



BRAIN FRAME

We give security, quality and compliance professionals the wings they deserve with a first of its kind solution combining ISMS, GRC, QMS and DMS in one platform for an efficient collaboration, documentation, implementation, certification and continuous improvement of any framework, regulation or standard.

W W W . B R A I N F R A M E . C O M

Helping you efficiently scale





Mission

We digitalize, centralize and remove all inefficiencies in security, compliance and regulatory work by providing professionals with an all-in-one integrated management system at a reasonable cost to help scale their business.



REDUCE COMPLIANCE COMPLEXITY

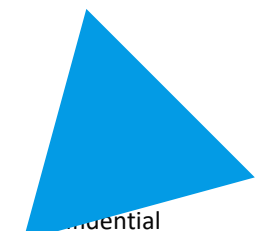




DIGITALIZE

The Implementation and Governance of any framework, regulation or standard

www.brainframe.com As a service
Or self-hosted



Confidential

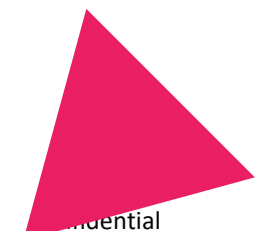
WWW.BRAINFRAME.COM



REDUCE TIME TO

- Understand requirements
- Reach certification
- Maintain compliance
- Improve posture

For all your compliance and security by centralizing all workflows in one place



ALL IN ONE SOLUTION



Document management



Versions & approvals



Document templates



Asset management



Requirement mapping



Maturity tracker



Task management



Workflows



Roadmaps & timeline



Request forms



Risk management



Website snapshots



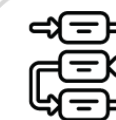
Objectives tracker



Document distribution



Multi customer/entity



Dependency tracker



Diagram editor

● ● ● Much more...

Digitalize your Security, Quality & Compliance management like a PRO

MADE FOR
CONSULTANTS

WWW.BRAINFRAME.COM



Document management



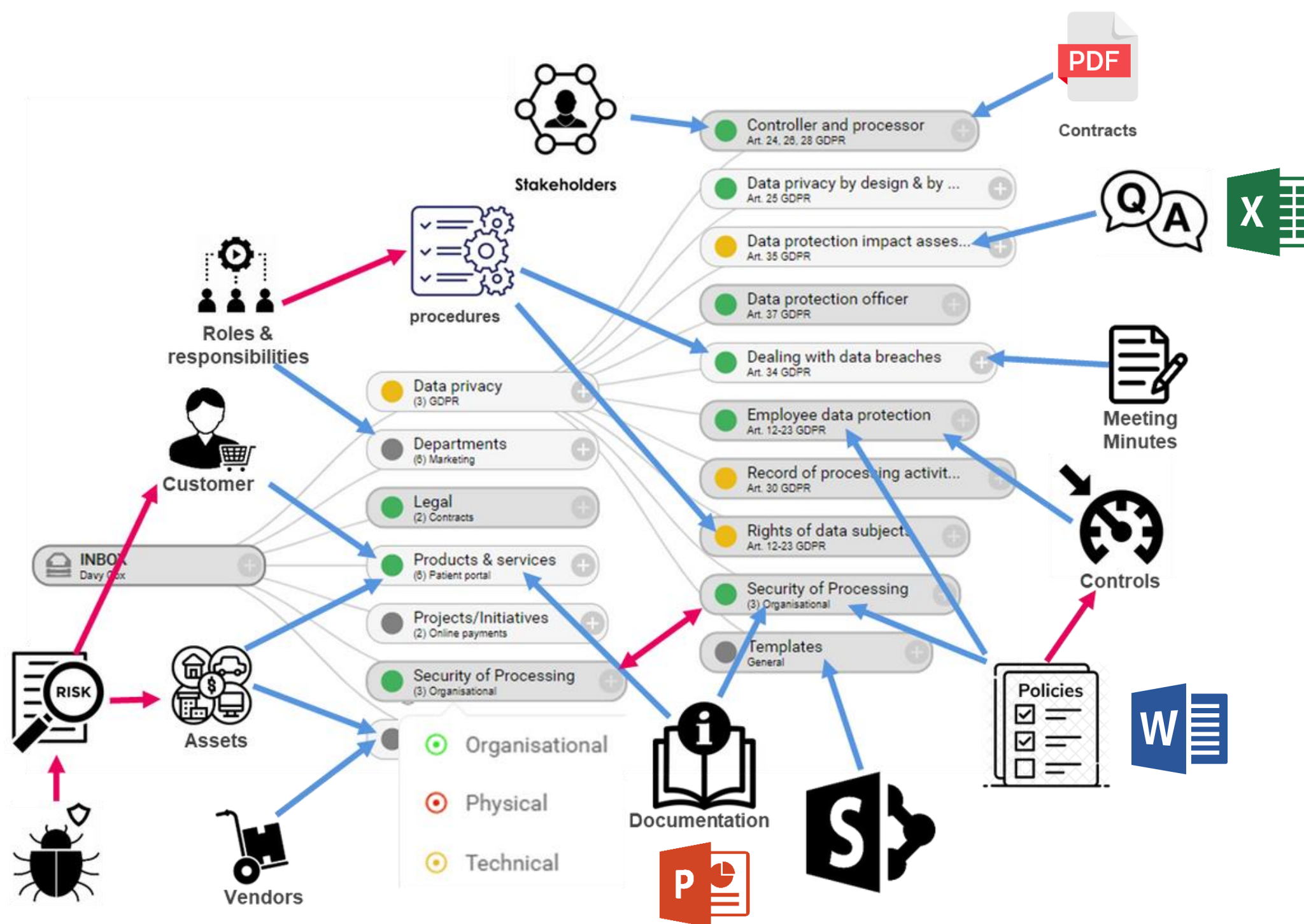
Asset management



BRAINFRAME



INTUITIVE & VISUAL



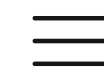


Document management



Asset management

CENTRAL AUDIT TRIALS



Risk evaluations

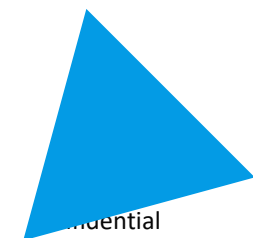
Declarations

Internal audit activities

Supplier workflows

Meeting minutes

Access requests & reviews



Confidential



AUGMENT YOUR EXISTING WORK



**Integrated version
control & change history**



2FA Document approvals



**Document comments &
notifications**

Use your docs as templates

CISO review

CEO review

Publication



STANDARDIZE REGULATORY COMPLIANCE



100+ Industry specific document types & templates
Or define your own document templates

Business Objective KPI	Role and responsibilities	Impact	Accounting system	Documentation system	Operating system (OS)	IT Room, Datacenter or cloud provider	Printer, fax, scanner or copy machine
Business risk	Stakeholder/Interested party	Policy	Algorithm	Domain name (DNS or similar)	PDF	Internet gateway provider/device (ISP)	Server
Certificate	Supplier or subcontractor	Procedure	Authentication system	Email	Sales system	Inventory of physical assets	Warehouse, storage or container
Company	Visual Collection	Security incident	Backend system	Email system	Sharepoint document	Measurement device	Workstation
Competitor	Administrative security control	Security objective KPI	Backups	Encryption key, software or mechanism	Software	Network router	Intellectual Property
Consultant	Auditable proof	Technical security control	Billing system	Frontend system	Software Firewall	Network switch	Legal risk
Contact person	Business Continuity Plan	Threat	Bus/Communication system	Helpdesk system	Source code repository	Other device	Non disclosure agreement
Customer	Confidentiality, integrity or availability Risk	Threat actor	CRM	Image	Spreadsheet	Phone	Patent, contract, certificate or ownership
Department or Working group	Guideline	Vulnerability	Cloud SaaS Product/Service	Intrusion detection system (IDS)	Technology	Physical asset	Regulation, Legislation or standard
	ISMS Management review meeting	Controller(s) of the data	Company landing page or portal	Mobile app	Webservice	Physical firewall	Regulatory exemption

Management reviews

Search document type

Inventory of Service assets

Meeting notes

Note or idea

Project or initiative

Service availability KPI

Search document type

man

ISMS Management review meeting

Document management and storage system

No Data found



ISMS Management review

Stage 1 - Preparation of meeting and definition of input to present to management

As a minimum, the following information and data are presented during the management review

1. Status of actions from previous management reviews

CISO reports on the status of action items from previous meetings. Items that are not completed are carried on as continuing actions and are recorded as such in the minutes

