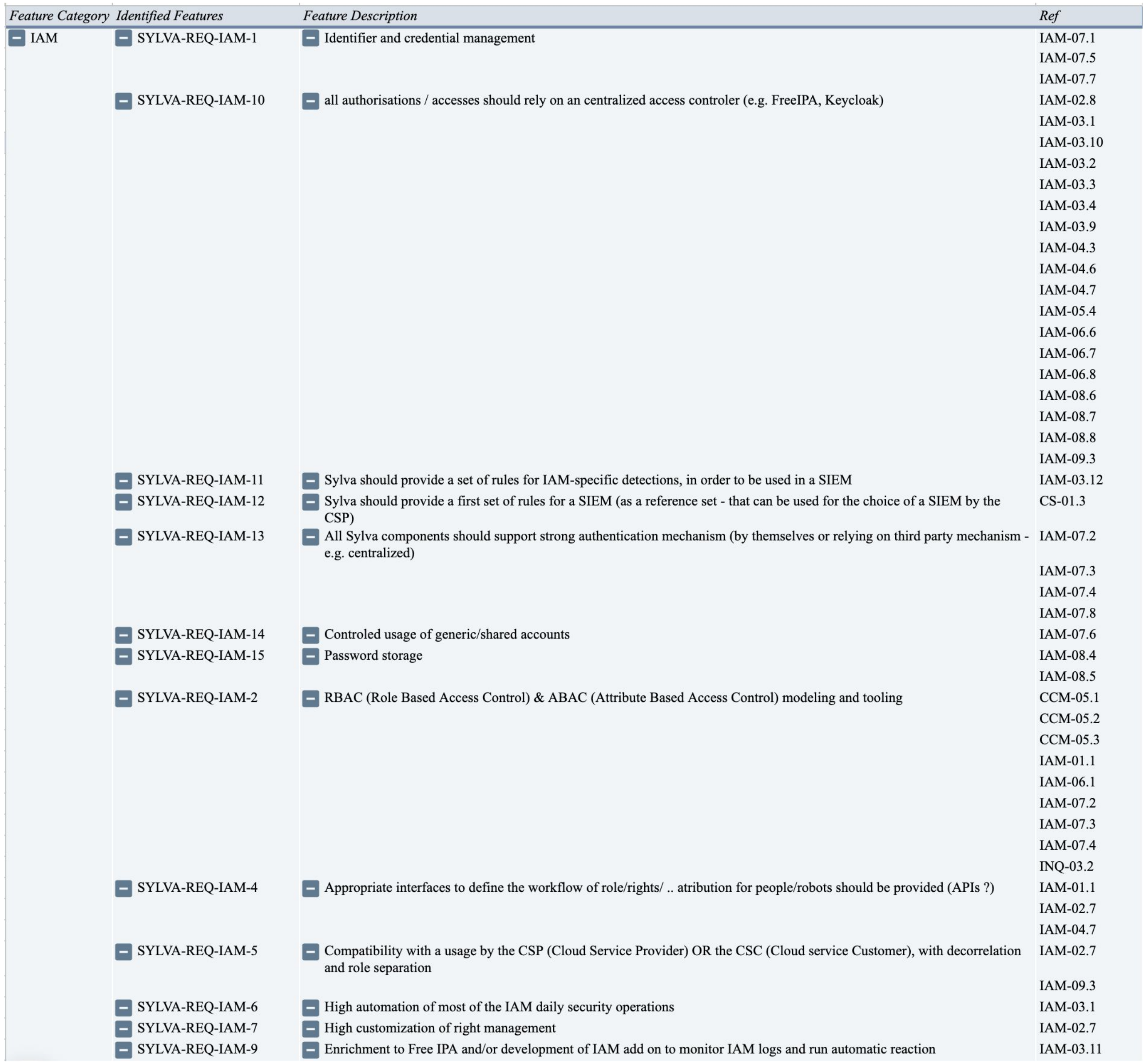
Feature Category	*Identified Features*	*Feature Description*	*Ref*
⊟ DOC	⊟ SYLVA-REQ-DOC-01	⊟ Release notes	AM-01.4 CS-03.4

