

BRAIN FRAME

Affordable Expert GRC Value – Flexible & Community Driven

WWW.BRAINFRA.ME.COM

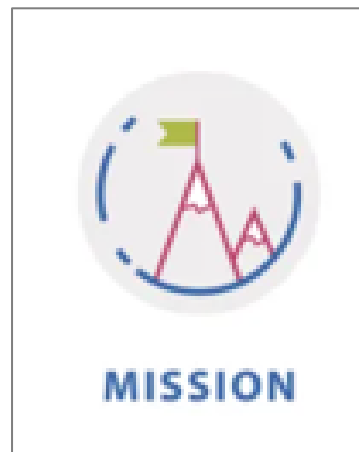
Who is Brainframe?

CONCEPTION



Brainframe started as a one-man project in Luxemburg to devise an **inexpensive solution to effectively counter** the typically expensive and complex-process driven solutions for the digital enterprise.

With the driving force of a **recognized GRC expert and CISO** - seeing how enterprises are increasingly impacted by expanding regulations and cyber risks – the Brainframe solution constantly provides proof to **be highly cost-effective with intuitive usage and automation concepts** for an entire organization.



MISSION STATEMENT

We are **democratizing GRC** by making it available to any size company and **digitalize, centralize and remove all inefficiencies in security, compliance and regulatory work** while bringing companies, consultants and suppliers closer together in an **all-in-one management** platform to **optimize the work of the limited specialists on the market**.

BRAINFRAME EVOLUTION

Today, Brainframe has a **dedicated R&D team and deployment services and consultancy force**.



The **Brainframe GRC SaaS platform** is a successful reference solution for both consultants and end-customers alike, with a **zero-churn** and a strongly growing customer base in the IT services and GRC domains.

With continuous **expert user** influenced improvements from an **operational user community and customer closed loop feedback**, the focus is always on offering direct value via a pragmatic cost-efficient software deployment.

This approach allows to **include AI and GRC 5.0 technical evolutions** to stay on the crest of the digitalization wave.

Agenda



Brainframe Understands your GRC Challenges



Insufficient GRC specialists

- **Expensive** to keep competency internally/train new people/align with existing work
 - General move to “**As a service/consultants**”

Inefficient GRC work

- **Loss of time** reinventing the wheel, duplicating work and missing best practices.
- **Lack of standardisation** in tools & content to be efficient (prevents JIT support)
- **Lack of knowledge retention** (on avg. people stay 2-3y)
- GRC Specialists should **focus on actions, not documentation**

Lack of visibility in assets & risks

- **Missing Primary/supporting asset identification and documentation**
- **Missing Business requirements (RTO/RPO/...)**
- **Missing view on dependencies** between assets, risks and incidents
- **Increasing (cyber) risks** are not identified/quantified/managed

Task management

- Difficult to decide **what work to prioritize and how to follow up**

Regulatory pressure

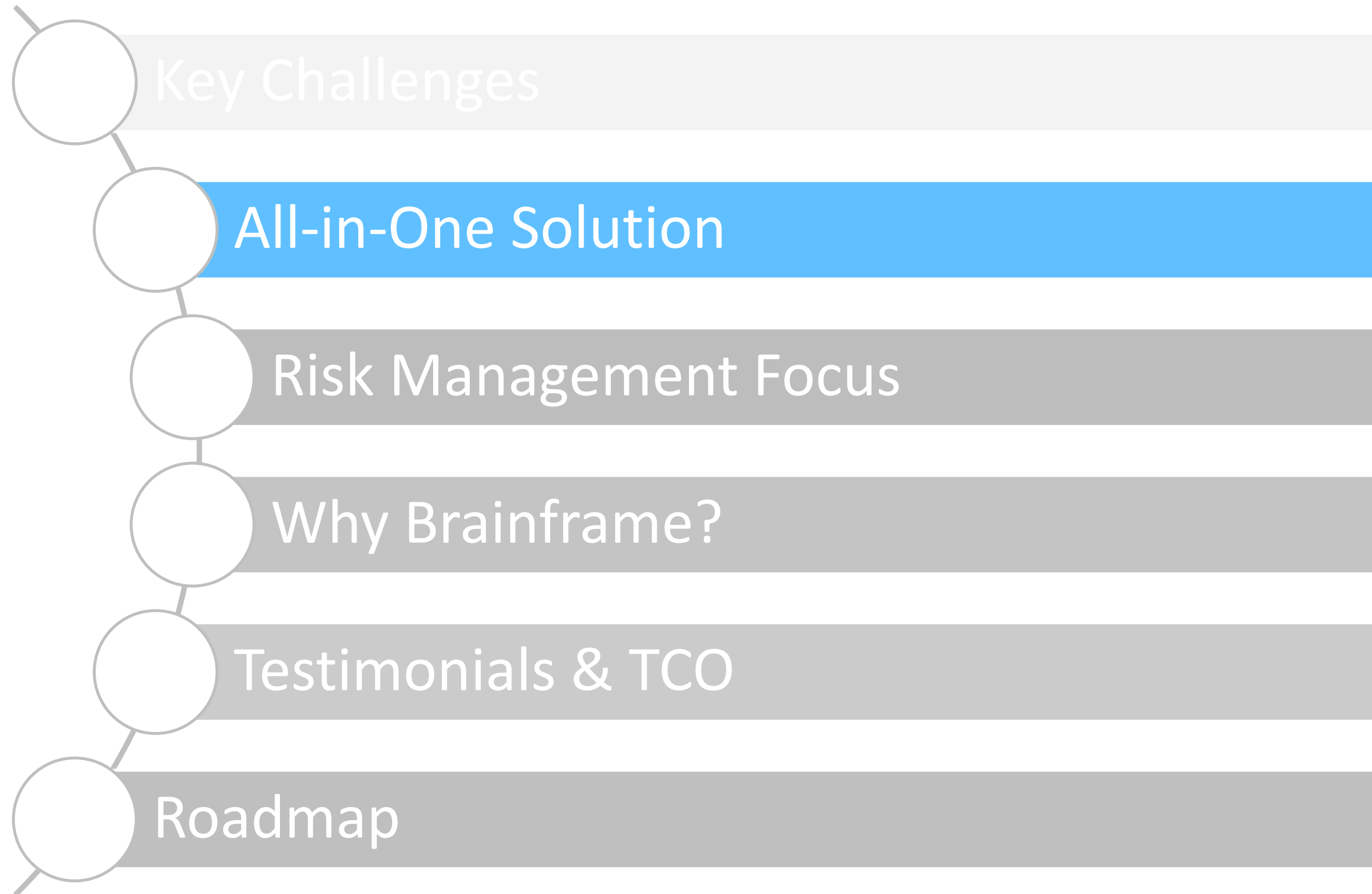
- Higher pressure from boards due to **Risk of big fines/permit loss**
- Missing **standardisation for auditing/reporting**