1.1 From previous management review Stage 2 feedback

Completed

- (topic 1-6) Task
 - Status

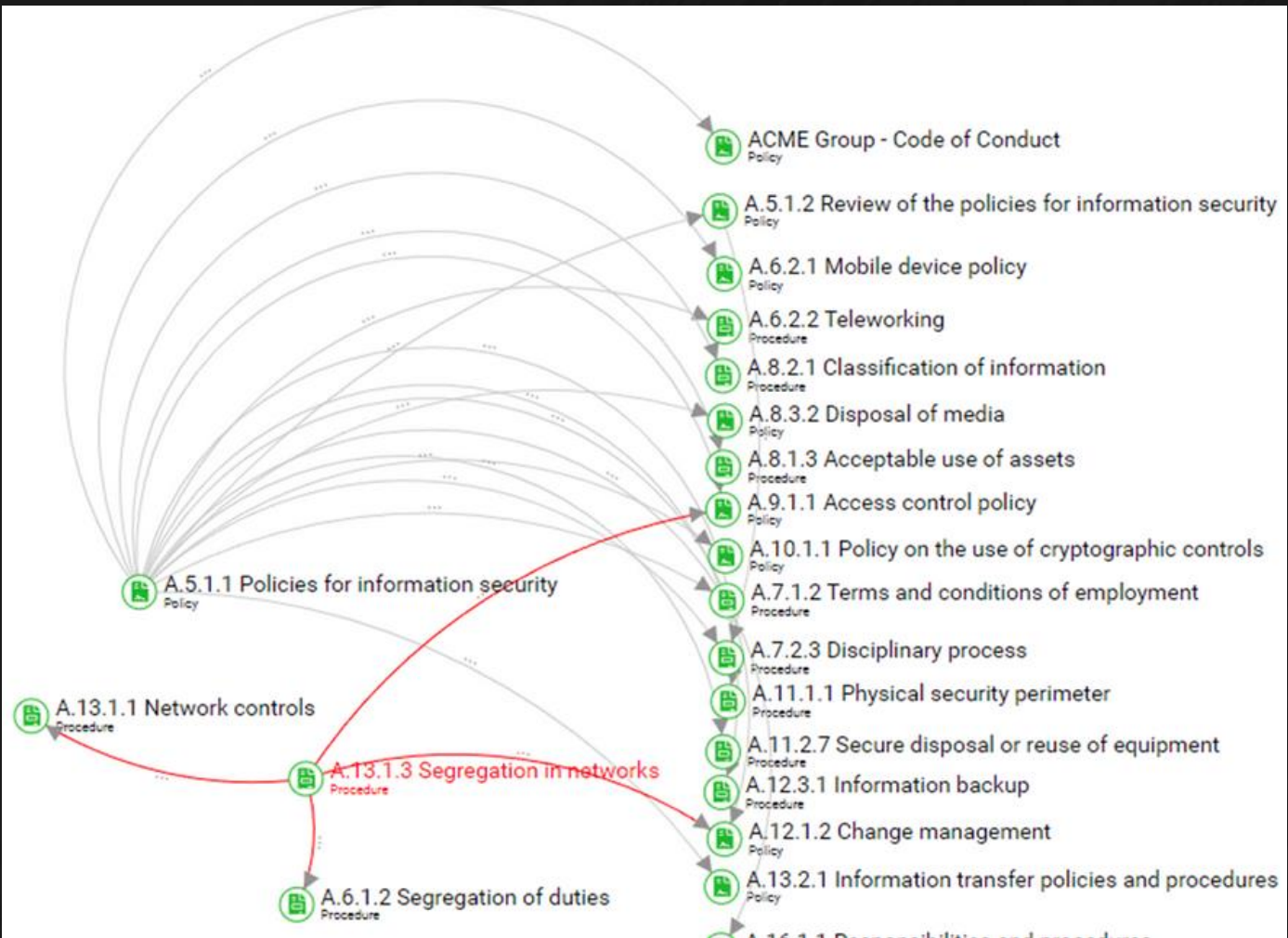
In progress

- (topic 1-6) Task
 - Status

Not completed

- (topic 1-6) Task
 - Justification

ASSET MAPPING & DEPENDENCIES



\$	Accounting system
⚡	Action to take
X	Algorithm
📄	Auditable proof
🔑	Authentication system
⚙️	Backend system
💾	Backups
📄	Billing system
🏢	Building, office or room
🚚	Business Continuity Plan (BCP)
📊	Business risk
👤	CRM
📄	Certificate
☁️	Cloud SaaS Product/Service
🏢	Company
🌐	Company landing page or portal
👤	Contact person
📄	Patent, contract, certificate or proof of ownership
🔧	Corrective or preventive action (CAPA)

MULTI-STANDARDS

- **Perfect for multi-standard mapping**

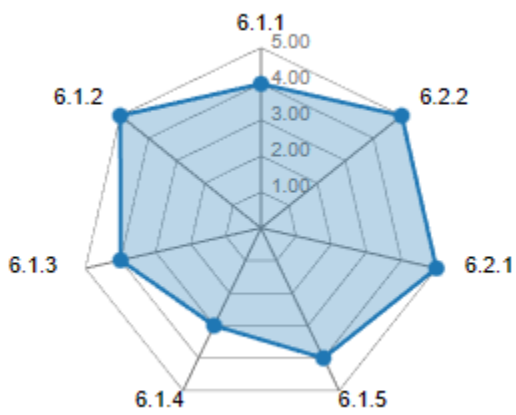
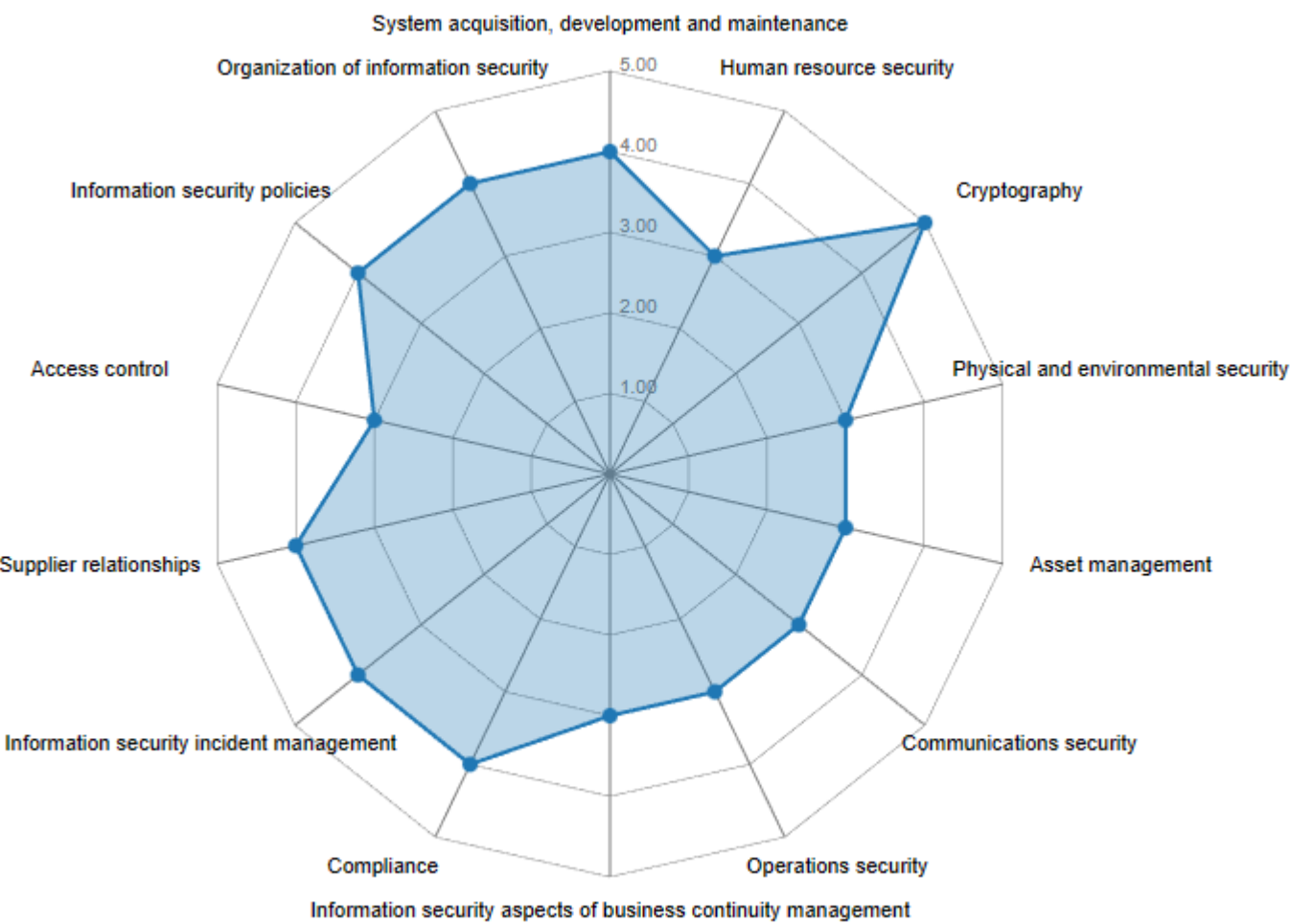
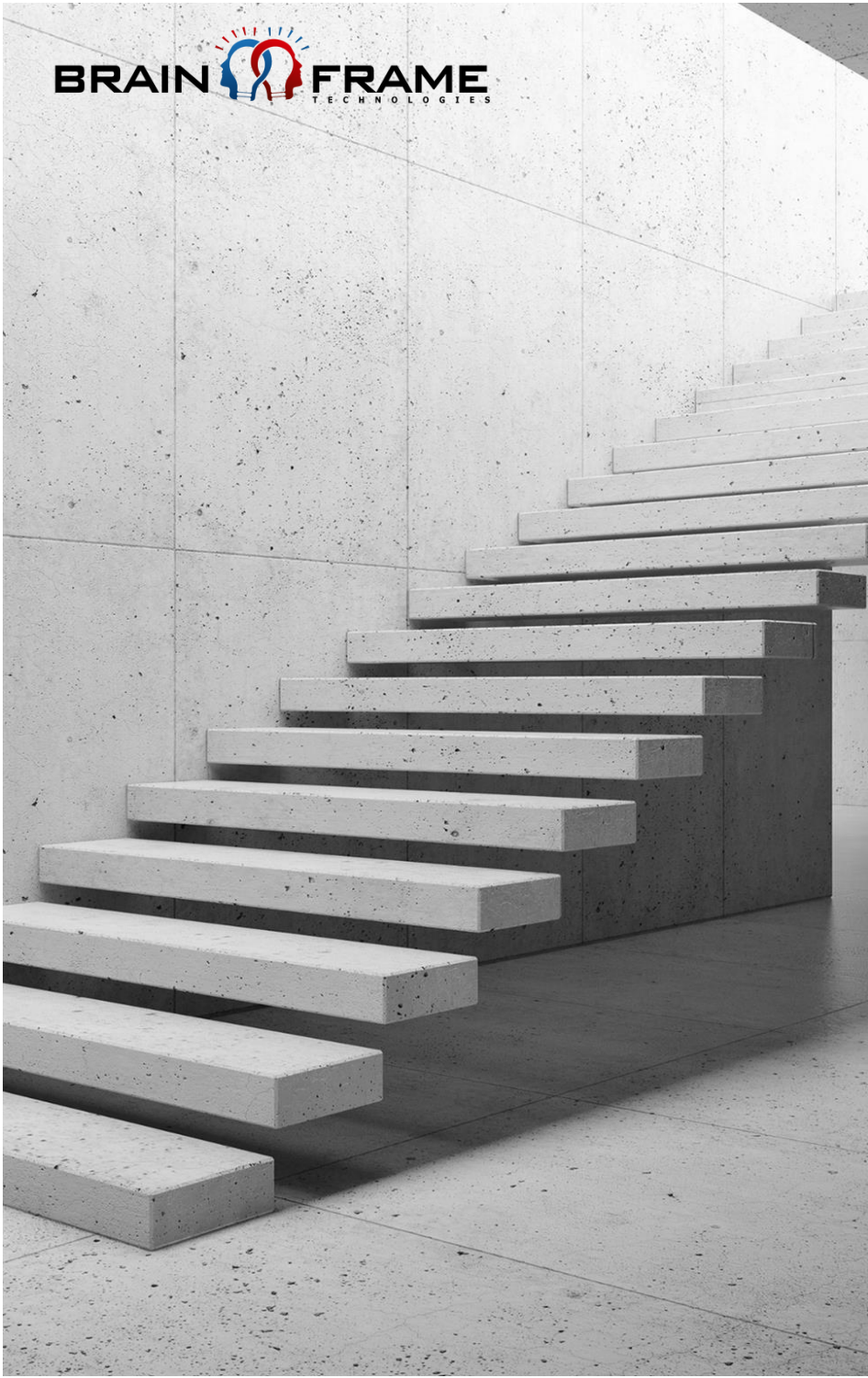
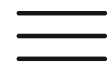
- | | | |
|------------|-----------------|-------------|
| • ISO27001 | • ISO9001 | • NIS, NIS2 |
| • ISO27017 | • ISO13485 | • GDPR |
| • ISO27701 | • FSSC CSSF PSF | • NIST |
| • SOC 2 | • PCI-DSS | • HIPAA, |