GEN - GENERIC (?) FEATURES



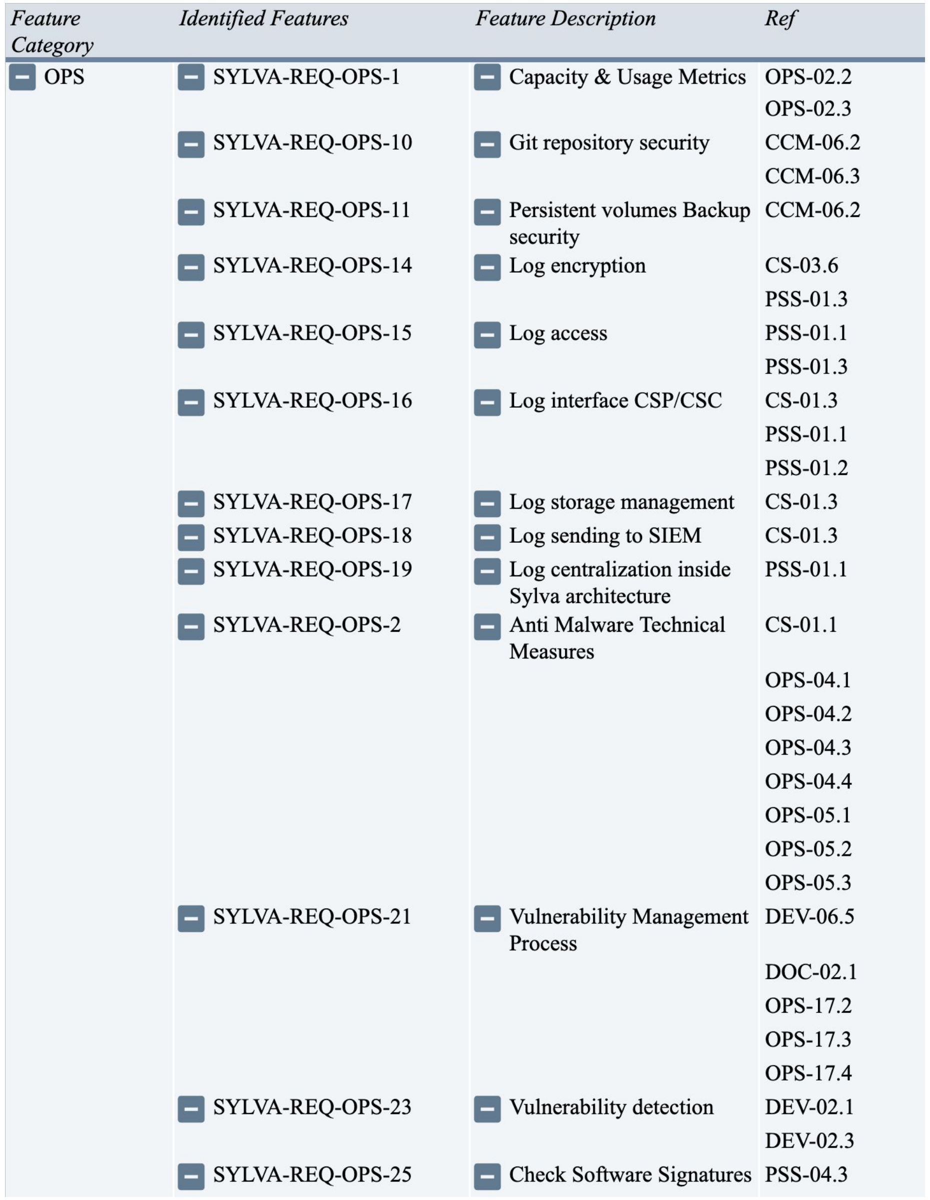
Feature Category	*Identified Features*	*Feature Description*	*Ref*
⊟ GEN	⊟ SYLVA-REQ-GEN-1	⊟ CAPACITY MANAGEMENT – CONTROLLING OF RESOURCES	CS-01.1 OPS-03.1

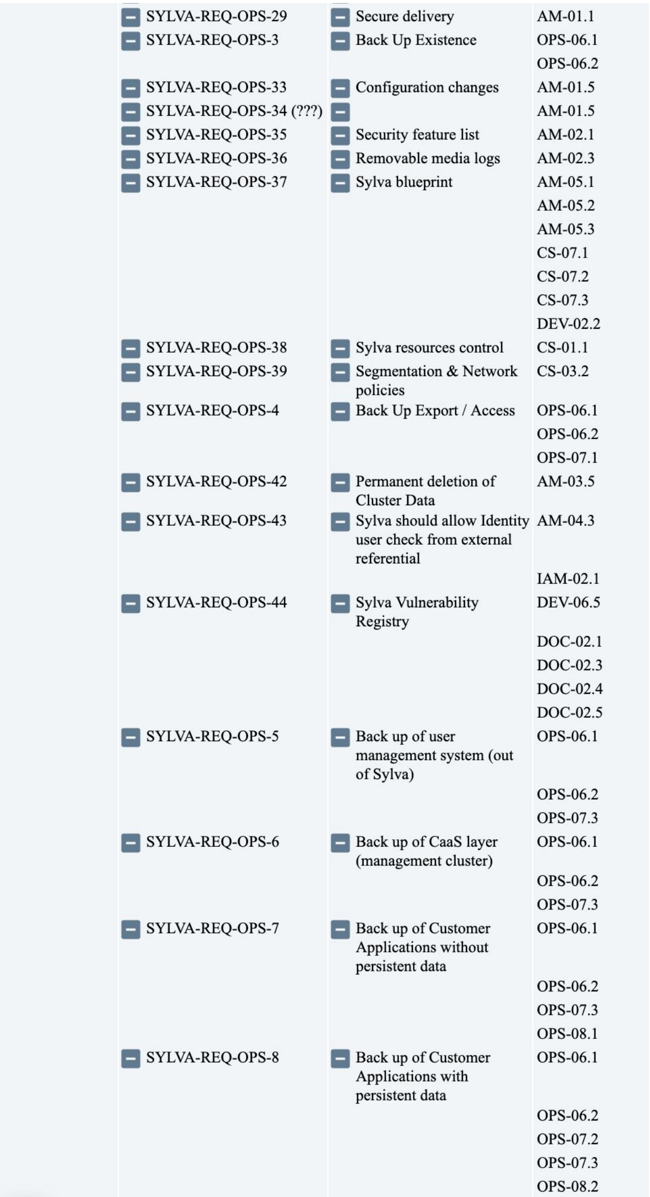
IAM – IDENTITY & ACCESS MANAGEMENT FEATURES



