

DESIGNING A CYBER-SECURE INFRASTRUCTURE FOR BELGIAN SMES

A MODULAR APPROACH ALIGNED WITH THE CYFUN
FRAMEWORK, WITH FOCUS ON THE ACCOUNTING SECTOR

OVERVIEW

01 Introduction

02 Problem Statement

03 Research Methods

04 Implementation

05 Result & Discussion

06 Conclusion

INTRODUCTION

- **Context** : Belgian SMEs, especially accounting firms, face increasing cybersecurity challenges.
- **Sector Motivation** : Accounting firms often lack time, staff, and resources to manage secure IT infrastructures and rely on digital workflows.
- **Framework Alignment** : The Belgian Cybersecurity Centre (CCB) introduced **CyFun**, a national framework with a Basic level designed to be accessible to all organizations.
- **Research Question** : Can we create a plug-and-play infrastructure that enables SMEs to meet baseline cybersecurity requirements with limited resources ?

PROBLEM STATEMENT

Limited financial and human resources

SMEs often lack the budget and internal staff to manage IT infrastructure.

01

02

Complexity of Security Frameworks

Frameworks like ISO 27001 or NIST CSF are too complex and rigid for SMEs to adopt without expert support.

Low Regulatory Awareness

Many small firms are not even aware of what regulations apply to them or how to become compliant

03

04

Lack of simple and automated solutions

Existing tools are rarely tailored to SME needs, they are often too technical, expensive.

Research Gap Identified

- Lack of ready-to-use, compliance-ready, and modular infrastructure solutions specifically designed for SMEs.
- No existing work applies the CyFun framework in a technical implementation for Belgian SMEs.

Approach : Identify real-world needs of small accounting firms to build a secure and compliant infrastructure aligned with CyFun via automation, reproducibility, and compliance artifacts.

- **1. Qualitative Needs Assessment :**
 - Interviews with 5 accounting SMEs
 - Identify gaps in compliance, awareness, and documentation
 - Define a Generic Profile
- **2. Technical Implementation :**
 - Adaptation of the JANUS infrastructure
 - Implementation of all sub-functions of CyFun Identify level Basic
 - Generation of compliance-ready artifacts and checklists

Goal : Deliver a modular, easy-to-use infrastructure that enables SMEs to reach CyFun compliance without requiring technical expertise.

QUALITATIVE NEEDS ASSESSMENT

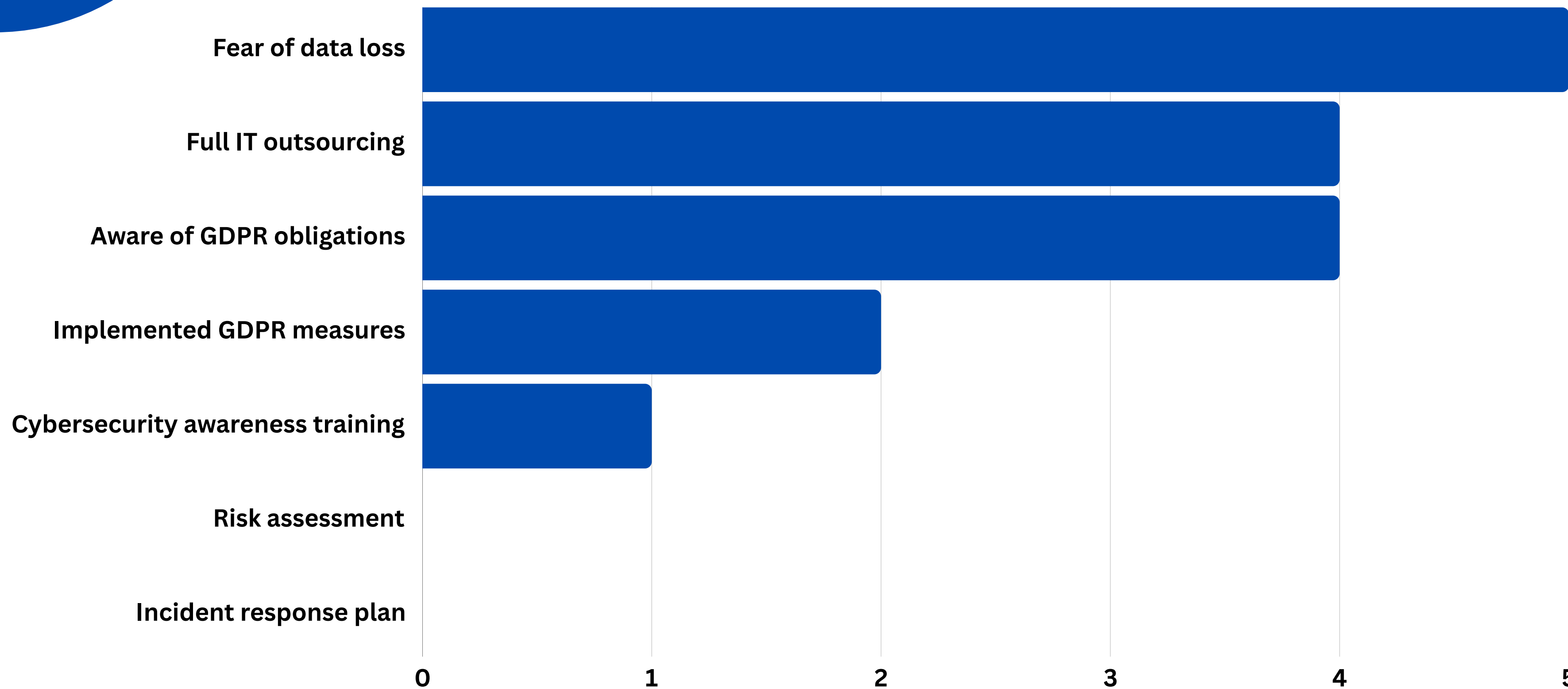
Objective

Validate the real needs of Belgian accounting firms and define a representative SME profile to guide infrastructure design.