...

- **Link documents to multiple folders**
- **Copy work between customers/entities**



Statement of applicability (SOA)



- Not applicable
- Applicable but not implemented
- Applicable and being implemented
- Applicable and implemented - DEFINED
- Applicable and implemented - **MANAGED**
- Applicable and implemented - OPTIMIZED

A.6.1.1 Information security roles and responsibilities

Applicable and implemented - **MANAGED**

Linked controls

PRC-HR-24 Information security roles and responsibilities

Evidence of implementation

PRC-ALL-24 Responsibilities and authorities for roles relevant to IS

2022 ISMS SoA (signed).pdf

INTEGRATED TASK PLANNER

(Multi customer)



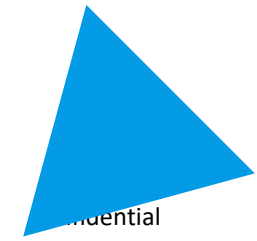
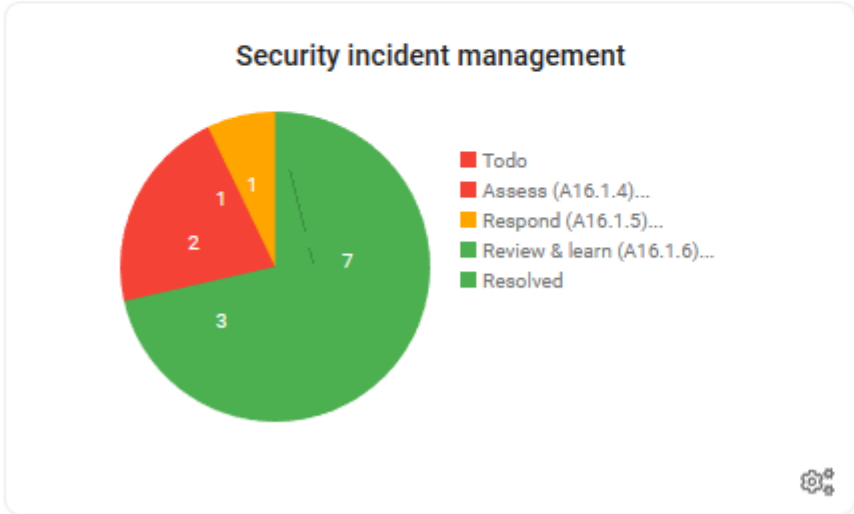
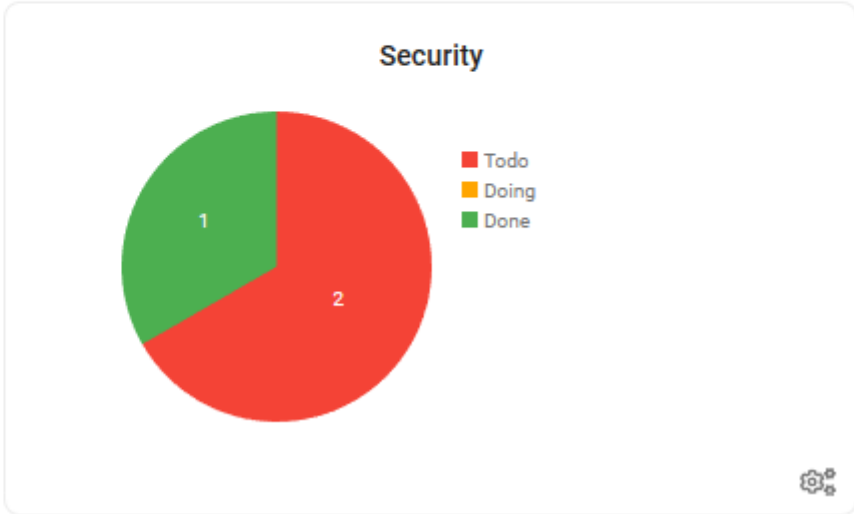
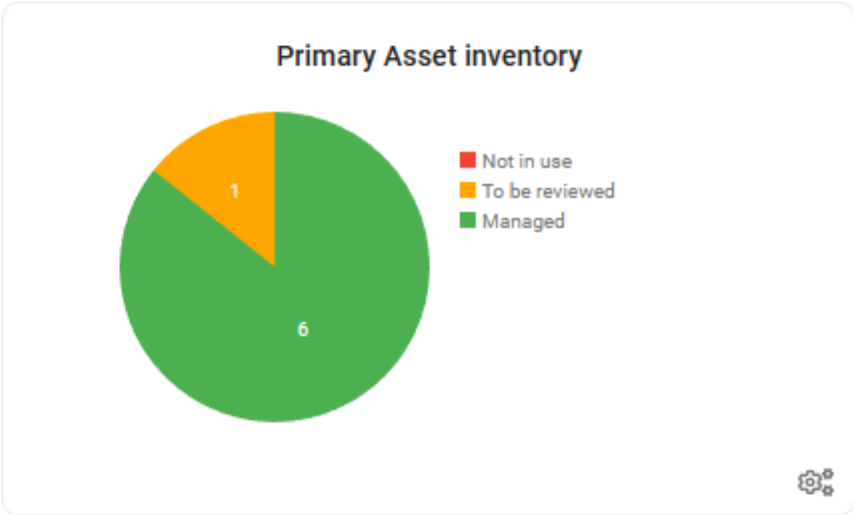
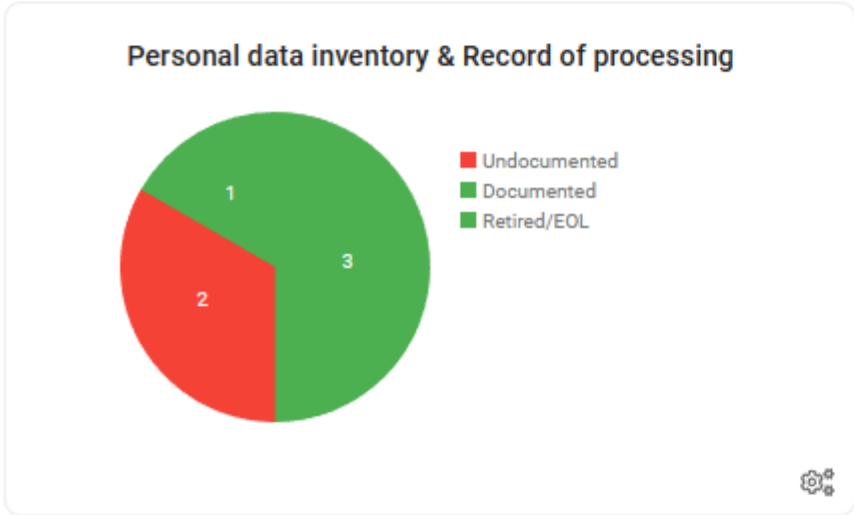
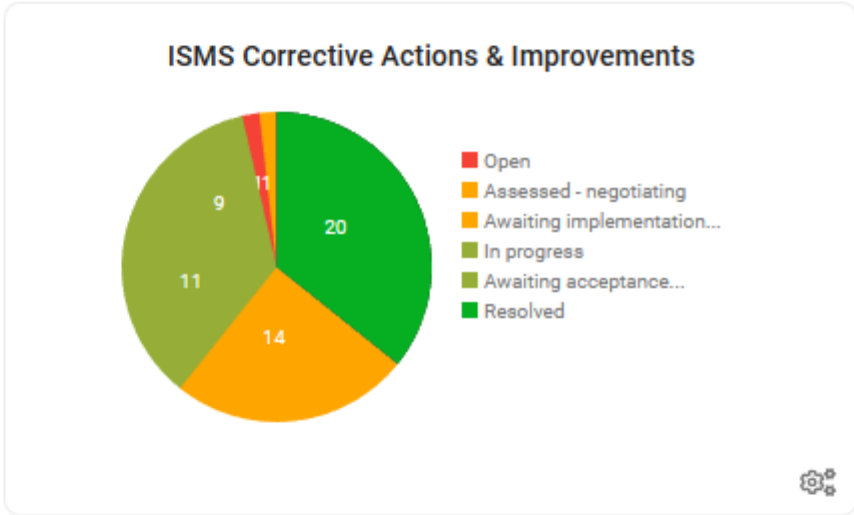
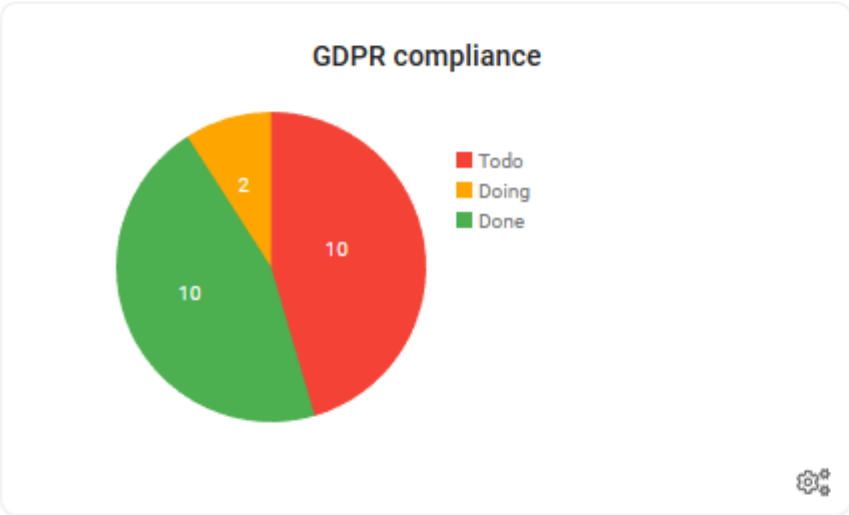
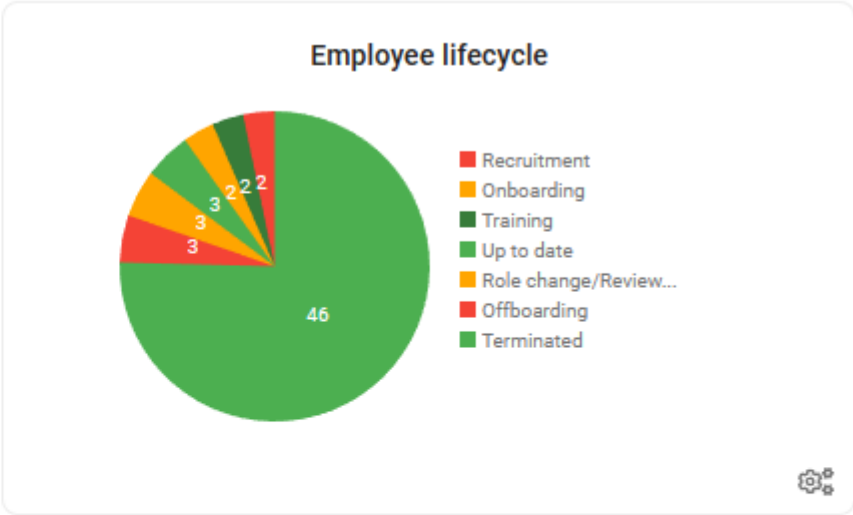
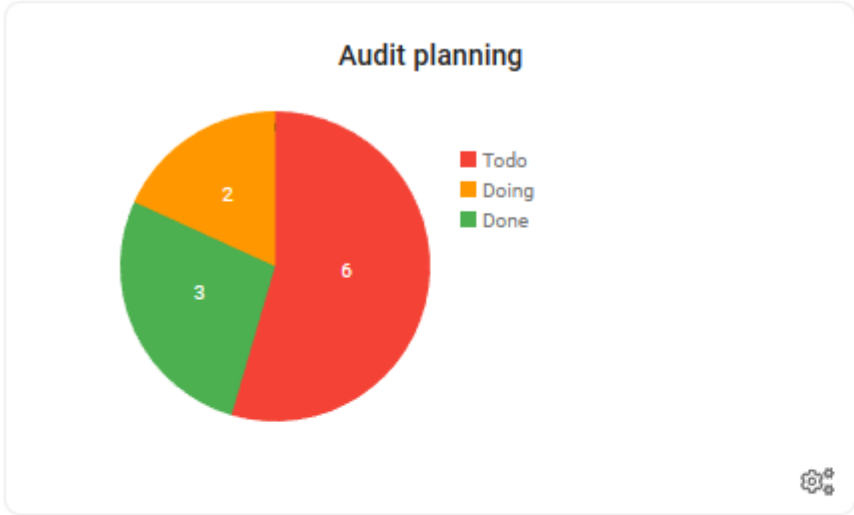
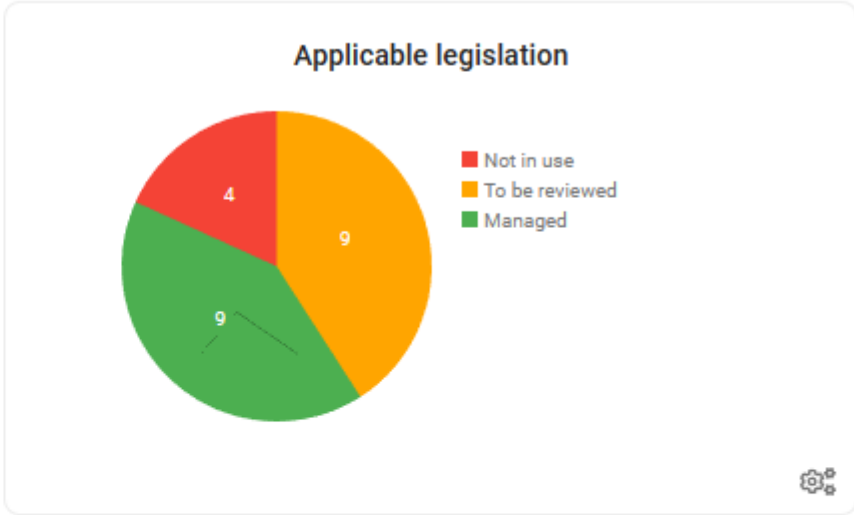
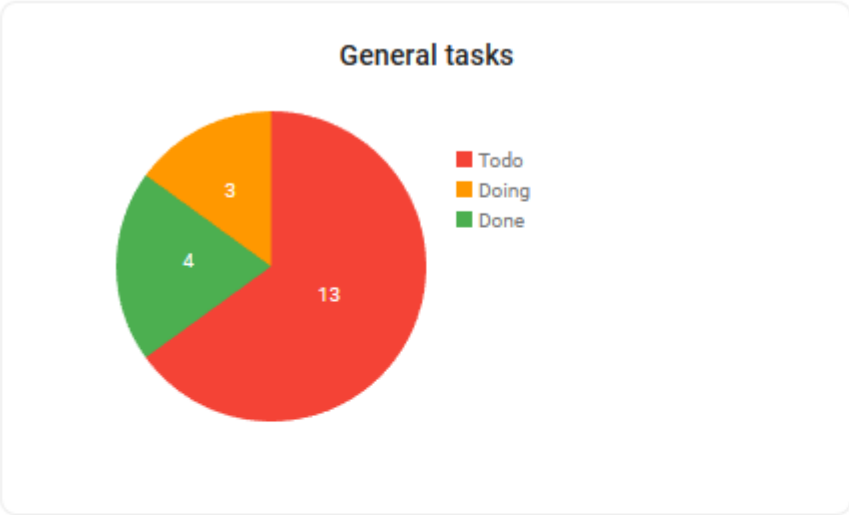
KANBAN BOARD