Feature Category	*Identified Features*	*Feature Description*	*Ref*
⊟ IAM	⊟ SYLVA-REQ-IAM-1	⊟ Identifier and credential management	IAM-07.1 IAM-07.5 IAM-07.7
	⊟ SYLVA-REQ-IAM-10	⊟ all authorisations / accesses should rely on an centralized access controler (e.g. FreeIPA, Keycloak)	IAM-02.8 IAM-03.1 IAM-03.10 IAM-03.2 IAM-03.3 IAM-03.4 IAM-03.9 IAM-04.3 IAM-04.6 IAM-04.7 IAM-05.4 IAM-06.6 IAM-06.7 IAM-06.8 IAM-08.6 IAM-08.7 IAM-08.8 IAM-09.3
	⊟ SYLVA-REQ-IAM-11	⊟ Sylva should provide a set of rules for IAM-specific detections, in order to be used in a SIEM	IAM-03.12
	⊟ SYLVA-REQ-IAM-12	⊟ Sylva should provide a first set of rules for a SIEM (as a reference set - that can be used for the choice of a SIEM by the CSP)	CS-01.3
	⊟ SYLVA-REQ-IAM-13	⊟ All Sylva components should support strong authentication mechanism (by themselves or relying on third party mechanism - e.g. centralized)	IAM-07.2 IAM-07.3 IAM-07.4 IAM-07.8
	⊟ SYLVA-REQ-IAM-14	⊟ Controled usage of generic/shared accounts	IAM-07.6
	⊟ SYLVA-REQ-IAM-15	⊟ Password storage	IAM-08.4 IAM-08.5
	⊟ SYLVA-REQ-IAM-2	⊟ RBAC (Role Based Access Control) & ABAC (Attribute Based Access Control) modeling and tooling	CCM-05.1 CCM-05.2 CCM-05.3 IAM-01.1 IAM-06.1 IAM-07.2 IAM-07.3 IAM-07.4 INQ-03.2
	⊟ SYLVA-REQ-IAM-4	⊟ Appropriate interfaces to define the workflow of role/rights/ .. atribution for people/robots should be provided (APIs ?)	IAM-01.1 IAM-02.7 IAM-04.7
	⊟ SYLVA-REQ-IAM-5	⊟ Compatibility with a usage by the CSP (Cloud Service Provider) OR the CSC (Cloud service Customer), with decorrelation and role separation	IAM-02.7 IAM-09.3
	⊟ SYLVA-REQ-IAM-6	⊟ High automation of most of the IAM daily security operations	IAM-03.1
	⊟ SYLVA-REQ-IAM-7	⊟ High customization of right management	IAM-02.7
	⊟ SYLVA-REQ-IAM-9	⊟ Enrichment to Free IPA and/or development of IAM add on to monitor IAM logs and run automatic reaction	IAM-03.11