Method

- 5 accounting firms interviewed
- 9 open-ended questions
- Data collected via phone and email (March 2025)
- Analysis: thematic matrix to extract common challenges

QUALITATIVE ANALYSIS



QUALITATIVE ANALYSIS

Key Findings

- 4 out of 5 firms fully outsource their IT.
- Most firms are aware of GDPR but have not implemented any concrete measures.
- Risk awareness is low: no company has conducted a security audit or implemented an incident response plan
- The top fear mentioned by all firms is data loss, mostly due to ransomware, human error, or technical failure.

Conclusion

- SMEs are aware of the risks and regulations, but they do not act on them.
- A clear gap exists between awareness and action.
- **This shows a need for a simple solution to drive action.**

Deployment:

- **1. Virtual Machine Provisioning**

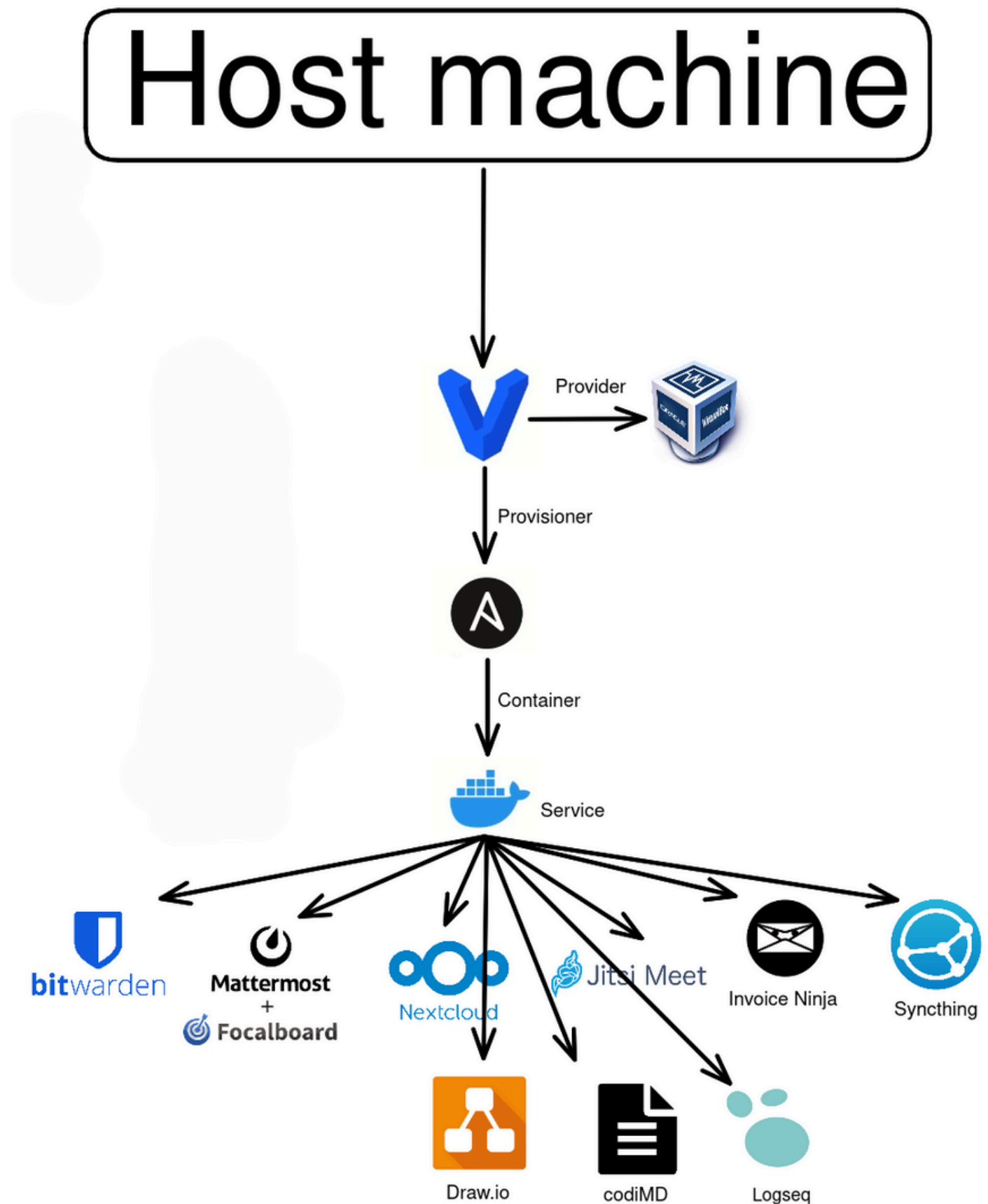
VMs are instantiated using Vagrant

- **2. Configuration & Automation**

Machines are configured using Ansible playbooks

- **3. Service Deployment (Apps & Tools)**


Web services and tools are deployed using Docker containers



- Infrastructure Adaptation
 - Customized the existing JANUS platform for SMEs real-world needs
 - Implemented the CyFun Identify function (Basic level)
- Automation using IaC and CaC
 - Developed Ansible Playbooks:
 - Asset inventory (physical/software)
 - Risk assessment & vulnerability scanning (Trivy)
 - Governance and compliance documentation
 - YAML-based automated documentation and inventory generation