GANTT ROADMAPS

CHECKLISTS

REMINDERS

CheckList	November 2022																			December 2022																								
	02 Wed	03 Thu	04 Fri	05 Sat	06 Sun	07 Mon	08 Tue	09 Wed	10 Thu	11 Fri	12 Sat	13 Sun	14 Mon	15 Tue	16 Wed	17 Thu	18 Fri	19 Sat	20 Sun	21 Mon	22 Tue	23 Wed	24 Thu	25 Fri	26 Sat	27 Sun	28 Mon	29 Tue	30 Wed	01 Thu	02 Fri	03 Sat	04 Sun	05 Mon	06 Tue	07 Wed	08 Thu	09 Fri	10 Sat	11 Sun	12 Mon	13 Tue	14 Wed	15 Thu
	CAPA_50 - Synchronise clocks on aws with amazon																			CAPA_36 - The 'auto run				CAPA_44 - The wifi guest				CAPA_54 - SSID of WIFI				CAPA_35 - The tour												
	CAPA_27 - Workstations are not labeled																			C				CAPA_1 - Su				CAPA_34 - Put in place				CAPA_52 - Update Overv												
	CAPA_18 - Configurations like remote wipe, [...] defu																			CAPA_47 - There is no detailed BCP and tested DRP plan for tourist site																								
	CAPA_31 - The AWS ALBs use the																			C															CAPA_49 - Some applicab									



FINDINGS TRACKER

(Multi customer)

Todo (22)	Assessment (13)	Awaiting board approval (5)	Implementation (7)	Monitoring (2)	Resolved (5)
<div><div>22 - Tightly review source code permissions (gitlab)</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>55 - Document approved removable media devices (HD, USB, ...)</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>97 - Properly document company provided assets</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>77 - Access badges contain too much information</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>7 - Implement central password manager</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>22 - Tightly review source code permissions (gitlab)</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>83 - Identification of the regulatory requirements from stakeholders and regulatory bodies</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div>	<div><div>20 - Fix door locks (entrance Demo Group, back door and server room)</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>CAPA_102 - Install smoke detector in kitchen</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>16 - Check correct license management & create document to track</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>93 - Implement content security policy (CSP)</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>17 - Remove special user permissions Azure</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>91 - Automate change management process for developers</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>6 - Implement VLANs</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>95 - AWS IAM token rotation</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div>	<div><div>94 - Organise external pentest</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>50 - Install lockable file cabinets with fire protection for physical document protection</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>86 - Provide company workstations for staff that have access to sensitive data</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>33 - KPI - Implement Employee NPS evaluation</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>88 - More clear segregation of duties between ZT/DS</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div>	<div><div>21 - Ensure crowdstrike is installed on all workstations</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div><div>28/05/2021</div></div> <div><div>13 - Gap Audit - 3 - ISO27001/HDS - BCP planning + simulation of disaster</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div><div>31/08/2021</div></div> <div><div>18 - Ensure all devices are encrypted</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div><div>31/08/2021</div></div> <div><div>87 - Fully document roles and responsibilities and competencies</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>54 - Centralize logging from network security gateway into Datadog</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>31 - Vendor/Sub-contractor review pri</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>48 - Implement workstation conditional access</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div>	<div><div>37 - Hire IT manager for segregation of duties</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>19 - GDPR - Communication of HR/Payroll data per mail</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div>	<div><div>29 - Implement a SAST automated vulnerability scan</div><div>20 Jun - 31 Aug (72 days)</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>CAPA_52 - Implement software depende vulnerability scanner</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>67 - Gap Audit - ISO27001 - External entir interfaces and dependencies</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>8 - Ensure proper logging in ERP</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div> <div><div>81 - More clearly define ISMS business objectives and rational</div><div>ISMS Corrective Actions & Improvements</div><div>Carlo RICHMOND</div></div>

Non-conformity management

Search document type

- Audit report
- Core Business Service
- Corrective or preventive action (CAPA)**
- Disaster recovery plan (DRP)
- Exception form



BRAINFRAME

TECHNOLOGIES

Files Workbench Overview Assets Forms Timeline Risks KPIs Collections Distributions SoA Search

Identifier Title

CAPA_58 ✓ No audit planning in place

Create And Add To Workbench Create

Document Properties

Non-conformity type *

Minor Non-Conformity

Owner *

Add Employee

Add Consultant

DOCUMENT RISK KPI **PLANNING** REMINDER PROPERTY

✓ Add to workbench

Assign checklist for this document

ISMS Corrective Actions & Improvements

Current Kanban stage

Awaiting implementation

People assigned to this document

James Bond ×

☐ Show on timeline

Add Checklist

Planning See planning tab

Severity minor

Source Internal audit

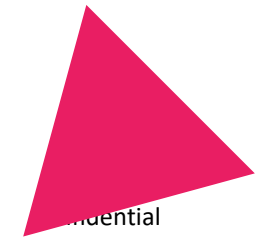
Article or reference of requirement causing the non-conformity A.18.2 Audit planning

Description of observed non-conformity or improvement

There are no frequent audits planned

Corrective action recommendation:

- Plan a yearly audit for ISMS policies & procedures in December
- Plan a 2 yearly GDPR audit (Jan/ July)





Task management



Workflows



Roadmaps & timeline

Internal audit planning

Search document type

Action to take

Audit report

Core Business Service

Corrective or preventive action (CAPA)

Disaster recovery plan (DRP)

CISO

Files Workbench Overview Assets Forms Timeline Risks KPIs Collections Distributions SoA Search

Kanban Tasks Table Include Subfolders Sort by deadline Only my tasks Show Other Workspace Filter tasks

Audit planning

Todo (5)

- AUD-2 - Initial ISO27001:2017 audit Stage 2
14 Nov - 16 Nov (2 days)
Audit planning
James Bond
16/11/2022
- AUD-3 - GDPR audit by DPO 2023
08 Jun - 09 Jun (1 days)
Audit planning
James Bond
09/06/2023
- Conduct internal audit
Audit planning
James Bond
01/09/2023
- Yearly Fiber consult audit
Audit planning
James Bond
10/02/2023
- AUD-4 - OWASP Pentest 2022 - tourist site and SkyPortPRO
27 Nov - 01 Dec (4 days)
Audit planning
James Bond
01/12/2022

Doing (1)

- Yearly external pentest audit on key applications
Audit planning
James Bond
01/09/2023

Done (3)

- Review of compliance with policies and procedures by managers
13 Oct - 21 Oct (8 days)
Audit planning
James Bond
21/10/2022
- AUD-1 ISO27001 Initial Blanc audit
26 Sep - 27 Sep (1 days)
Audit planning
James Bond
27/09/2022
- CISOMatic - ISO 27001 Rapport d'audit a blanc VD 10102022.docx
26 Sep - 27 Sep (1 days)
Audit planning
James Bond
27/09/2022

CISO

Files Workbench Overview Assets Forms Timeline Risks KPIs Collections Distributions SoA Search

Include Subfolders

	September 2022				October 2022				November 2022				December					
CheckList	04 - 10 Sun - Sa	11 - 17 Sun - Sa	18 - 24 Sun - Sa	25 - 01 Sun - Sa	02 - 09 Sun - Sa	10 - 16 Sun - Sa	17 - 23 Sun - Sa	24 - 30 Sun - Sa	01 - 07 Sun - Sa	08 - 14 Sun - Sa	15 - 21 Sun - Sa	22 - 28 Sun - Sa	29 - 05 Sun - Sa	06 - 12 Sun - Sa	13 - 19 Sun - Sa	20 - 26 Sun - Sa	27 - 03 Sun - Sa	04 - 10 Sun - Sa
Audit planning	<≡			■													AL	Now