DORA, NIS2:

10X

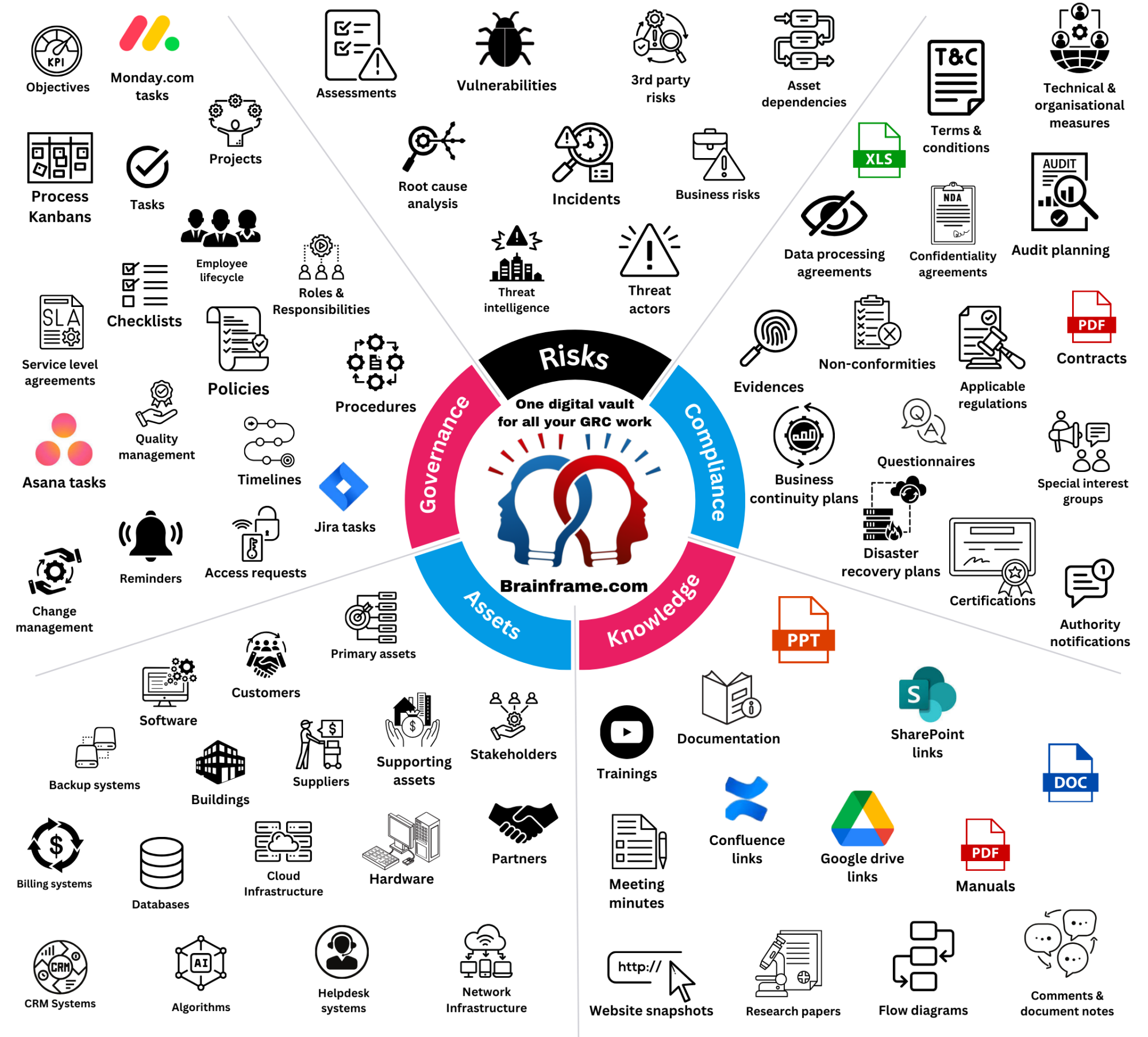
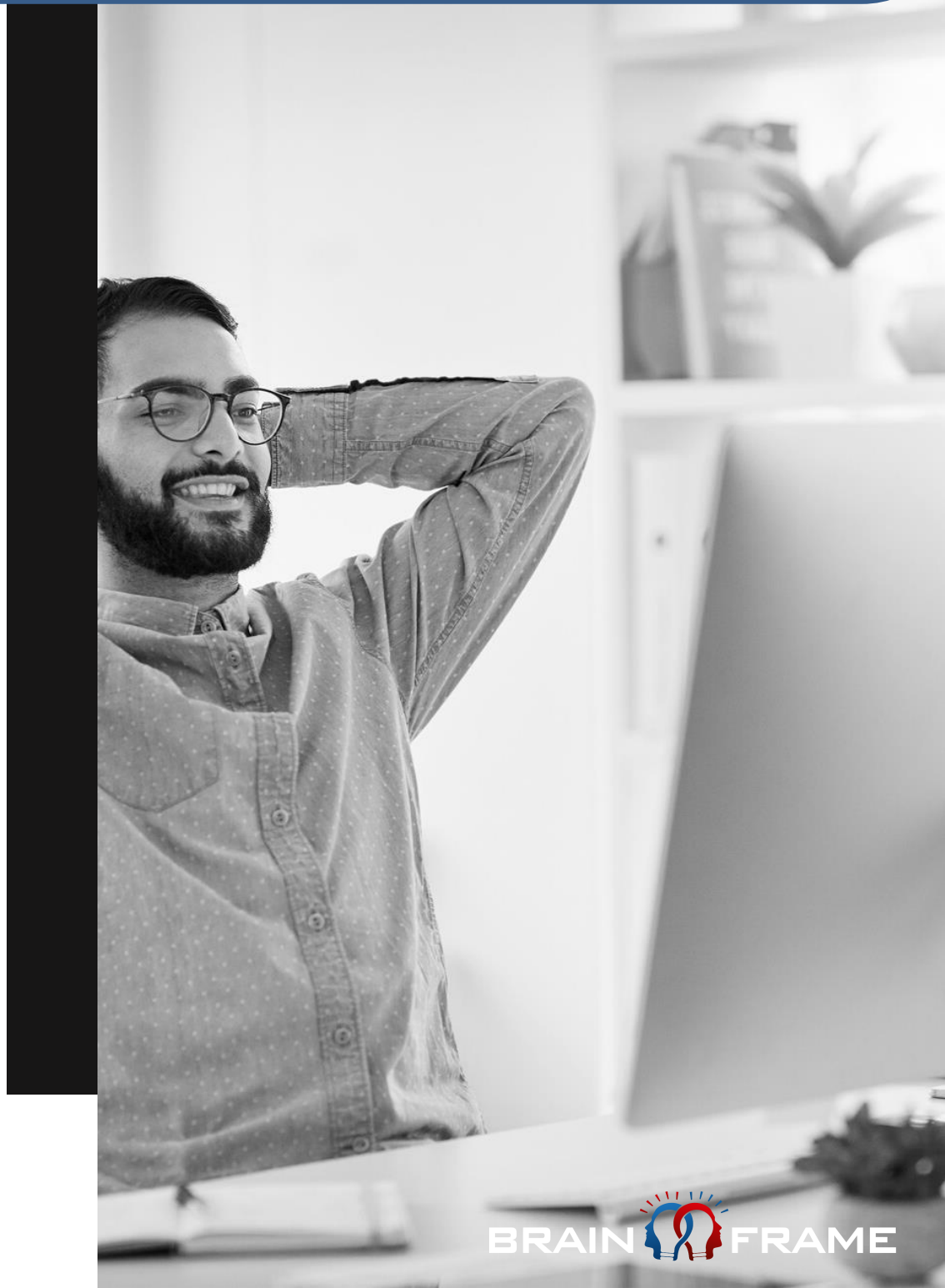