TECHNICAL IMPLEMENTATION

OUTPUT PHYSICAL ASSETS (ID.AM-1)

```
domain > cyfun > identify > assets > output >  assets.yml
1  asset_type: infrastructure
2  assets:
3  - cpu: 4 cores
4    id: vagrant
5    ip: 10.0.2.15
6    name: vagrant
7    os: Debian 12.6
8    ram: 3914 MB
9    type: vm
10 collected_on: '2025-06-14'
11 description: Auto-collected infrastructure asset for CyFun ID.AM-1 compliance
```

EXAMPLE OF AUTOMATIC GENERATED INVENTORY OF INFRASTRUCTURE ASSETS

TECHNICAL IMPLEMENTATION

MANUAL ASSETS (ID.AM-1)

```
domain > cyfun > identify > assets > manuals > manual-assets.yml
1  asset_type: human-assets
2  description: >
3      This file is intended to document all organizational assets that cannot be
4      automatically collected via the system (e.g. user laptops, mobile phones, printers,
5      routers, or any other physical or offline assets).
6
7      Fields marked as REQUIRED must be filled to ensure CyFun ID.AM-1 compliance.
8      Fields marked as OPTIONAL can be left blank or marked as TO_DO if unknown.
9
10 last_review: TO_BE_FILLED # REQUIRED - Last time this file was reviewed (format: YYYY-MM-DD)
11
12 assets:
13     - id: TO_BE_FILLED # REQUIRED - Unique asset ID (e.g. Laptop-jdoe-001)
14       name: TO_BE_FILLED # REQUIRED - Human-readable name (e.g. John's Laptop)
15       type: TO_BE_FILLED # REQUIRED - Device type (e.g. Laptop, printer, router, phone, etc.)
16       owner: TO_BE_FILLED # REQUIRED - Assigned user or department (e.g. Alice, Accounting)
17       location: TO_BE_FILLED # REQUIRED - Physical location or office (e.g. Floor 2, Room 210)
18       os: TO_DO # OPTIONAL - Operating system (e.g. Windows 11, iOS 16.1)
19       ip: TO_DO # OPTIONAL - IP address (can be null if offline or unmanaged)
20       network: TO_DO # OPTIONAL - "connected", "not connected", "unknown"
21       serial_number: TO_DO # OPTIONAL - Device serial number or inventory label
22       manufacturer: TO_DO # OPTIONAL - Manufacturer or brand (e.g. Dell, HP)
23       purchase_date: TO_DO # OPTIONAL - Date of purchase (format: YYYY-MM-DD)
24       last_review: TO_BE_FILLED # REQUIRED - Date this asset entry was last checked or updated
25
```

TECHNICAL IMPLEMENTATION

SOFTWARE ASSETS (ID.AM-2)

```
domain > cyfun > identify > software > output > assets_software.yml
1  - collected_on: '2025-06-14'
2    host: vagrant
3    inventory_type: software
4    os: Debian 12.6
5    software:
6      docker_services:
7        - name: logseq
8          versions:
9            - ghcr.io/logseq/logseq-webapp:latest
10       - name: drawio
11         versions:
12           - jgraph/drawio
13       - name: codimd-codimd
14         versions:
15           - hackmdio/hackmd:2.4.2
16       - name: codimd
17         versions:
18           - postgres:11.6-alpine
19       - name: syncthing
20         versions:
21           - syncthing/syncthing
22       - name: nextcloud
23         versions:
24           - nextcloud
```

TECHNICAL IMPLEMENTATION

PRIORITIZED INVENTORY (ID.AM-5)

```
domain > cyfun > identify > inventory > output > prioritized_inventory.yml
1  - classification: critical
2    criticality: critical
3    name: Credentials and Access Information
4    value: very_high
5  - classification: internal
6    criticality: high
7    name: nextcloud
8    value: high
9  - classification: confidential
10   criticality: high
11   name: bitwarden
12   value: very_high
13  - classification: confidential
14   criticality: high
15   name: Client Data
16   value: very_high
17  - classification: confidential
18   criticality: high
```

TECHNICAL IMPLEMENTATION

LEGAL DOCUMENTATION (ID.GV-3)

```
domain > cyfun > identify > policies > output > legal_compliance.md > # Legal and Regulatory Compliance > ## 2. Our Actions
1  # Legal and Regulatory Compliance
2
3  This document explains the main legal and cybersecurity rules for our accounting firm in Belgium.
4  It helps meet CyFun ID.GV-3 (governance) and refers to NIS2, active since October 2024.
5  All team members (managers, accountants, secretary) must know these rules.
6  The Directive Manager ensures they are followed.
7
8
9  ## 1. Main Legal Rules
10
11  ### 1.1 General Data Protection Regulation (GDPR)
12
13  We handle clients personal and financial data.
14  Data must be safe (strong passwords, encryption, secure backups).
15  Clients can ask to see, change, or delete their data.
16  If there's a data breach, we must tell the Belgian Data Protection Authority (APD) within 72 hours.
17
18
19  ### 1.2 Belgian Accounting Law
20
21  Accounting documents must be kept for at least 7 years.
22  Documents must be ready for tax authorities if requested.
23  Digital storage is allowed but must be secure and organized.
24
25
26  ### 1.3 Confidentiality Rules
27
28  As accountants, we must keep client data private.
29  Only authorized staff can access sensitive files.
30  Personal USB drives or private email accounts are not allowed.
31
```