Review of compliance with policies and procedures by managers from 2022-10-13 to 2022-10-21

Review

Visual roadmaps

CISO

Files Workbench Overview Assets Forms Timeline Risks KPIs Collections Distributions SoA Search

Please select checklist

General tasks

GDPR compliance

Applicable legislation

ISMS Corrective Actions & Improvements

CISO

Files Workbench Overview Assets Forms Timeline Risks KPIs Collections Distributions SoA Search

BRAIN FRAME TECHNOLOGIES CISOMatic Switch Workspace DA

Kanban Tasks Table Include Subfolders Sort by deadline Only my tasks Show Other Workspace Filter tasks

ISMS Corrective Actions & Improvements

Open (1)

Assessed - negotiating solution (2)

Awaiting implementation (15)

In progress (8)

Awaiting acceptance (11)

Resolved (20)

CAPA_52 - Update Overview on technical and organizational measures for data security acc. Art. 32 GDPR

CAPA_29 - No log-on banner is shown on bastion and worst case backup server informing the use of the device, [...] is for authorized users only

CAPA_51 - Missing Data Privacy by Design and Data Privacy by Default Documentation

CAPA_6 - There are no controls defined on closed risks/accepted risks (green)

CAPA_22 - Employees that are offboarded are not consistently reminded about their information security responsibilities

CAPA_12 - Several risks are flashing, indicating they have not received a timely risk reading according to the methodology

CAPA_34 - Put in place a formal maintenance log for key devices to ensure continued availability/integrity

CAPA_50 - Synchronise clocks on aws with amazon.pool.ntp.org

CAPA_27 - Workstations are not labeled

CAPA_18 - Configurations like remote wipe, [...] defined in POL-ALL-03 are not configured

CAPA_4

CAPA_5 - Multiple risks don't have enough details in the objective/treatment

CAPA_31 - The AWS ALBs use the ELBSecurityPolicy 2

CAPA_41 - Currently users have admin rights on their workstation

CAPA_32 - There is currently no central repository of public and private keys

CAPA_9 - There are no job description documents for the roles defined in the SoA

CAPA_40 - Formally document the review of administrator and operator

CAPA_55 - During the management of non-conformities, the analysis of the root cause is not documented

CAPA_24 - Primary and secondary SoA level of implementation needs to be updated

CAPA_6 - There are no controls defined on closed risks/accepted risks (green)

CAPA_7 - The SoA level of implementation needs to be updated

CAPA_36 - The 'auto run' is not configured

CAPA_1 - Surveys are not consistently reminded about their information security responsibilities

CAPA_44 - The wifi guest access is not configured

CAPA_54 - SSID of Wi-Fi is not configured

CAPA_34 - Put in place a formal maintenance log for key devices to ensure continued availability/integrity

CAPA_47 - There is no detailed BCP and tested DRP plan for tourist site

Timeline

October 2022

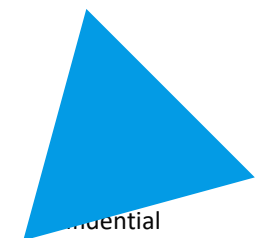
November 2022

December 2022



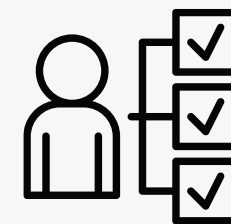
ONLINE FORMS

- Let others start your workflows/process & Stop running behind them
- Use your own Word documents in the form to start the flow
- Embed forms into your intranet





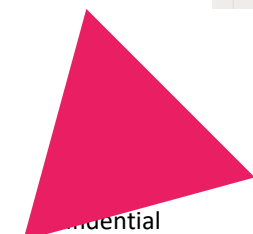
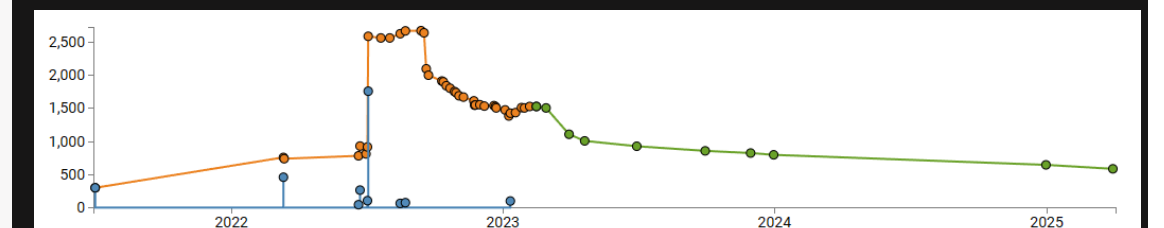
RISK ASSESSMENT & TREATMENT



Task management



Risk forecasting





Risk management – Threats & Vulns



Search document type

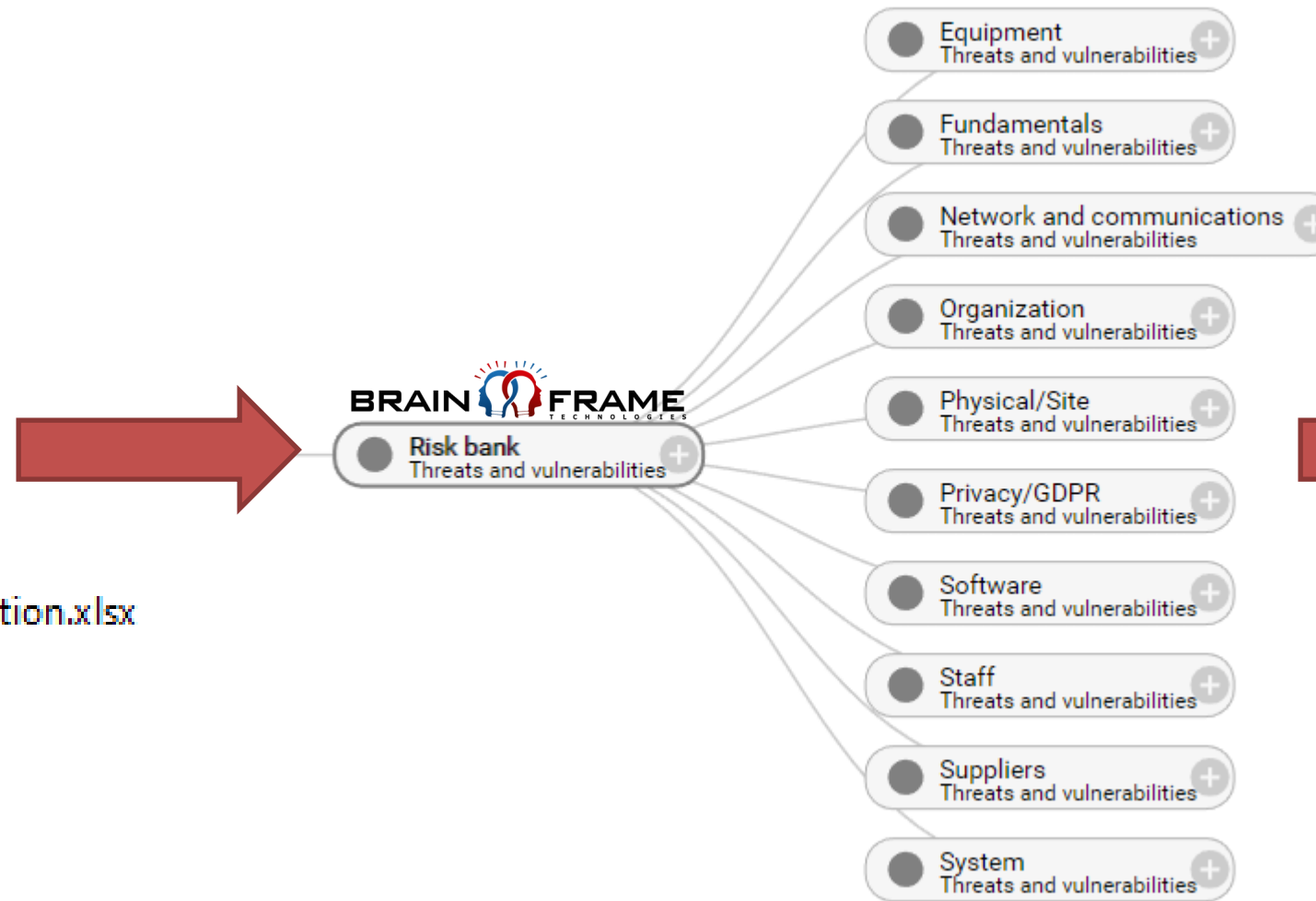
threat

Threat

Threat actor

No Data found

- Equipment.xlsx
- Network and Communication.xlsx
- Organization.xlsx
- Site.xlsx
- Software.xlsx
- Staff.xlsx
- System.xlsx
- Fundamentals.xlsx
- GDPR.xlsx



Privacy/GDPR

Threats and vulnerabilities

Create new document

All Threat (89)