Agenda



One digital vault for all your GRC work

Document management Asset management



All-in-One Solution

A first of its kind **management solution** combining **ISMS, GRC, AMT, QMS and DMS** in one single **platform** for an efficient establishment, implementation, maintenance, collaboration, certification and continuous improvement of **any framework, regulation or standard** with quick access to **trusted specialists**.

A **modular** platform that can effortlessly **scale out** in both **volume and functional scope** dimensions.

SAVE TIME (SAVE MONEY)

Due to all-in-one digitalization

INCREASE OUTPUT

More with fewer resources

REDUCE RISKS

With central context and asset aware views

WWW.**BRAIN FRAME**.COM
TECHNOLOGIES

Document management	Versions & approvals	Document templates
Asset management	Risk management	Requirement mapping
Task management	Workflows	Request forms
Roadmaps & timeline	Objectives tracker	Maturity tracker
Document distribution	Diagram editor	Dependency tracker
Website snapshots	Multi customer/entity	●●● Much more...

SaaS Delivery - In the cloud or self-hosted

ISO27001, DORA & NIS(2) Coverage

1.Document Management: Aligns with regulatory requirements for maintaining, organizing, and retrieving critical documents efficiently. We help track document changes, maturity, formal approvals, reminders and notifications to relevant stakeholders.

Using our easy document template features, you can comply with the requirements for standardizations in all domains,

2.Task Management: Facilitates systematic task assignment, ownership and tracking of work on any control, asset, supplier, risk or non-conformity. Combined with integrations in JIRA, Asana, Monday.com you get a focused view on all relevant risk reduction work.

3.Process Management: Enables the design, execution, and monitoring of business processes for transparent and efficient process management per department/product line. Combined with the process-driven residual risk management we give you an unprecedented contextual view on your suppliers, employees, stakeholders, non-conformities, risks and applicable legislations.

4.Inventory Overview: Offers an immediate listing of all document types (asset types, policies, procedures, employees, roles and responsibilities, contracts/DPAs/NDAs, suppliers, vulnerabilities ...), that can be provided to Authorities when requested.

5.Asset Management: Assists in centrally cataloging your primary asset and their supporting assets, responsibility/accountability, related risks and non-conformities and business requirements (CIA, RTO, RPO, Privacy requirements, ...)

6.Request Forms: Simplifies following process for your staff, customers and suppliers by capturing process data with notifications to relevant stakeholders. Due to its deep integration to the risk module, we automate the initial risk evaluation process based on form questions and replies that map to the risk reading.

7.Roadmaps/Timeline: Visualizes strategic goals and milestones, aiding organizations in meeting regulatory requirements for clear, strategic planning and milestone tracking. This includes the audit planning, risk reduction and non-conformity treatment plans as well as any other work you planned.

8.Risk Management: Significantly accelerates the management and mitigation of risks per departments/product line with easy risk documentation, prioritization, timely review tracking, risk evolution in time and risk reduction based on planning mitigations.

9.Objectives Tracker (KPIs): Monitors and facilitates key performance tracking for different stakeholders with a central overview per department/product line.

10.Dependency Tracking: Provides visual and automatic insights into how assets, processes, suppliers, risks, non-conformities and controls are linked together.

11.Document Distribution: Automates distribution of documents to stakeholders and employees with collection of proof for “Read and understood”. This module can also be used to host and collect evidence of your department specific trainings and procedures using of video, PowerPoint, PDF and other materials.

12.Requirement/Maturity Mapping (SOA): Maps controls to requirements and tracks compliance frameworks' maturity. Thanks to its deep integration with the task manager and evidence collection, you can quickly show your progress and highly improve your efficiency during audits,

13.Diagram Editor: The build in editor allows you to draw and instantly store different version of your different process flows

14.Website snapshots: Quickly capture any website (terms, vulnerability, documentation, ...) and link it to your suppliers, risks or other investigative work