TECHNICAL IMPLEMENTATION

VULNERABILITY SCANNING WITH TRIVY (ID.RA-1)

```
domain > cyfun > identify > risk > output >  vulnerabilities.yml
1  collected_on: '2025-06-14'
2  scanner: trivy_container
3  unique_cve_count: 346
4  vulnerabilities:
5  - VulnerabilityID: CVE-2025-4802
6    severity: HIGH
7    title: 'glibc: static setuid binary dlopen may incorrectly search LD_LIBRARY_PATH'
8    cwe:
9      - CWE-426
10   images:
11     - ghcr.io/bitwarden/admin:2025.6.1
12     - ghcr.io/bitwarden/attachments:2025.6.1
13     - ghcr.io/bitwarden/events:2025.6.1
14     - hackmdio/hackmd:2.4.2
15     - ghcr.io/bitwarden/icons:2025.6.1
16     - ghcr.io/bitwarden/identity:2025.6.1
17     - invoiceninja/invoiceninja-debian:latest
18     - jitsi/jicofo:stable-9220-1
19     - jitsi/jvb:stable-9220-1
20     - nextcloud:latest
21     - ghcr.io/bitwarden/nginx:2025.6.1
22     - jitsi/prosody:stable-9220-1
23     - ghcr.io/bitwarden/setup:2025.6.1
24     - ghcr.io/bitwarden/sso:2025.6.1
25     - ghcr.io/bitwarden/web:2025.6.0
26     - jitsi/web:stable-9220-1
27  - VulnerabilityID: CVE-2025-5222
28    severity: HIGH
29    title: 'icu: Stack buffer overflow in the SRBRoot::addTag function'
30    cwe:
31      - CWE-120
```


How it aligns with the Framework ?

- **ID.AM-1 to ID.AM-5 – Asset Management**
 - Inventories auto-generated (physical, software, dependencies and Inventory)
 - Manual templates for what cannot be detected
- **ID.GV-1 to ID.GV-4 – Governance**
 - Policies, legal compliance, risk strategy -> produced as Markdown
 - Written for non-technical users
- **ID.RA-1 & ID.RA-5 – Risk Assessment**
 - Trivy scans vulnerabilities (ID.RA-1)
 - Manual templates of threats and risks + mitigation (ID.RA-5)
- **Additional Compliance Tools**
 - Ready-to-use checklists provided for easy compliance tracking

LIMITATIONS & FUTURE WORK

Limitations

- **Scope limitation** : Focus only on the Identify function (not full CyFun)
- **No field testing** : The solution was not evaluated in real accounting firms
- **Target-specific** : Solution tailored to Belgian accounting firms only

Future Work

- Extend to other CyFun functions (Protect, Detect...)
- Deploy and validate in real accounting firms
- Improve asset detection (e.g., passive scanning)
- Add a simple GUI for non-technical users

CONCLUSION

- **Objective achieved** : A modular and automated infrastructure was successfully built, aligned with Cyfun Identify function (Basic level)
- **Using Automation** : Tools like Ansible and Trivy reduce manual effort and technical dependency.
- **Reusable & extensible** : JANUS-based setup can be adapted to other SME sectors or extended to other CyFun functions.
- **Research question answered** : Yes, a plug-and-play infrastructure is achievable for the Identify function, proving that SMEs can meet baseline requirements with minimal resources.

REFERENCE

Key References

- Alahmari, A., & Duncan, B. (2020). Cybersecurity Risk Management in SMEs: A Systematic Review of Recent Evidence. IEEE CSR 2020.
- Ozkan, Y., & Spruit, M. (2023). Adaptable Security Maturity Assessment and Standardization for Digital SMEs. Journal of Computer Information Systems.
- Latic, A. (2022). Cybersecurity Threats to Small Accounting Organizations.
- CCB – Centre pour la Cybersécurité Belgique (2024). Cadre des CyberFundamentals (CyFun).
- Ponsard, C., Massonet, P., Grandclaudon, J., & Point, N. (2020). From Lightweight Cybersecurity Assessment to SME Certification Scheme in Belgium. IEEE EuroS&PW.
- Chidukwani, A., Zander, S., & Koutsakis, P. (2024). Cybersecurity Preparedness of SMBs. Computers & Security.
- Rombaldo Junior, C., Becker, I., & Johnson, S. (2024). Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. arXiv:2309.17186.



THANK YOU !

ANY QUESTIONS ?