Title Filter

Modified date

Lack of clauses for transfers to third countries not providing the appropriate level of protection	01/12/2022 08:44 am
Inadequate level of protection of the third country	01/12/2022 08:44 am
Absence of binding corporate rules	01/12/2022 08:44 am
Poor subcontracting conditions in cascade	01/12/2022 08:44 am
Poor cooperation with the controller	01/12/2022 08:44 am
Lack of contractual clauses between the controller and the processor	01/12/2022 08:44 am
Personal data are excessive in relation to the purpose of the processing	01/12/2022 08:44 am
Instructions from the controller are not documented	01/12/2022 08:44 am
The processor does not have sufficient guarantees to ensure data protection	01/12/2022 08:44 am
Poor subcontracting conditions in cascade	01/12/2022 08:44 am
Poor cooperation with the controller	01/12/2022 08:44 am
Lack of contractual clauses between the controller and the processor	01/12/2022 08:44 am
Personal data are excessive in relation to the purpose of the processing	01/12/2022 08:44 am
Instructions from the controller are not documented	01/12/2022 08:44 am



Risk management



Website snapshots

Vulnerabilities



Risks KPIs Collections Distributions SoA Search

Vulnhub
Threats and vulnerabilities

https://vuldb.com/

Add Website

URL of website
https://vuldb.com/?id.214609

We will make an image snapshot of the whole page and analyse its contents so you can easily find it back in the future

Cancel Create

All Vulnerability (2)

Title Filter

- CVE-2022-4135 | Microsoft Edge GPU heap-based overflow
- CVE-2022-1606 | M-Files Server privilege management

BRAINFRAME TECHNOLOGIES

CISO

Files Workbench Overview Assets Forms Timeline Risks KPIs Collections Distributions SoA Search

DOCUMENT RISK KPI PLANNING REMINDER PRO CVE-2022-4135 | Microsoft Edge GPU heap-based overflow

Latest Version... Assign Version 5 minutes ago

https://vuldb.com/?id.214612
A vulnerability was found in Microsoft Edge. It has been declared as critical. This vulnerability was named CVE-2022-4135. It is recommended to apply a patch to fix this issue.

MICROSOFT EDGE GPU HEAP-BASED OVERFLOW

Microsoft

CVSS Meta Temp Score	Current Exploit Price (~)	CTI Interest Score
6.0	\$5k-\$25k	3.80-

A vulnerability was found in Microsoft Edge (Web Browser) (the affected version is unknown). It has been declared as critical. This vulnerability affects some unknown processing of the component GPU. The manipulation with an unknown input leads to a heap-based overflow vulnerability. The CWE definition for the vulnerability is CWE-122. A heap overflow condition is a buffer overflow, where the buffer that can be overwritten is all located in the heap portion of memory, generally meaning that the buffer was allocated using a routine such as malloc(). As an impact it is known to affect confidentiality, integrity, and availability.

Vulnhub
Threats and vulnerabilities

https://vuldb.com/

Create new document

All Website (1)

Title Filter

CVE-2022-4135 | Microsoft Edge GPU heap-based overflow

Link Reminder Diagram Add Task Link/Move Archive Favorite



Risk management – Assessment

Title
Evaluation of HR Department

Create And Add To Workbench Create X

Physical assets Office USA (275) (Building, office or room) X

Personal data Employee salary details X

Threat No protection of equipment against theft (anti-theft cable) X

Threat actor External attacker X Employees X GDPR Supervisory authority X

Document Properties

Owner Add Employee Add Consultant

HR Manager X Add Role and responsibilities

3. Risk analysis

- ↑ Title Filter
- GDPR Supervisory authority
 - Employees
 - External attacker
 - Employee salary details

Search document type

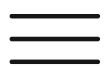
risk



- Business risk
- Confidentiality, integrity or availability Risk (CIA)
- Security risk assessment
- Legal risk

No Data found

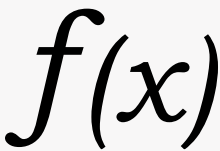
CISO: Security risk analysis						Technical/Development/CISO : Technical measures [T] to identified risks Business/CISO : Organizational measures [O] to identified risks				Business: Acceptance of risk residual	
Ref. risk	Risk scenario	Assets	Impacted criteria (CIAP)	Level of risk 1-25	CISO comments & recommendations	Risk reduction measures : « Technical » measures [T] « Organizational » measures [O]		Residual risk		Acceptation (accepted, refused, partially accepted)	Comments
						Description	Efficiency L/M/H	Residual severity 0/L/M/H	Description of the residual risk		
R-001											



KPI & OKR TRACKING



KPI OVERVIEW



COMPLEX FORMULA



TARGETS & TRENDS



Objectives & metrics - objectives

DOCUMENT RISK KPI PLANNING REMINDER PROPERTIES

Latest Version Assign Version 23 days ago Edit

Objectives and measures:
The objectives, measures and frequencies for measurement we have chosen below are business led, pragmatic and aim to deliver on one or more of the standards we have chosen to apply. The table below sets out the headline information:

Objective	Measure	Target	Frequency	Owner	Source and Evidence
High web service availability	% Availability of frontend and backend combined.	>= 99.5%	Monthly	CTO	Web service availability KPI-WEBUP
Secure Workstations	% of compliant workstations - Encryption enabled - Antivirus enabled - Admin rights removed - No software with critical/high vulnerabilities - Firewall enabled - Onboarded in MDM with applied policies	>=90%	Monthly	IT Manager	Secure workstations KPI-SECWS
Good cloud infrastructure security score	% security score on AWS security hub	>=80%	Monthly	CTO	Good security posture KPI-SECPOS
Security/Privacy awareness training for all staff	% of staff that received both security and privacy training on https://compliance-center.eu/	100% after 1 month	Monthly	CISO	Security/Privacy awareness training KPI-AWAR
No privacy/security incidents	Count of newly opened privacy/security incidents	0 incidents	Monthly	CISO	No privacy/security incidents KPI-INC
No important vulnerabilities - Elitrix	Count of unresolved 'critical' and 'high' vulnerabilities in snyk	<10	Monthly	CTO	No important vulnerabilities - Elitrix KPI-GWVULN
No important vulnerabilities - Infrastructure	Count of unresolved 'critical' and 'high' vulnerabilities in snyk	<10	Monthly	CTO	No important vulnerabilities - Infrastructure KPI-INFRAVULN

KPIs ISMS

Search document type
kpi

Service availability KPI
Business Objective KPI
Security objective KPI
Privacy objective KPI
Quality Objective KPI

Link Reminder Diagram Ac

Identifier Title

Create And Add To Workbench Create

Owner Add Employee
Add Consultant
Add Role and responsibilities

Objective description

Objective identifier	
Objective description	
Objective target	e.g. 100%
Objective measurement instructions	e.g. (count of done/count of planned)*100
Frequency of objective measurement	Daily/Weekly/Monthly/Quarterly/Yearly
Link to Mission/Vision	Describe how this objective supports the company mission/vision
Objective owner	Person responsible for obtaining this objective
Stakeholders	Key people or groups impacted by this objective

DOCUMENT RISK KPI PLANNING REMINDER PROPERTIES

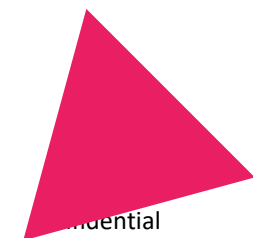
Users to be reminded
Brandon Walrof

When to send reminder

Recurring reminder

2022-12-01

Repeat every: 1 Select duration
Month





Objectives & metrics - readings

↑ Title

- KPI-GWVULN No important vulnerabilities - Elitrixs
- KPI-SOAVULN No important vulnerabilities - SOA/tools
- KPI-VIDVULN No important vulnerabilities - Fiber consultation
- KPI-SANVULN No important vulnerabilities - Clearview
- KPI-ONBVULN No important vulnerabilities - Onboarding tool
- KPI-CPPVULN No important vulnerabilities - tourist site**
- KPI-PROVULN No important vulnerabilities - CISOMatic PRO
- KPI-INFRAVULN No important vulnerabilities - Infrastructure

Link Reminder Diagram Add Task Link/Move Archive Favorite Distribute **KPI reading** Risk

Add Reading - (KPI-CPPVULN-No important vulnerabilities - tourist site)

- Weather prediction
- Unit tracking**
- Financial tracking
- Percentage tracking
- Service availability percentage

Measure name	Value
Units	<input type="text" value="Enter Value (Number)"/>
	<input type="text" value="17"/>