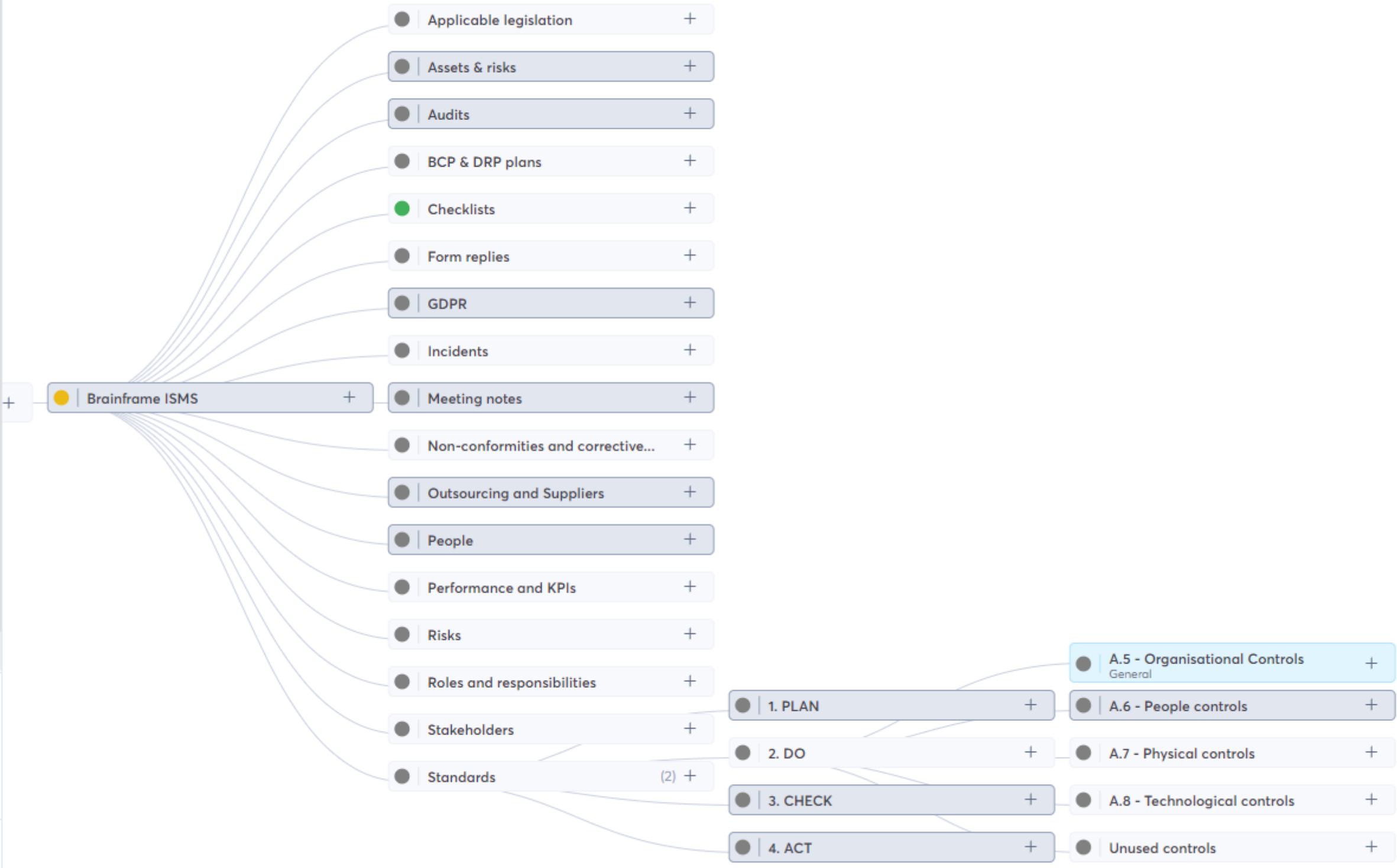
15.Multi Entity Management: Keep common data centralized (e.g. policies) with “golden documents” that update in all workspaces, while fully isolating entity specific work in dedicated workspaces. On governance level you can manage who can access which parts of your different workspaces for full control



User interface

Search

- Files
- Tasks
- Workbench
- Overview
- Primary assets
- Vendors
- Forms
- Timeline
- Risks
- KPIs
- Collections
- Distributions
- SoA
- Ideas/Roadmap
- Profile
- Settings
- Logout



NEW A.5 - Organisational Controls
General

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. (e.g. important contacts,, breach procedures, acceptable use data handling, threat intelligence, Project Classification, data protection, access control, identity...

[Convert To Note](#)

All Policy (25) Procedure (46)

TITLE ↓	Filter	MODIFIED DATE ↓
is-policy - Employee Handbook and Policy Quick Reference		06/06/2024 10:21 pr
cp-risk-mgmt - Risk Management Process		06/06/2024 12:13 pr
cp-risk-mitigation - Risk Mitigation and Monitoring		06/06/2024 11:43 ar
Business Risk Assessment and Treatment Methodology.docx		06/06/2024 11:24 ar
cp-risk-assess - Risk Assessment and Analysis		06/06/2024 11:08 ar
cp-risk-registry - Risk Registry		05/06/2024 09:47 p
cp-risk-mgmt-objectives - Risk Management Objectives		05/06/2024 09:41 pi
sdlc - Secure Product		

User interface

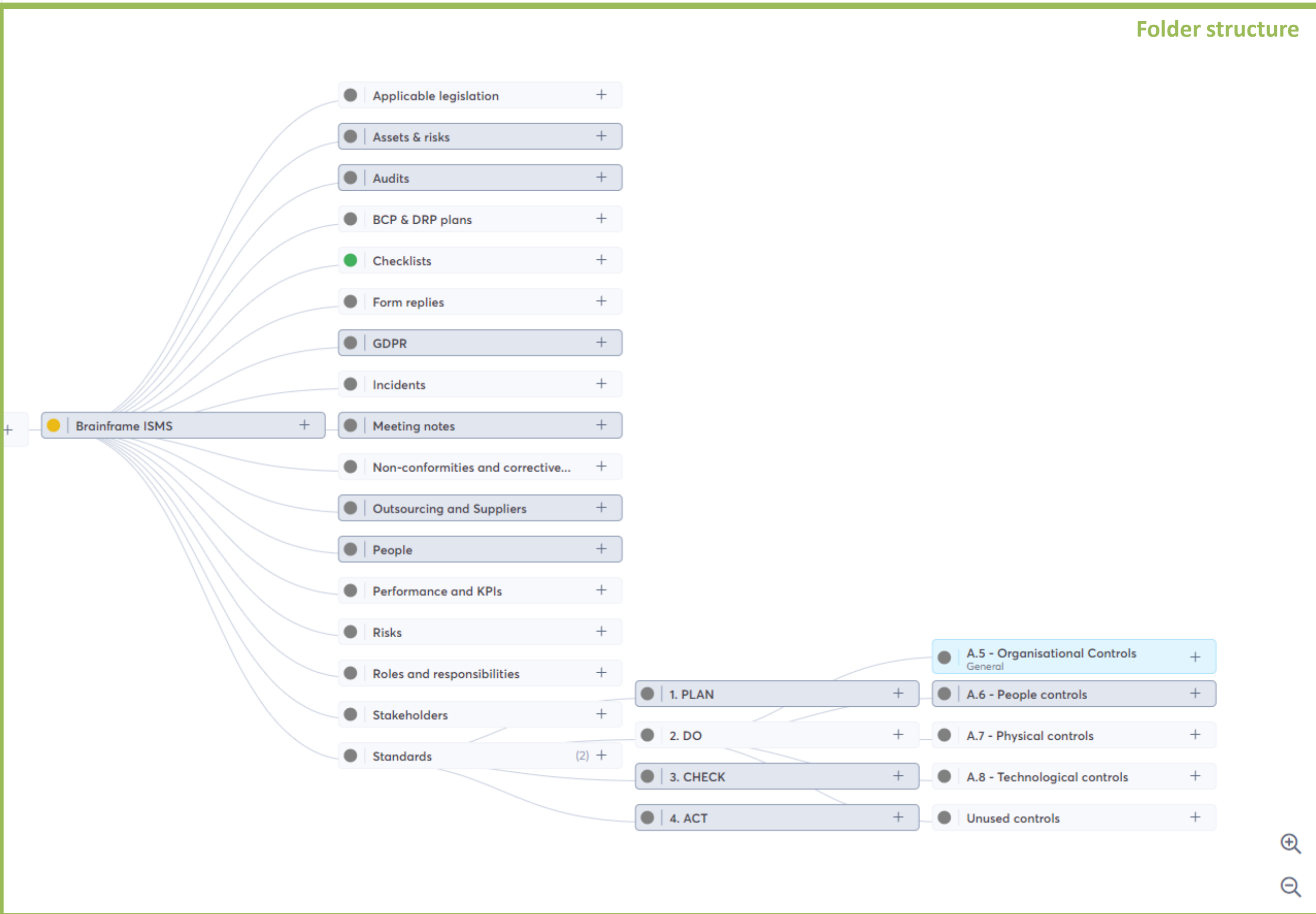
The screenshot displays the Brainframe ISMS user interface. On the left is a navigation menu with sections for 'Modules' (Files, Tasks, Workbench, Overview, Primary assets, Vendors, Forms, Timeline, Risks, KPIs, Collections, Distributions, SoA) and user settings (Ideas/Roadmap, Profile, Settings, Logout). The main area features a central diagram with 'Brainframe ISMS' at the center, branching into 'Standards' (1. PLAN, 2. DO, 3. CHECK, 4. ACT) and various control categories (Applicable legislation, Assets & risks, Audits, BCP & DRP plans, Checklists, Form replies, GDPR, Incidents, Meeting notes, Non-conformities and corrective..., Outsourcing and Suppliers, People, Performance and KPIs, Risks, Roles and responsibilities, Stakeholders). The right panel shows a document editor for 'A.5 - Organisational Controls' with a rich text editor and a table of documents.