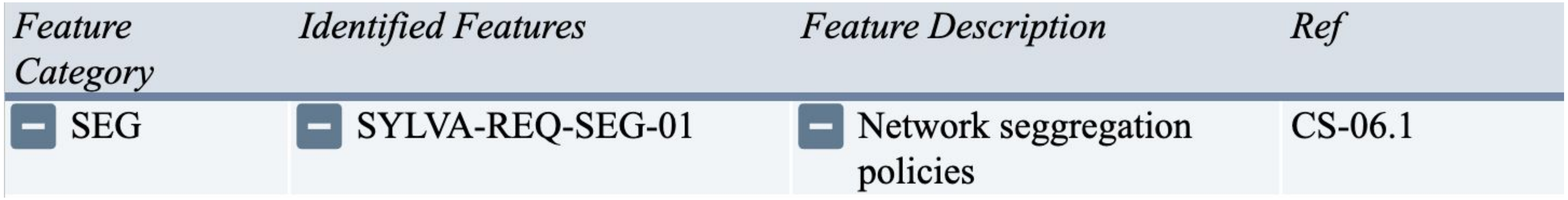
OPS – OPERATIONAL SECURITY FEATURES





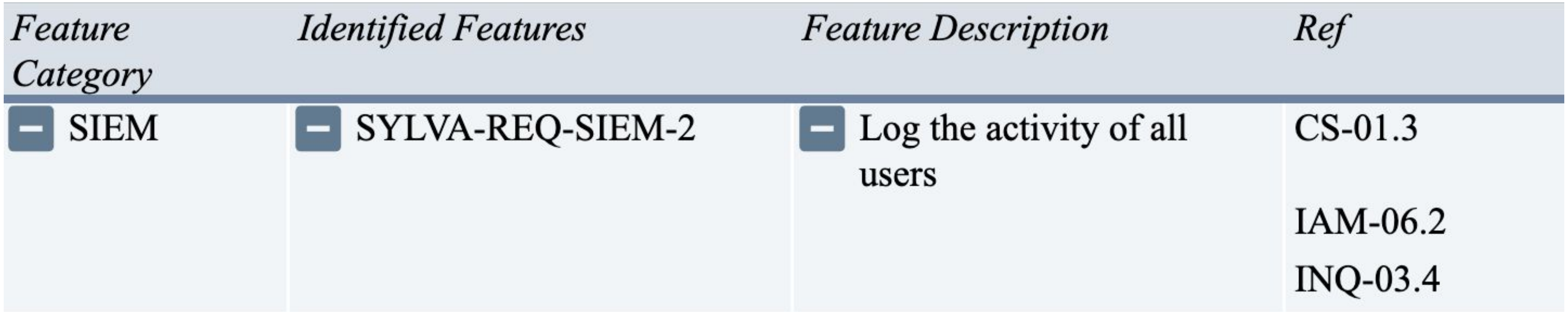
Feature Category	*Identified Features*	*Feature Description*	*Ref*
⊟ OPS	⊟ SYLVA-REQ-OPS-1	⊟ Capacity & Usage Metrics	OPS-02.2 OPS-02.3
	⊟ SYLVA-REQ-OPS-10	⊟ Git repository security	CCM-06.2 CCM-06.3
	⊟ SYLVA-REQ-OPS-11	⊟ Persistent volumes Backup security	CCM-06.2
	⊟ SYLVA-REQ-OPS-14	⊟ Log encryption	CS-03.6 PSS-01.3
	⊟ SYLVA-REQ-OPS-15	⊟ Log access	PSS-01.1 PSS-01.3
	⊟ SYLVA-REQ-OPS-16	⊟ Log interface CSP/CSC	CS-01.3 PSS-01.1 PSS-01.2
	⊟ SYLVA-REQ-OPS-17	⊟ Log storage management	CS-01.3
	⊟ SYLVA-REQ-OPS-18	⊟ Log sending to SIEM	CS-01.3
	⊟ SYLVA-REQ-OPS-19	⊟ Log centralization inside Sylva architecture	PSS-01.1
	⊟ SYLVA-REQ-OPS-2	⊟ Anti Malware Technical Measures	CS-01.1 OPS-04.1 OPS-04.2 OPS-04.3 OPS-04.4 OPS-05.1 OPS-05.2 OPS-05.3
	⊟ SYLVA-REQ-OPS-21	⊟ Vulnerability Management Process	DEV-06.5 DOC-02.1 OPS-17.2 OPS-17.3 OPS-17.4
	⊟ SYLVA-REQ-OPS-23	⊟ Vulnerability detection	DEV-02.1 DEV-02.3
	⊟ SYLVA-REQ-OPS-25	⊟ Check Software Signatures	PSS-04.3
	⊟ SYLVA-REQ-OPS-29	⊟ Secure delivery	AM-01.1
	⊟ SYLVA-REQ-OPS-3	⊟ Back Up Existence	OPS-06.1 OPS-06.2
	⊟ SYLVA-REQ-OPS-33	⊟ Configuration changes	AM-01.5
	⊟ SYLVA-REQ-OPS-34 (???)	⊟	AM-01.5
	⊟ SYLVA-REQ-OPS-35	⊟ Security feature list	AM-02.1
	⊟ SYLVA-REQ-OPS-36	⊟ Removable media logs	AM-02.3
	⊟ SYLVA-REQ-OPS-37	⊟ Sylva blueprint	AM-05.1 AM-05.2 AM-05.3 CS-07.1 CS-07.2 CS-07.3 DEV-02.2
	⊟ SYLVA-REQ-OPS-38	⊟ Sylva resources control	CS-01.1
	⊟ SYLVA-REQ-OPS-39	⊟ Segmentation & Network policies	CS-03.2
	⊟ SYLVA-REQ-OPS-4	⊟ Back Up Export / Access	OPS-06.1 OPS-06.2 OPS-07.1
	⊟ SYLVA-REQ-OPS-42	⊟ Permanent deletion of Cluster Data	AM-03.5
	⊟ SYLVA-REQ-OPS-43	⊟ Sylva should allow Identity user check from external referential	AM-04.3 IAM-02.1
	⊟ SYLVA-REQ-OPS-44	⊟ Sylva Vulnerability Registry	DEV-06.5 DOC-02.1 DOC-02.3 DOC-02.4 DOC-02.5
	⊟ SYLVA-REQ-OPS-5	⊟ Back up of user management system (out of Sylva)	OPS-06.1 OPS-06.2 OPS-07.3
	⊟ SYLVA-REQ-OPS-6	⊟ Back up of CaaS layer (management cluster)	OPS-06.1 OPS-06.2 OPS-07.3
	⊟ SYLVA-REQ-OPS-7	⊟ Back up of Customer Applications without persistent data	OPS-06.1 OPS-06.2 OPS-07.3 OPS-08.1
	⊟ SYLVA-REQ-OPS-8	⊟ Back up of Customer Applications with persistent data	OPS-06.1 OPS-06.2 OPS-07.2 OPS-07.3 OPS-08.2