Question	Company 1	Company 2	Company 3	Company 4	Company 5
IT / cybersecurity team	Externalized + internal contact	Internal accountant manages IT	External provider	Freelance external	Dedicated IT company
Accounting software used	BOB 50, Sage Cloud Demat	Sage BOB 50, HORUS, SaaS for tax returns	Bob, Horus	Sage BOB	Sage BOB 50
Software for compliance/continuity	Client portfolio management, administrative tools	Sage BOB and Horus	Bob and Horus	Microsoft 365, BOB	Email, BOB 50
Regulations to follow	GDPR	GDPR	No idea	GDPR	GDPR
Information security (GDPR, NIS2, CyFun)	GDPR implemented, client protocol	GDPR yes, CyFun unknown	Basic knowledge of GDPR	GDPR	Basic knowledge of GDPR
Cybersecurity audit / risk assessment	Never done	No	No	No	No
Main risks and threats	Attacks preventing access to data	Malware, phishing	Data loss	Ransomware, data loss	Data loss
Sensitive data protection	None	Dropbox backup + strong passwords	2FA + daily backups on two sites	Restricted access	Weekly backup
Incident response plan / employee awareness	None	Informal awareness, no plan	None	No formal plan	No plan, no training

```
domain > cyfun > identify > risk > 📄 vulnerabilities.yml
1 | collected_on: "2025-05-22"
2 | scanner: trivy_container
3 | images_scanned: 4
4 | unique_cve_count: 88
5 | vulnerabilities:
6 | - VulnerabilityID: CVE-2022-3715
7 |   cwe:
8 |     - CWE-119
9 |     - CWE-787
10 |   images:
11 |     - jitsi/jicofo:stable-9220-1
12 |     - jitsi/jvb:stable-9220-1
13 |     - jitsi/prosody:stable-9220-1
14 |     - jitsi/web:stable-9220-1
15 |   severity: HIGH
16 |   title: 'bash: a heap-buffer-overflow in valid_parameter_transform'
17 | - VulnerabilityID: CVE-2022-1304
18 |   cwe:
19 |     - CWE-125
20 |     - CWE-787
21 |   images:
22 |     - jitsi/jicofo:stable-9220-1
23 |     - jitsi/jvb:stable-9220-1
24 |     - jitsi/prosody:stable-9220-1
25 |     - jitsi/web:stable-9220-1
26 |   severity: HIGH
27 |   title: 'e2fsprogs: out-of-bounds read/write via crafted filesystem'
28 | - VulnerabilityID: CVE-2024-2961
29 |   cwe:
30 |     - CWE-787
31 |   images:
32 |     - jitsi/jicofo:stable-9220-1
```