TITLE	MODIFIED DATE
is-policy - Employee Handbook and Policy Quick Reference	06/06/2024 10:21 pr
cp-risk-mgmt - Risk Management Process	06/06/2024 12:13 pr
cp-risk-mitigation - Risk Mitigation and Monitoring	06/06/2024 11:43 ar
Business Risk Assessment and Treatment Methodology.docx	06/06/2024 11:24 ar
cp-risk-assess - Risk Assessment and Analysis	06/06/2024 11:08 ar
cp-risk-registry - Risk Registry	05/06/2024 09:47 p
cp-risk-mgmt-objectives - Risk Management Objectives	05/06/2024 09:41 pi
sdlc - Secure Product	

User interface – Document management

Search

- Files
- Tasks
- Workbench
- Overview
- Primary assets
- Vendors
- Forms
- Timeline
- Risks
- KPIs
- Collections
- Distributions
- SoA
- Ideas/Roadmap
- Profile
- Settings
- Logout



Folder structure

NEW A.5 - Organisational Controls
 General +

Rich text editor toolbar: Bold, Italic, Underline, Text color, Background color, Bulleted list, Numbered list, Indent, Link, Unlink, Insert.

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. (e.g. important contacts,, breach procedures, acceptable use data handling, threat intelligence, Project Classification, data protection, access control, identity...

[Convert To Note](#)

Filter: All | Policy (25) | Procedure (46)

TITLE ↓	Filter	MODIFIED DATE ↓
is-policy - Employee Handbook and Policy Quick Reference		06/06/2024 10:21 pr
cp-risk-mgmt - Risk Management Process		06/06/2024 12:13 pr
cp-risk-mitigation - Risk Mitigation and Monitoring		06/06/2024 11:43 ar
Business Risk Assessment and Treatment Methodology.docx		06/06/2024 11:24 ar
cp-risk-assess - Risk Assessment and Analysis		06/06/2024 11:08 ar
cp-risk-registry - Risk Registry		05/06/2024 09:47 p
cp-risk-mgmt-objectives - Risk Management Objectives		05/06/2024 09:41 pi
sdlc - Secure Product		

User interface – Document management

The screenshot displays the Brainframe ISMS user interface. On the left is a navigation sidebar with options like Files, Tasks, Workbench, Overview, Primary assets, Vendors, Forms, Timeline, Risks, KPIs, Collections, Distributions, SoA, Ideas/Roadmap, Profile, Settings, and Logout. The main area shows a hierarchical tree structure under 'Brainframe ISMS', including categories like 'Applicable legislation', 'Assets & risks', 'Audits', 'BCP & DRP plans', 'Checklists', 'Form replies', 'GDPR', 'Incidents', 'Meeting notes', 'Non-conformities and corrective...', 'Outsourcing and Suppliers', 'People', 'Performance and KPIs', 'Risks', 'Roles and responsibilities', 'Stakeholders', and 'Standards'. The 'Standards' category is expanded to show '1. PLAN', '2. DO', '3. CHECK', and '4. ACT'. Under '2. DO', the folder 'A.5 - Organisational Controls' is highlighted with a green box. To the right, a detailed view of this folder is shown, titled 'A.5 - Organisational Controls' with a 'General' tab. It includes a rich text editor with a 'Convert To Note' button and a table of documents. A green arrow points from the folder in the tree to this detailed view.