SEG - SEGREGATION FEATURES



Feature Category	*Identified Features*	*Feature Description*	*Ref*
⊟ SEG	⊟ SYLVA-REQ-SEG-01	⊟ Network seggregation policies	CS-06.1

SIEM – SECURITY INFORMATION AND EVENT MANAGEMENT FEATURES

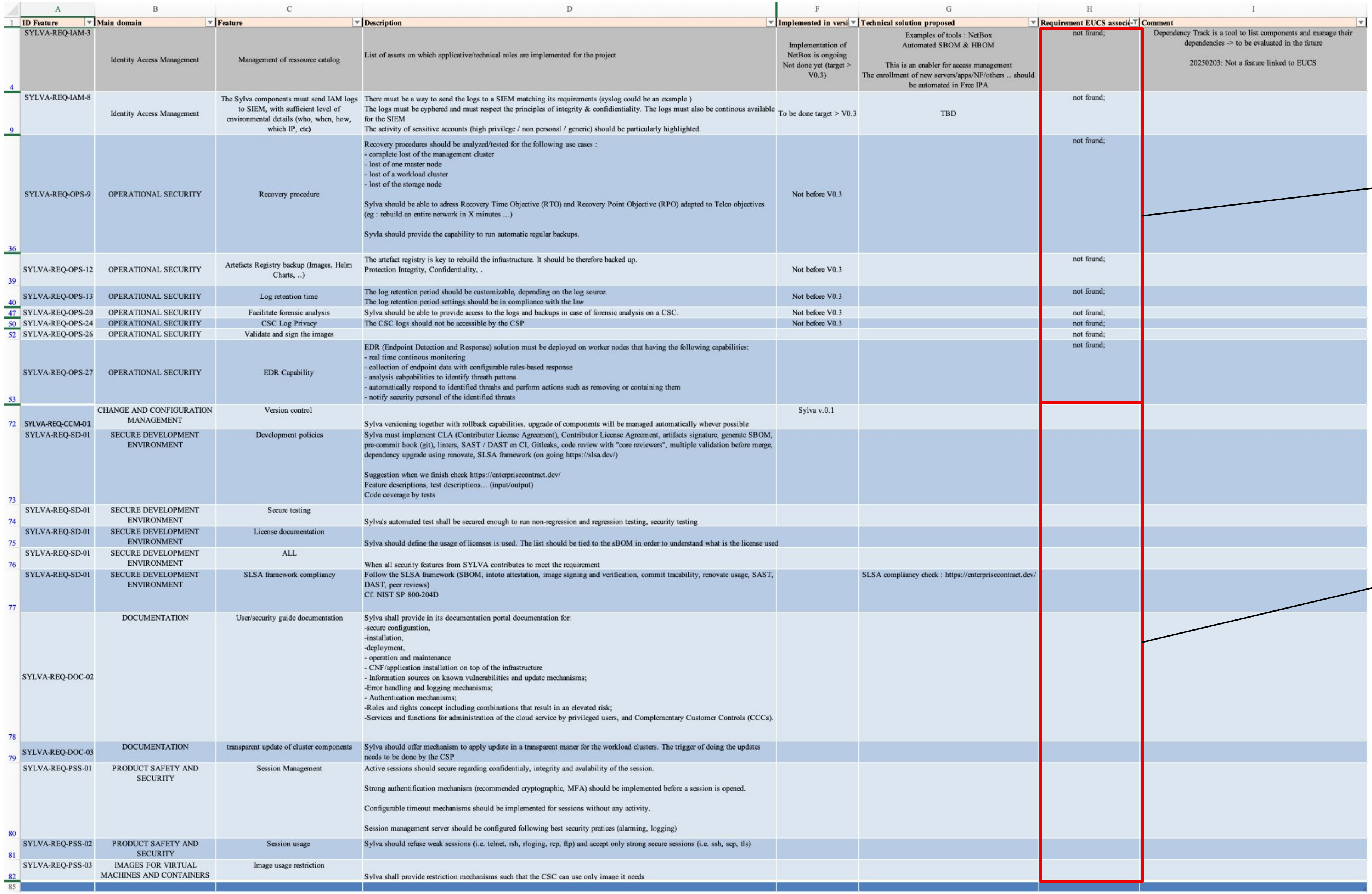


Feature Category	*Identified Features*	*Feature Description*	*Ref*
− SIEM	− SYLVA-REQ-SIEM-2	− Log the activity of all users	CS-01.3 IAM-06.2 INQ-03.4

FEEDBACK RELATED TO FEATURE ANALYSIS

- Not consistent feature naming e.g. -01 and -1
- Some features are not found or mapped to a requirement