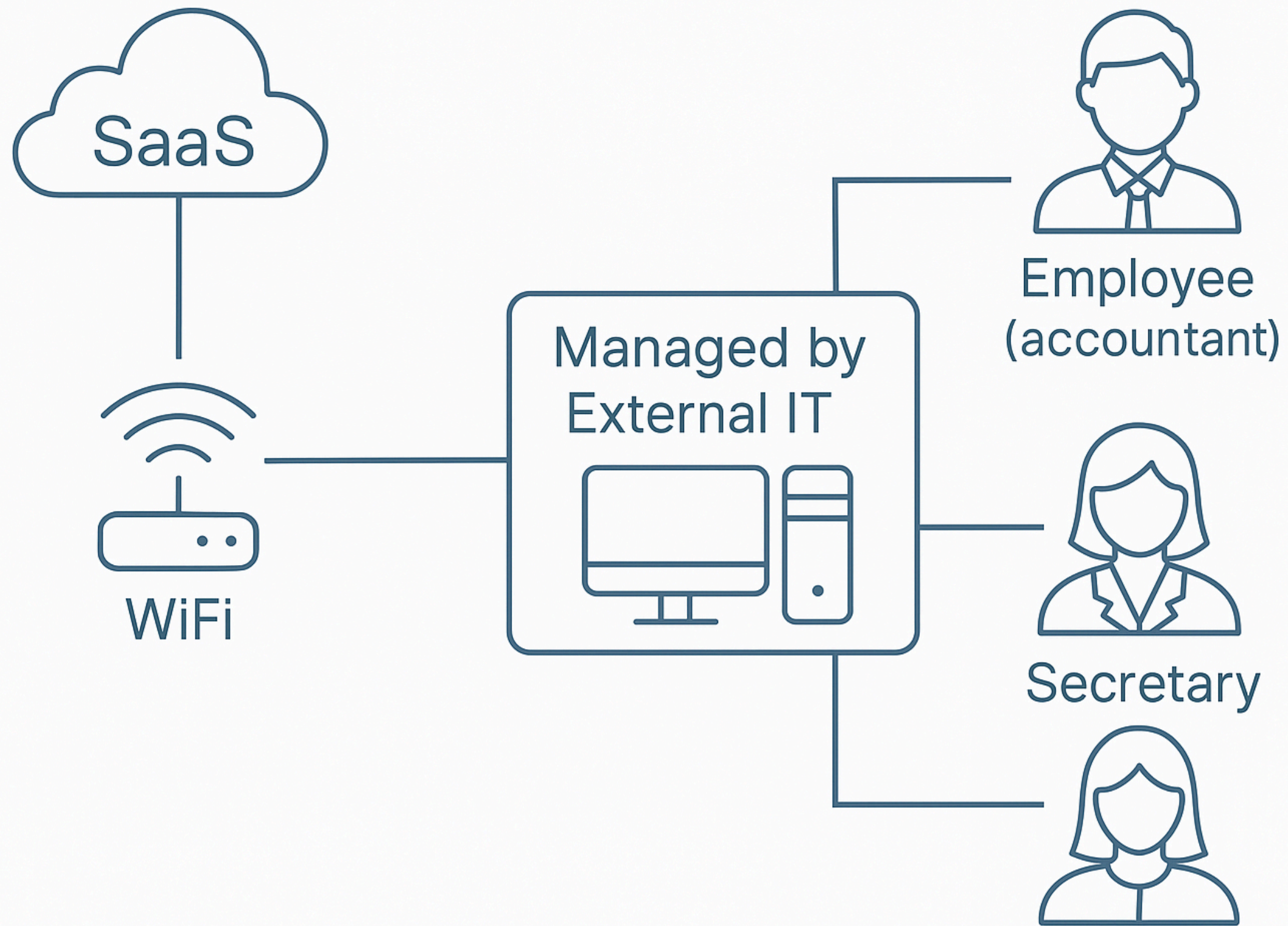


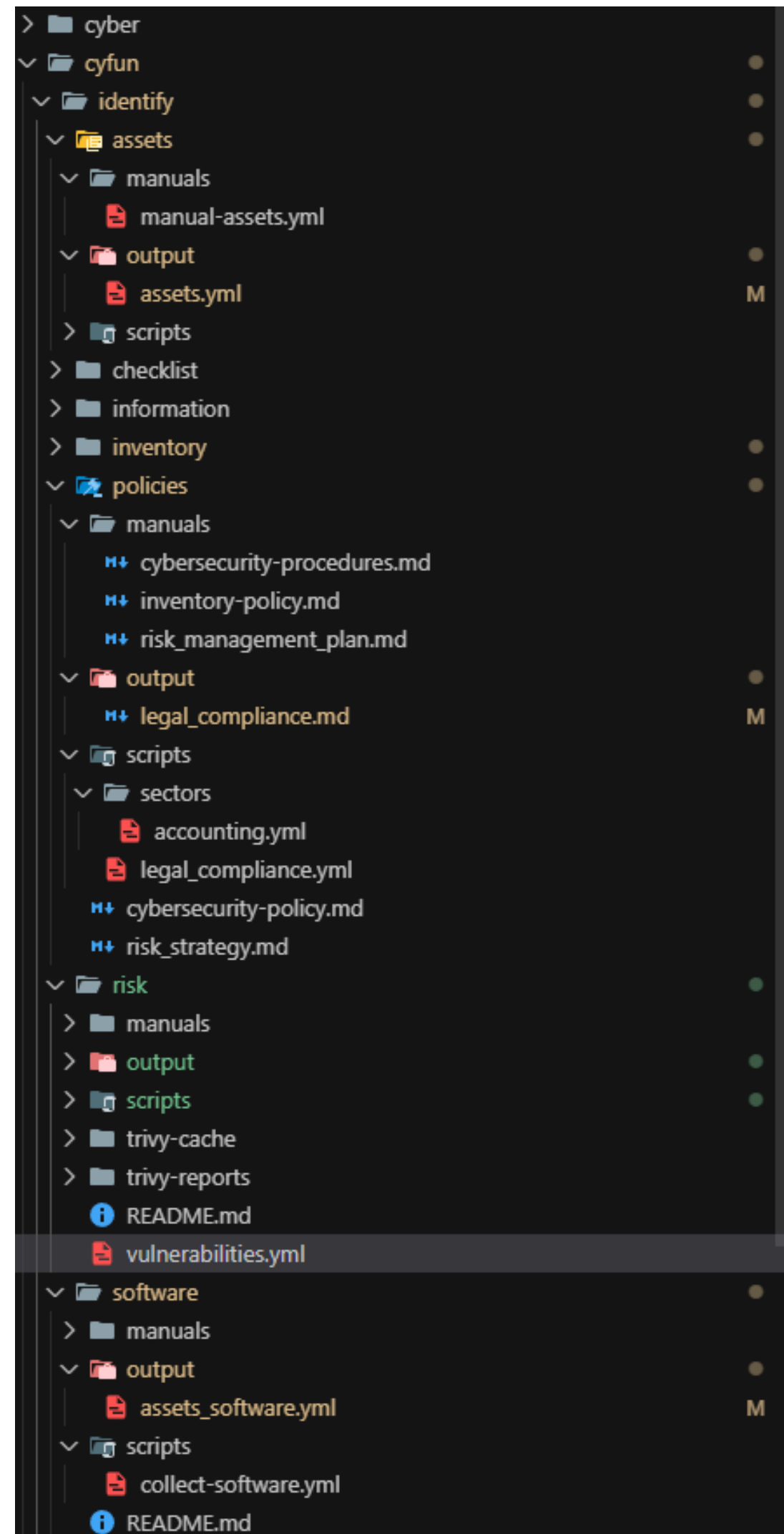
```
Invite de commandes X + v
}

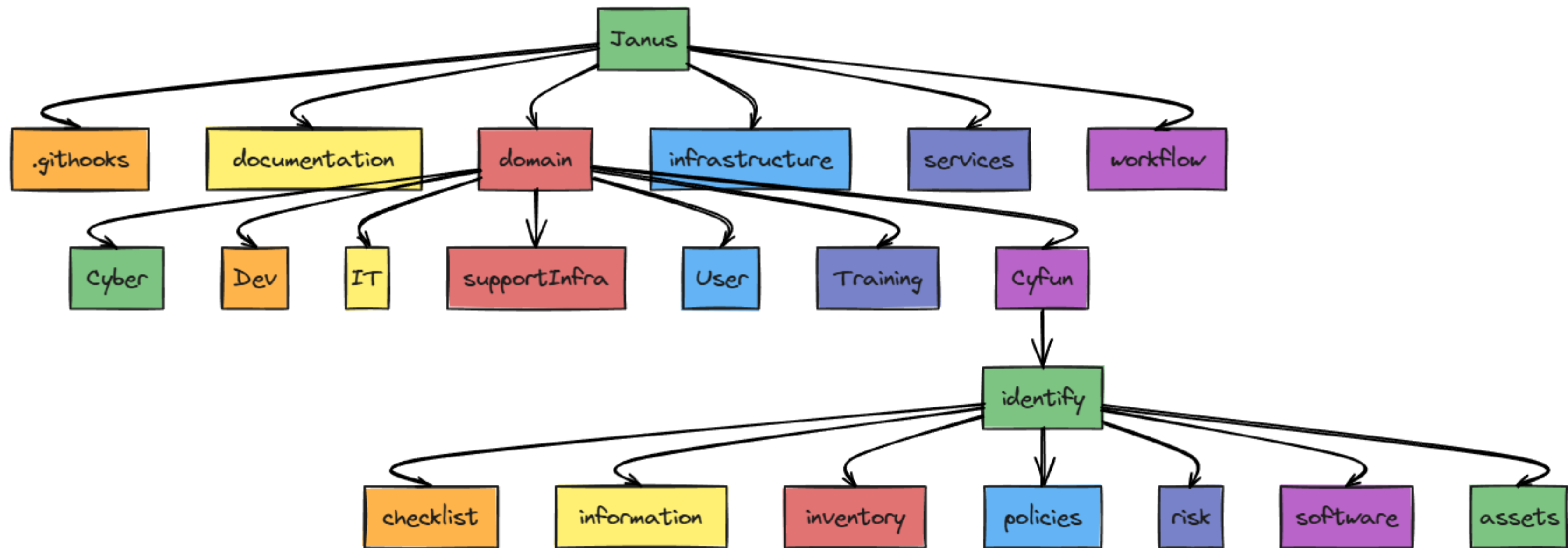
PLAY RECAP *****
10.10.10.12 : ok=12 changed=5 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

==> user_domain: Machine 'user_domain' has a post `vagrant up` message. This is a message
==> user_domain: from the creator of the Vagrantfile, and not from Vagrant itself:
==> user_domain:
==> user_domain: #####
==> user_domain: 🚀 Janus Services Deployment Report 🚀
==> user_domain: #####
==> user_domain:
==> user_domain: 🌐 Access Services via Web (local machine):
==> user_domain:
==> user_domain: ❤️ Mattermost + Focalboard: http://localhost:8081
==> user_domain: 💬 SyncThing: http://localhost:8082
==> user_domain: 📞 Jitsi Meet: https://localhost:8443
==> user_domain: 📁 Nextcloud: http://localhost:8084
==> user_domain: 📁 Bitwarden: https://localhost:8444
==> user_domain: 📄 Drawio: https://localhost:8446
==> user_domain: 📄 codiMD: http://localhost:8086
==> user_domain: 💰 Invoice Ninja: http://localhost:8087
==> user_domain: 📖 logseq: http://localhost:8088
==> user_domain:
==> user_domain: 🎉 Explore and Enjoy! 🎉
==> user_domain:
==> user_domain: 🙌 Greetings from your friendly cyber-intern! 🐙
==> user_domain:

C:\Users\arnau\OneDrive\Bureau\ULB\MA2INFO\MEMOIRE\janus\domain\user>
```