Folder content

NEW A.5 - Organisational Controls
General

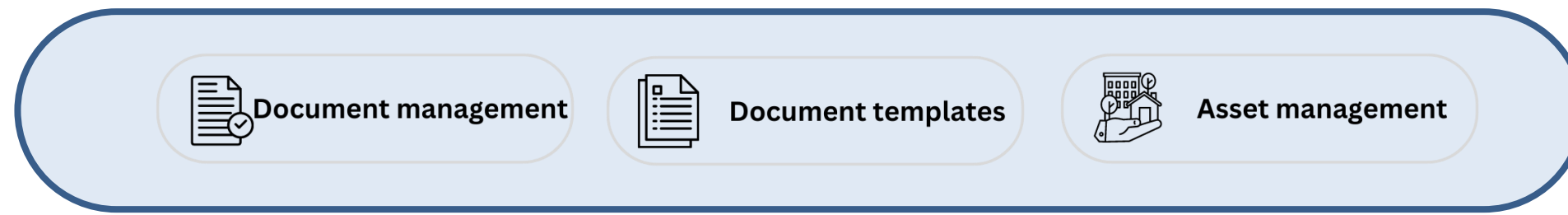
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. (e.g. important contacts,, breach procedures, acceptable use data handling, threat intelligence, Project Classification, data protection, access control, identity

Convert To Note

All Policy (25) Procedure (46)

TITLE ↓	Filter	MODIFIED DATE ↓
is-policy - Employee Handbook and Policy Quick Reference		06/06/2024 10:21 pr
cp-risk-mgmt - Risk Management Process		06/06/2024 12:13 pr
cp-risk-mitigation - Risk Mitigation and Monitoring		06/06/2024 11:43 ar
Business Risk Assessment and Treatment Methodology.docx		06/06/2024 11:24 ar
cp-risk-assess - Risk Assessment and Analysis		06/06/2024 11:08 ar
cp-risk-registry - Risk Registry		05/06/2024 09:47 p
cp-risk-mgmt-objectives - Risk Management Objectives		05/06/2024 09:41 pi
sdic - Secure Product		

Standardize your Compliance Work



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
Decision	Guideline	Vulnerability	Cloud SaaS Product/Service	Intrusion detection system (IDS)	Technology	Physical asset	Regulation, Legislation or standard
Department or Working group	ISMS Management review meeting	Controller(s) of the data	Company landing page or portal	Mobile app	Webservice	Physical firewall	Regulatory exemption

Policies

More than 40 ready to use policies aligned with ISO 27001:2022

Employee Handbook and Policy Quick Manual:

- Third Party Security, Vendor Risk Management and Systems/Services Acquisition Policy
- Configuration and Change Management Policy
- System Audits, Monitoring and Assessments Policy
- Asset Inventory Management Policy
- Facility Access and Physical Security Policy
- Vulnerability Management
- Compliance Audits and External Communications Policy
- HR and Personnel Security Policy
- Roles, Responsibilities and Training Policy
- Employee Handbook and Policy Quick Reference
- Privacy Policy
- Corporate Governance Policy
- Business Continuity and Disaster Recovery Policy
- Secure Product Development and Product Security
- Incident Response Policy
- Breach Investigation and Notification Policy
- Management Policy
- Cookie Policy
- Privacy and Consent Policy
- Mobile Device Security and Storage Media Management Policy
- Data Management Policy
- Threat Detection and Prevention Policy
- Access Policy
- Risk Management Policy
- Data Protection Policy

Procedures

More than 145 ready to use procedures aligned with ISO 27001:2022

- Threat Intelligence Monitoring
- Training, Education, Awareness and Responsibilities
- Understanding the Policies and Documents
- Use of USB Flash Drive and External Storage Device
- Emergency Change
- Acceptable Use of End-user Computing
- Assignment of Roles and the Security Committee
- Metrics, Measurements and Continuous Monitoring
- Policy and Compliance Training
- Production Data Access
- Digital Asset Inventory
- Dynamic Application Security Testing
- Encryption Key Management
- Free and Open Source Software (FOSS) Security.
- Employee Onboarding Procedures
- Employee Performance Review Process
- Employee Screening Procedures
- Employee Workstation / Endpoints Access and Usage
- Fraud Risks
- Non-Compliance Investigation and Sanctions
- Ongoing Awareness Training
- Outsourced Software Development
- Physical Asset Inventory
- Physical Security
- Policies and Controls Framework
- Policy Management Process
- Privacy Policy
- Production Deploy / Code Promotion Processes
- Production Environments and Data Recovery
- Production System Monitoring and Paging
- Production Systems Provisioning
- Protecting Data At Rest
- Provisioning AWS Accounts
- Quality of Service
- Remediation of Control Deficiencies
- Access to PHI/ePHI
- HR Management and Reporting
- Incident Categories and Playbooks
- Incident Management Process
- Incident Tracking and Records
- Information Security Program and Scope
- Internal Business Communications
- Internal/Manual Auditing Activities
- Requesting Audit and Compliance Reports
- Review and Reporting of Audit Findings
- Security Architecture
- Security Findings Reporting, Tracking and Remediation
- Security Principles
- Risk Management Process
- Security Program Overview
- Sample Letter to Customers in Case of Breach
- Employee Exiting/Termination Procedures
- Employee Issue Escalation
- Stakeholder overview
- List of Contacts for Authorities
- Whistleblower Policy and Process
- Work Site Recovery
- Vendor Contractual Agreements
- Audit Trails and Application Security Events Logging Standard
- Audit Trail Integrity
- Data Deletion
- Automated change management for deploys to AWS
- Backup and Recovery
- Configuration and Management of Network Controls
- Configuration and Provisioning of Management Systems
- Configuration Management Processes
- Configuration Monitoring and Auditing
- Data Integrity Protection
- Data Handling Requirements Matrix
- Data Inventory and Lifecycle Management
- Review and Reporting
- Auditing Customer and Partner Activity
- BCDR Objectives and Roles
- Breach Investigation Process
- Platform Customer Responsibilities
- Compliance Program Management
- Continuous Compliance Monitoring
- Cyber Liability Insurance
- Data Classification Model
- Emergency Operations Mode
- General Disaster Recovery Procedures
- Monitoring Vendor Risks
- Vulnerability Scanning and Infrastructure Security Testing
- Web Application Protection
- Static Application Security Testing (SAST)
- HIPAA Awareness Training
- Paper Records
- Responsible Disclose and Bug Bounty Program
- Temporary Access to AWS Accounts and Resources
- Data Center Security
- Support and Management of BYOD Devices
- Board of Directors Responsibilities
- Audit Requests
- Protecting Data In Transit
- Protecting Data In Use
- Remote Access / VPN
- Role Based Access Control (RBAC)
- Risk Assessment and Analysis
- Risk Management Objectives
- Risk Mitigation and Monitoring
- Risk Registry
- High Level Application Security Requirements
- Data Protection Implementation and Processes
- Secure Design and Application Threat Modeling
- Access Control of the Application
- Access Establishment, Modification and Termination
- Access Reviews
- Application Service Event Recovery
- Auditing and Assessment Tools
- Media Disposal Process
- Multi-factor Authentication
- Network Intrusion Detection
- Office Network and Wireless Access
- Password Reset and other Helpdesk Requests
- Penetration Testing
- Privileged Access
- Production Access and Secrets Management
- System Malware Protection
- HIPAA Best Practices for Software Development
- Patch Management Procedures
- Server Hardening Guidelines and Processes
- Service Accounts
- Password Management
- Approved Software
- Firewall Protection
- Platform Customer Access to Systems
- Certificate Management
- Host Intrusion Detection
- Centralized Security Information and Event Management
- Clean Desk Policy and Procedures
- Continuous Education and Skills Development
- Employee Incentives and Rewards
- Security Incident Response Team (SIRT)
- Single Sign On
- Software and Systems Acquisition Process
- Software Development Process
- Source Code Management
- Standards for Access Provisioning
- Testing and Maintenance
- User Endpoint Security Controls and Configuration
- Tabletop Exercise
- Types of System Audits
- Vendor Technology Risk Review