SOME FEATURES ARE NOT FOUND OR MAPPED TO ANY EUCS REQUIREMENT



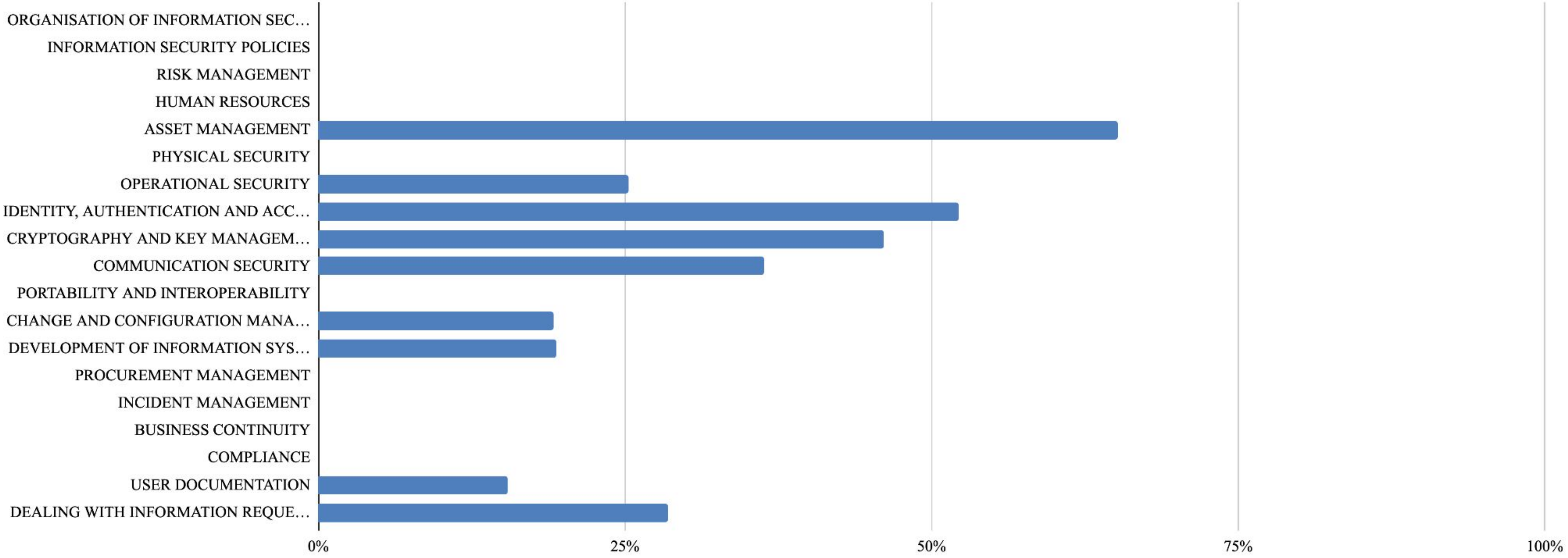
	A	B	C	D	F	G	H	I
1	ID Feature	Main domain	Feature	Description	Implemented in versi	Technical solution proposed	Requirement EUCS associ	Comment
4	SYLVA-REQ-IAM-3	Identity Access Management	Management of ressource catalog	List of assets on which applicative/technical roles are implemented for the project	Implementation of NetBox is ongoing Not done yet (target > V0.3)	Examples of tools : NetBox Automated SBOM & HBOM This is an enabler for access management The enrollment of new servers/apps/NF/others .. should be automated in Free IPA	not found;	Dependency Track is a tool to list components and manage their dependencies -> to be evaluated in the future 20250203: Not a feature linked to EUCS
9	SYLVA-REQ-IAM-8	Identity Access Management	The Sylva components must send IAM logs to SIEM, with sufficient level of environmental details (who, when, how, which IP, etc)	There must be a way to send the logs to a SIEM matching its requirements (syslog could be an example) The logs must be cyphered and must respect the principles of integrity & confidientiality. The logs must also be continous available for the SIEM The activity of sensitive accounts (high privilege / non personal / generic) should be particularly highlighted.	To be done target > V0.3	TBD	not found;	
36	SYLVA-REQ-OPS-9	OPERATIONAL SECURITY	Recovery procedure	Recovery procedures should be analyzed/tested for the following use cases : - complete lost of the management cluster - lost of one master node - lost of a workload cluster - lost of the storage node Sylva should be able to adress Recovery Time Objective (RTO) and Recovery Point Objective (RPO) adapted to Telco objectives (eg : rebuild an entire network in X minutes ...) Syvla should provide the capability to run automatic regular backups.	Not before V0.3		not found;	
39	SYLVA-REQ-OPS-12	OPERATIONAL SECURITY	Artefacts Registry backup (Images, Helm Charts, ..)	The artefact registry is key to rebuild the infrastructure. It should be therefore backed up. Protection Integrity, Confidentiality, .	Not before V0.3		not found;	
40	SYLVA-REQ-OPS-13	OPERATIONAL SECURITY	Log retention time	The log retention period should be customizable, depending on the log source. The log retention period settings should be in compliance with the law	Not before V0.3		not found;	
47	SYLVA-REQ-OPS-20	OPERATIONAL SECURITY	Facilitate forensic analysis	Sylva should be able to provide access to the logs and backups in case of forensic analysis on a CSC.	Not before V0.3		not found;	
50	SYLVA-REQ-OPS-24	OPERATIONAL SECURITY	CSC Log Privacy	The CSC logs should not be accessible by the CSP	Not before V0.3		not found;	
52	SYLVA-REQ-OPS-26	OPERATIONAL SECURITY	Validate and sign the images				not found;	
53	SYLVA-REQ-OPS-27	OPERATIONAL SECURITY	EDR Capability	EDR (Endpoint Detection and Response) solution must be deployed on worker nodes that having the following capabilities: - real time continous monitoring - collection of endpoint data with configurable rules-based response - analysis cabpabilities to identify threath pattens - automatically respond to identified threahs and perform actions such as removing or containing them - notify security personel of the identified threats			not found;	