Financial market infrastructures				Common skills		Common skills		Common skills		Extended Skills		Extended Skills			
Banking															
Organization Size (L/M/S = 3/2/1)		1	Threat Actor Type	Competitors		Ideologues Hactivists		Terrorist		Cyber Criminals		Nation State actor			
Cyber Attack Category		Global or Targetted	Impact	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score		
Sabotage/ Disruption (DDOS,...)		2	High	Low	0	Med	10	Med	10	Low	0	Med	10		
Information Theft (espionage, ...)		2	High	Low	0	Low	0	Med	10	High	20	Med	10		
Crime (Ransom attacks)		1	High	Low	0	Low	0	Low	0	High	10	Low	0		
Hactivism (Subversion, defacement...)		1	Med	Low	0	Med	2,5	Low	0	Low	0	Med	2,5		
Disinformation (political influencing)		1	Low	Low	0	Med	0	Low	0	Low	0	Low	0	Score	CyFun Level
Total		Total	Total		0		12,5		20		30		22,5	85	BASIC

 assets.yml M X

domain > cyfun > identify > assets > output >  assets.yml

```
1  asset_type: infrastructure
2  assets:
3  - cpu: 4 cores
4    id: vagrant
5    ip: 10.0.2.15
6    name: vagrant
7    os: Debian 12.6
8    ram: 3914 MB
9    type: vm
10 collected_on: '2025-06-14'
11 description: Auto-collected infrastructure asset for CyFun ID.AM-1 compliance
12
```

```
assets_software.yml M X
domain > cyfun > identify > software > output > assets_software.yml
1  - collected_on: '2025-06-14'
2    host: vagrant
3    inventory_type: software
4    os: Debian 12.6
5    software:
6      docker_services:
7        - name: logseq
8          versions:
9            - ghcr.io/logseq/logseq-webapp:latest
10       - name: drawio
11         versions:
12           - jgraph/drawio
13       - name: codimd-codimd
14         versions:
15           - hackmdio/hackmd:2.4.2
16       - name: codimd
17         versions:
18           - postgres:11.6-alpine
19       - name: syncthing
20         versions:
21           - syncthing/syncthing
22       - name: nextcloud
23         versions:
24           - nextcloud
25           - mariadb:10.6
26       - name: jitsi
27         versions:
28           - jitsi/jvb:stable-9220-1
```

```
assets_software.yml M X
domain > cyfun > identify > software > output > assets_software.yml
1  - collected_on: '2025-06-14'
5    software:
44     - name: bitwarden
54       - ghcr.io/bitwarden/notifications:2025.6.1
55       - ghcr.io/bitwarden/sso:2025.6.1
56       - ghcr.io/bitwarden/icons:2025.6.1
57     packages:
58     - name: acl
59       version: 2.3.1-3
60     - name: adduser
61       version: '3.134'
62     - name: ansible
63       version: 7.3.0+dfsg-1
64     - name: ansible-core
65       version: 2.14.3-1
66     - name: apparmor
67       version: 3.0.8-3
68     - name: apt
69       version: 2.6.1
70     - name: apt-listchanges
71       version: '3.24'
72     - name: apt-utils
73       version: 2.6.1
74     - name: base-files
75       version: 12.4+deb12u6
76     - name: base-passwd
77       version: 3.6.1
78     - name: bash
79       version: 5.2.15-2+b7
80     - name: bash-completion
81       version: 1:2.11-6
82     - name: bind9-dnsutils
83       version: 1:9.18.28-1~deb12u2
84     - name: bind9-host
```