“Come as You Are” to Improve GRC Productivity



Integrated version control,
change history and document
age tracking

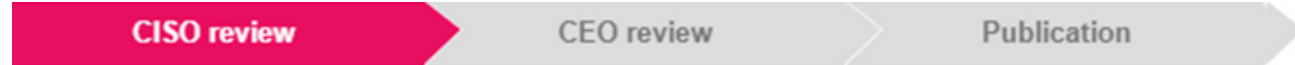


2FA Document approvals



Document comments & notifications

Use your docs as templates



User interface – Document management

Document content

- Search
- Files
- Tasks
- Workbench
- Overview
- Primary assets
- Vendors
- Forms
- Timeline
- Risks
- KPIs
- Collections
- Distributions
- SoA
- Ideas/Roadmap
- Profile
- Settings
- Logout

Document Latest version

is-policy - Employee Handbook and Policy Quick Reference

Revisions > Dependencies (0) > Properties (2) > **Linked Documents (40)** > Linked As Property (0) > Tasks (2) > Comments (20) >

Policy ⓘ

Access control policy
Code of Conduct
Information_Security_Policy_1.0.1.docx
POL-ALL-02 Review of the policies for information security

POL-ALL-04 Acceptable use of assets
POL-FACILITIES-01 Clean desk and clear screen policy
POL-HR-01 Equal Opportunities Policy

POL-IT-01 Secure development policy
POL-IT-02 Network controls
POL-IT-04 Management of removable media
POL-IT-05 Change management

Document ID: POL-ALL-01	Owner: Chief information security officer - CISO	Document Type: Policy	Version: 1.1.0	
Title				
<h2>Policies for information security</h2>				

Status	Name	Date
Created	James Bond	2022-03-12
Review	James Bond	2023-10-10
Publication	James Bond	2023-10-10

Information Security Policy

NEW A.5 - Organisational Controls

General +

B I U X² X S Averta PE 12

Insert ▾

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. (e.g. important contacts,, breach procedures, acceptable use, data handling, threat intelligence, Project management, Classification, data protection, access control, identity management, ...)

[Convert To Note](#)

> All **Policy (25)** Procedure (46)

TITLE ↓	Filter	MODIFIED DATE ↓	ACTION
is-policy - Employee Handbook and Policy Quick Reference		06/06/2024 11:52 pm	⋮
sdlc - Secure Product Development and Product Security		03/06/2024 12:25 pm	⋮
corp-gov - Corporate Governance Policy		31/05/2024 11:07 am	⋮
breach - Business Continuity and Disaster Recovery Policy		31/05/2024 11:07 am	⋮
ir - Incident Response Policy		31/05/2024 11:07 am	⋮
bcdr - Breach Investigation and Notification Policy		31/05/2024 11:06 am	⋮
policy-mgmt - Management Policy		31/05/2024 11:06 am	⋮
cookie - Cookie Policy		31/05/2024 11:05 am	⋮
privacy - Privacy and Consent Policy		31/05/2024 11:05 am	⋮

User interface – Integrated Task Management

INBOX > Brainframe ISMS > Standards > 2. DO > A.5 - Organisationa...

+ Add Task + Add Checklist + Add Kanban

Sort by deadline
 Show all tasks
 Show finished tasks

- Files
- Tasks
- Workbench
- Overview
- Primary assets
- Vendors
- Forms
- Timeline
- Risks
- KPIs
- Collections
- Distributions
- SoA
- Ideas/Roadmap
- Profile
- Settings
- Logout

- Create task in Brainframe
- Link to task in ASANA
- Link to task in JIRA
- Link to task in Monday.com

Access requests (0)

Asset lifecycle (0)

Audit planning (0)

Document review (0)

Employee lifecycle (0)

Incident management (0)

Legislation (0)

Non-conformity management (0)

Personal data inventory (0)

Risk management (0)

General tasks (3)

<input type="radio"/> Integrate template handbook into new handbook document	Details NC	2024-Jun-06 - 2024-Jun-07	
<input type="radio"/> Review approvals and signing of residual risks (wait until all risks are imported)	Details NC	2024-Jun-06 - 2024-Jun-07	
<input type="radio"/> Check the privacy and security URL on website	Details FL	2024-Jun-28 - 2024-Jun-28	

Access requests (0)

Asset lifecycle (0)

Audit planning (0)

Document review (0)

Employee lifecycle (0)