72	SYLVA-REQ-CCM-01	CHANGE AND CONFIGURATION MANAGEMENT	Version control	Sylva versioning together with rollback capabilities, upgrade of components will be managed automatically whever possible	Sylva v.0.1			
73	SYLVA-REQ-SD-01	SECURE DEVELOPMENT ENVIRONMENT	Development policies	Sylva must implement CLA (Contributor License Agreement), Contributor License Agreement, artifacts signature, generate SBOM, pre-commit hook (git), linters, SAST / DAST en CI, Gitleaks, code review with "core reviewers", multiple validation before merge, dependency upgrade using renovate, SLSA framework (on going https://slsa.dev/) Suggestion when we finish check https://enterprisecontract.dev/ Feature descriptions, test descriptions... (input/output) Code coverage by tests				
74	SYLVA-REQ-SD-01	SECURE DEVELOPMENT ENVIRONMENT	Secure testing	Sylva's automated test shall be secured enough to run non-regression and regression testing, security testing				
75	SYLVA-REQ-SD-01	SECURE DEVELOPMENT ENVIRONMENT	License documentation	Sylva should define the usage of licenses is used. The list should be tied to the sBOM in order to understand what is the license used				
76	SYLVA-REQ-SD-01	SECURE DEVELOPMENT ENVIRONMENT	ALL	When all security features from SYLVA contributes to meet the requirement				
77	SYLVA-REQ-SD-01	SECURE DEVELOPMENT ENVIRONMENT	SLSA framework compliancy	Follow the SLSA framework (SBOM, intoto attestation, image signing and verification, commit tracability, renovate usage, SAST, DAST, peer reviews) Cf. NIST SP 800-204D		SLSA compliancy check : https://enterprisecontract.dev/		
78	SYLVA-REQ-DOC-02	DOCUMENTATION	User/security guide documentation	Sylva shall provide in its documentation portal documentation for: -secure configuration, -installation, -deployment, - operation and maintenance - CNF/application installation on top of the infrastructure - Information sources on known vulnerabilities and update mechanisms; -Error handling and logging mechanisms; - Authentication mechanisms; -Roles and rights concept including combinations that result in an elevated risk; -Services and functions for administration of the cloud service by privileged users, and Complementary Customer Controls (CCCs).				
79	SYLVA-REQ-DOC-03	DOCUMENTATION	transparent update of cluster components	Sylva should offer mechanism to apply update in a transparent maner for the workload clusters. The trigger of doing the updates needs to be done by the CSP				
80	SYLVA-REQ-PSS-01	PRODUCT SAFETY AND SECURITY	Session Management	Active sessions should secure regarding confidentialy, integrity and avalability of the session. Strong authentification mechanism (recommended cryptographic, MFA) should be implemented before a session is opened. Configurable timeout mechanisms should be implemented for sessions without any activity. Session management server should be configured following best security pratices (alarming, logging)				
81	SYLVA-REQ-PSS-02	PRODUCT SAFETY AND SECURITY	Session usage	Sylva should refuse weak sessions (i.e. telnet, rsh, rloging, rcp, ftp) and accept only strong secure sessions (i.e. ssh, scp, tls)				
82	SYLVA-REQ-PSS-03	IMAGES FOR VIRTUAL MACHINES AND CONTAINERS	Image usage restriction	Sylva shall provide restriction mechanisms such that the CSC can use only image it needs				
85								