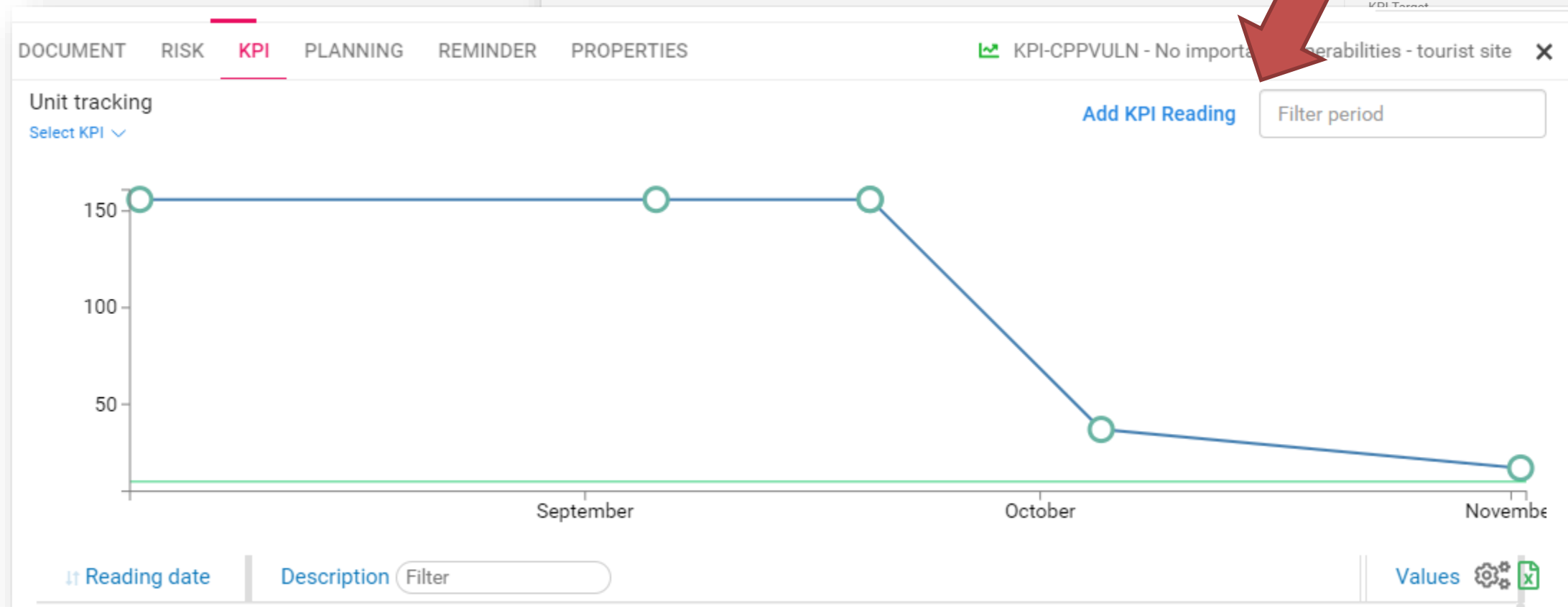
Reading Result

Formula: Units

Calculation: 17 = 17.00

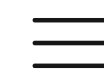
Information/remarks on this measurement

KPI Target





Objectives & metrics – overview & trends



CISO							
Files Workbench Overview Assets Forms Timeline Risks KPIs Collections Distributions SoA Search							
KPIS							
↑↓ KPI Name	↑↓ KPI Type	KPI Type Description	KPI target	Last reading	↑↓ Last reading date	Trend	Document properties
No important vulnerabilities - Infrastructure	Unit tracking	Track the unit progress	10	90.00	01/11/2022 03:04 PM	Stable	Owner: Chief Technology Officer - CTO
No important vulnerabilities - CISOMatic PRO	Unit tracking	Track the unit progress	10	15.00	01/11/2022 03:02 PM	Decreasing	Owner: Chief Technology Officer - CTO
No important vulnerabilities - tourist site	Unit tracking	Track the unit progress	10	17.00	01/11/2022 03:00 PM	Decreasing	Owner: Chief Technology Officer - CTO
No important vulnerabilities - Onboarding tool	Unit tracking	Track the unit progress	10	6.00	01/11/2022 02:59 PM	Decreasing	Owner: Chief Technology Officer - CTO
No important vulnerabilities - Clearview	Unit tracking	Track the unit progress	10	47.00	01/11/2022 02:58 PM	Decreasing	Owner: Chief Technology Officer - CTO
No important vulnerabilities - Fiber consultation	Unit tracking	Track the unit progress	10	11.00	01/11/2022 02:56 PM	Increasing	Owner: Chief Technology Officer - CTO
No important vulnerabilities - SOA/tools	Unit tracking	Track the unit progress	10	186.00	01/11/2022 02:55 PM	Decreasing	Owner: Chief Technology Officer - CTO
No important vulnerabilities - Elitrixs	Unit tracking	Track the unit progress	10	56.00	01/11/2022 02:51 PM	Decreasing	Owner: Chief Technology Officer - CTO

DOCUMENT DISTRIBUTION



- Send your policies & procedures to staff & suppliers per mail for online review
- Get auditable approval per document
- Central progress tracking

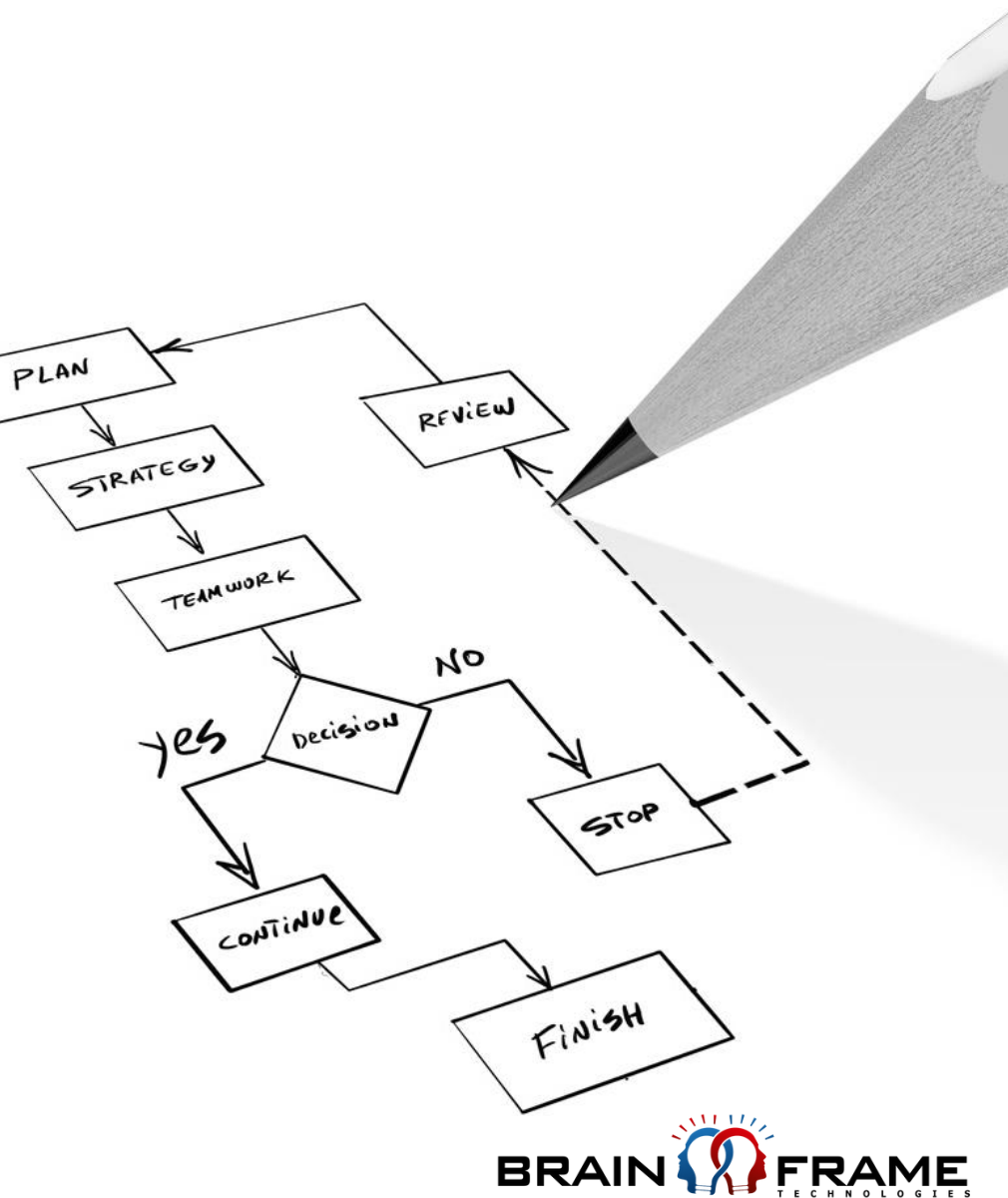


DIAGRAM EDITOR

- Quickly draw any process/flow
- Track diagram versions
- No more external tools



Roadmap

- AI powered document generation (policies, procedures, configuration recommendations)
- AI powered risk assessment
- Business continuity management
- External risk tool integration
- SIEM & ITSM integrations

And anything you consider important can be added to our roadmap!

Brainframe = Your local digitalization partner



OUR CONTACT

+352 27867914

WWW.BRAINFRAME.COM

INFO@BRAINFRAME.COM

Junglinster, Luxembourg