JANUS

.githubhooks

commit-msg

pre-commit

README.md

archive

code

documentation

domain

cyber

cyfun

identify

assets

manuals

output

assets.yml

scripts

checklist

information

inventory

policies

manuals

cybersecurity-procedures.md

inventory-policy.md

risk_management_plan.md

output

legal_compliance.md

scripts

sectors

accounting.yml

legal_compliance.yml

cybersecurity-policy.md

risk_strategy.md

risk

software

manuals

output

assets_software.yml

scripts

collect-software.yml

README.md

README.md

policies

domain > cyfun > identify > policies > scripts > sectors > accounting.yml

1

#

2

Legal rules & cybersecurity for the accounting sector

3

#

4

sector_rules:

5

sector_name: "Accounting (Belgium)"

6

last_updated: "2025-06-10"

7

8

intro: |

9

This document explains the main legal and cybersecurity rules for our accounting firm in Belgium.

10

It helps meet **CyFun ID.GV-3** (governance) and refers to **NIS2**, active since October 2024.

11

All team members (managers, accountants, secretary) must know these rules.

12

The **Directive Manager** ensures they are followed.

13

14

legal_sections:

15

- title: "1.1 General Data Protection Regulation (GDPR)"

16

content: |

17

We handle clients personal and financial data.

18

Data must be safe (strong passwords, encryption, secure backups).

19

Clients can ask to see, change, or delete their data.

20

If there's a data breach, we must tell the Belgian Data Protection Authority (APD) within 72 hours.

21

22

- title: "1.2 Belgian Accounting Law"

23

content: |

24

Accounting documents must be kept for at least 7 years.

25

Documents must be ready for tax authorities if requested.

26

Digital storage is allowed but must be secure and organized.

27

28

- title: "1.3 Confidentiality Rules"

29

content: |

30

As accountants, we must keep client data private.

31

Only authorized staff can access sensitive files.

32

Personal USB drives or private email accounts are not allowed.

33

34

- title: "1.4 NIS2 Directive (optional)"

35

content: |

36

Our firm may be an "important entity" or a supplier to critical sectors (e.g., healthcare, finance).

37

CyFun level 1 meets basic NIS2 needs, but extra steps (e.g., audits, documentation) may be needed for full compliance.

38

39

actions_table:

40

- rule: "GDPR Protect Client Data"

41

how: "Strong passwords, limited access, encrypted backups via JANUS"

42

who: "Directive Manager"

43

44

- rule: "GDPR Client Data Requests"

45

how: "Clients can email to update or delete data"

46

who: "Secretary"

47

48

- rule: "GDPR Report Data Breach"

49

how: "Process in place, reviewed yearly"

domain > cyfun > identify > checklist > checklist-ID.AM-1.md > # CyFun ID.AM-1 Compliance Checklist – Infrastructure & Asset Inventory > ## Checklist

```
1  # CyFun ID.AM-1 Compliance Checklist – Infrastructure & Asset Inventory
2
3  This checklist ensures compliance with the CyFun sub-control ID.AM-1:
4  _"Physical devices and systems within the organization are inventoried."_
5
6  ---
7
8  ## OBJECTIVE
9  To maintain a complete, accurate, and up-to-date inventory of all physical and virtual devices involved in information processing.
10
11  ---
12
13  ## Checklist
14
15  | Requirement | Status | Evidence / Notes |
16  |-----|-----|-----|
17  | 1. An inventory tool exists and is version-controlled | [x] | `collect-assets.yml` in Git |
18  | 2. Infrastructure is automatically inventoried | [x] | Generated on `vagrant up` (`assets.yml`) |
19  | 3. A manual inventory template exists for non-automated assets | [ ] | `manual-assets.yml` |
20  | 4. Manual inventory includes required fields (id, name, type, etc.) | [x] | Template with TO_BE_FILLED placeholders |
21  | 5. There is a review policy that defines frequency and roles | [x] | `inventory-policy.md` |
22  | 6. Inventory includes network and non-network assets | [ ] | Instructions in `manual-assets.yml` |
23  | 7. All inventory files are tracked in Git | [x] | Git versioning of `assets.yml`, `manual-assets.yml` |
24  | 8. Last review date is visible and up-to-date | [ ] | `last_review:` field in both YAML files |
25  | 9. Team roles and responsibilities are clearly assigned | [x] | Documented in `inventory-policy.md` |
26  | 10. Auditability is ensured (readability, reproducibility) | [x] | Markdown, Git, YAML, Ansible-based |
27
28  ---
29
```