NOT FOUND

NOT MAPPED

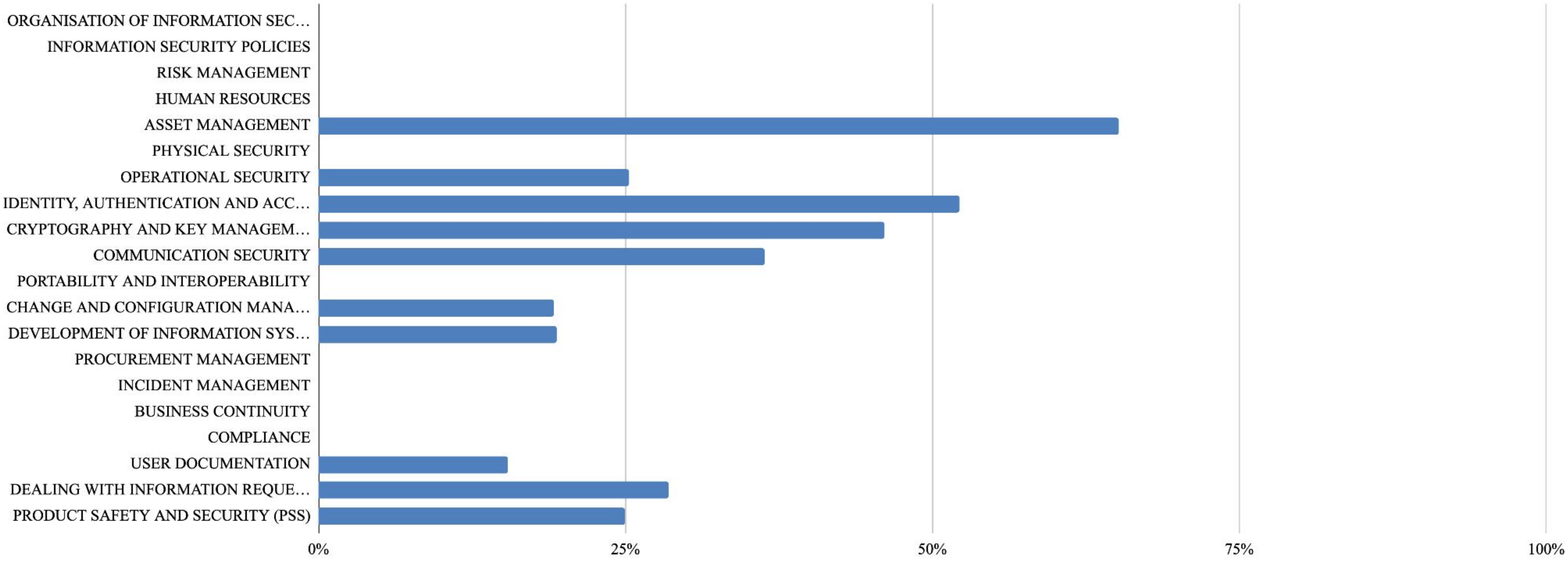
Percentage of requirements per category for which at least one Sylva feature has been identified

19 CATEGORIES



Percentage of requirements per category for which at least one Sylva feature has been identified

20 CATEGORIES



Red Hat

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

- linkedin.com/company/red-hat
- youtube.com/user/RedHatVideos
- facebook.com/redhatinc
- twitter.com/RedHat

Red Hat