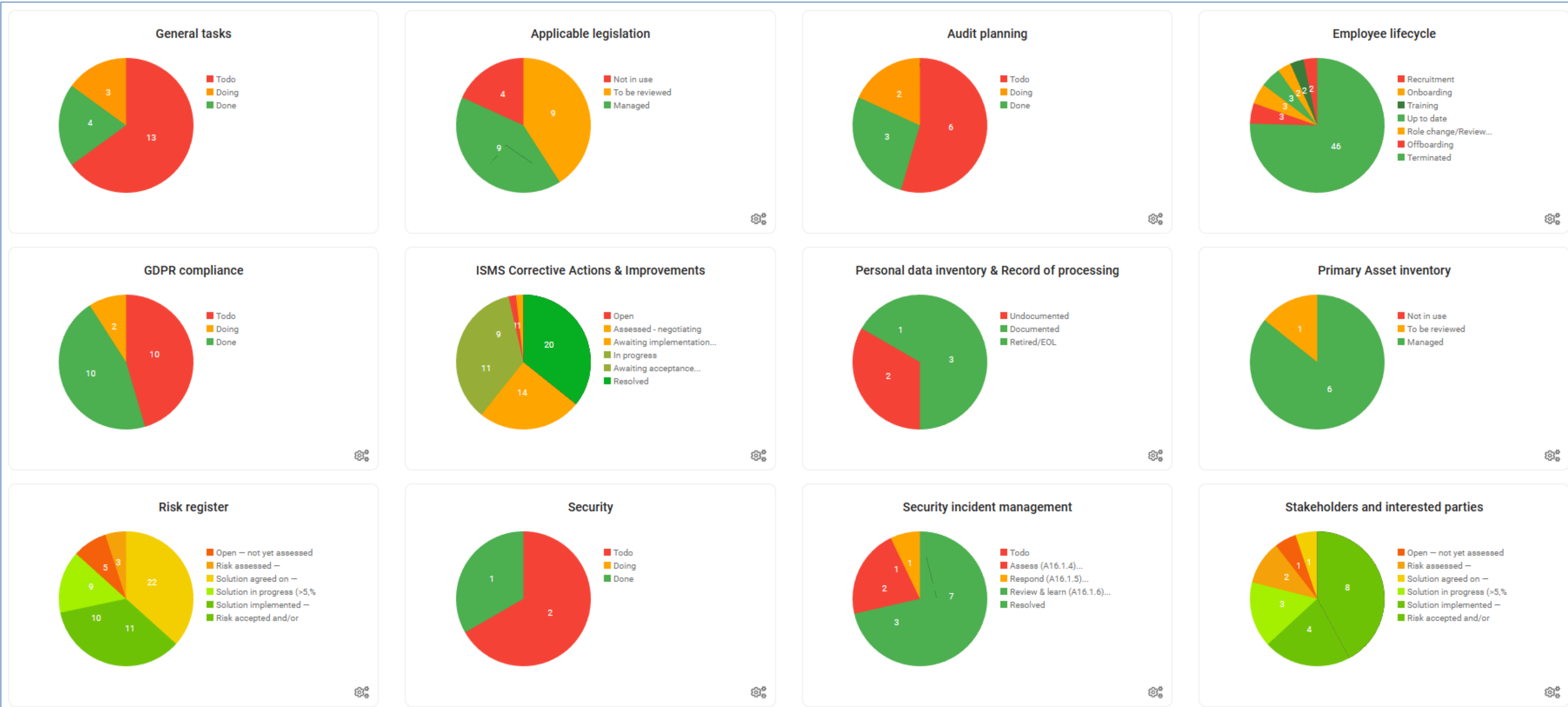
GDPR Requests (0)

CISOMatic
Switch Workspace

© BRAINFRAME TECHNOLOGIES s.à.r.l.
PRIVACY POLICY 20240605-3654

Process Status Overview

✓ Task management
📋 Workflows
⚖️ Risk management



User interface – Process To Kanban management

The screenshot displays the CISOMatic Kanban management interface. On the left, a sidebar contains navigation options: Files, Tasks, **Workbench** (highlighted), Overview, Primary assets, Vendors, Forms, Timeline, Risks, KPIs, Collections, Distributions, SoA, Ideas/Roadmap, Profile, Settings, and Logout. The main workspace is titled 'INBOX' and features a search bar and various filters: Kanban, Table, Include Subfolders, Sort by deadline, Only my tasks, Show brainframe tasks, Show Other Workspace, Filter risks, Show Risk Details, Show archived files, and Employee lifecycle. The Kanban board is organized into five columns:

- Todo (22)**:
 - 22 - Tightly review source code permissions (gitlab) - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 55 - Document approved removable media devices (HD, USB, ...) - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 97 - Properly document company provided assets - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 77 - Access badges contain too much information - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 7 - Implement central password manager - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 22 - Tightly review source code permissions (gitlab) - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 83 - Identification of the regulatory requirements from stakeholders and regulatory bodies - ISMS Corrective Actions & Improvements
- Assessment (13)**:
 - 20 - Fix door locks (entrance Demo Group, back door and server room) - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - CAPA_102 - Install smoke detector in kitchen - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 16 - Check correct license management & create document to track - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 93 - Implement content security policy (CSP) - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 17 - Remove special user permissions Azure - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 91 - Automate change management process for developers - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 6 - Implement VLANs - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 95 - AWS IAM token rotation
- Awaiting board approval (5)**:
 - 94 - Organise external pentest - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 50 - Install lockable file cabinets with fire protection for physical document protection - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 86 - Provide company workstations for staff that have access to sensitive data - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 33 - KPI - Implement Employee NPS evaluation - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 88 - More clear segregation of duties between ZT/DS - ISMS Corrective Actions & Improvements - Carlo RICHMOND
- Implementation (7)**:
 - 21 - Ensure crowdstrike is installed on all workstations - ISMS Corrective Actions & Improvements - Carlo RICHMOND (28/06/2021)
 - 13 - Gap Audit - 3 - ISO27001/HDS - BCP planning + simulation of disaster - ISMS Corrective Actions & Improvements - Carlo RICHMOND (31/08/2021)
 - 18 - Ensure all devices are encrypted - ISMS Corrective Actions & Improvements - Carlo RICHMOND (31/08/2021)
 - 87 - Fully document roles and responsibilities and competencies - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 54 - Centralize logging from network security gateway into Datadog - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 31 - Vendor/Sub-contractor review pri - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 48 - Implement workstation conditional access
- Monitoring (2)**:
 - 37 - Hire IT manager for duties - ISMS Corrective Actions & Improvements - Carlo RICHMOND
 - 19 - GDPR - Communicate data per mail - ISMS Corrective Actions & Improvements - Carlo RICHMOND

User interface – Knowledge Inventory Register

☰
🔍
INBOX

CISOMatic

Grouped per document type (26)
Total documents count: 372

	Title ↑↓ <input style="width: 50px;" type="text" value="Filter"/>	Count
	Action to take	1
	Business impact assessment (BIA)	14
	Certificate	1
	Consultant	3
	Core Business Service	40
	Corrective or preventive action (CAPA)	1
	Data Record	1
	Document	21
	Employee	13
	Form/Survey reply	1
	Image	16
	Security objective KPI	1
	KPI Reading	1
	Regulation, Legislation or standard	1
	Meeting notes	1
	PDF	17
	Personal data	2
	Policy	25
	Procedure	146
	Data processing activity	1
	Role and responsibilities	13
	Spreadsheet	1
	Stakeholder/Interested party	1

🔍 Search

📁 Files

✓ Tasks

🛠 Workbench

☰ Overview

📁 Primary assets

🏢 Vendors

📄 Forms

📅 Timeline

⚠ Risks

📊 KPIs

🔗 Collections

📦 Distributions

📈 SoA

💡 Ideas/Roadmap

👤 Profile

⚙ Settings

🚪 Logout

CISOMatic
Switch Workspace

© BRAINFRAME TECHNOLOGIES s.p.a. | WWW.BRAINFRAME.COM

User interface – Asset inventory & dependencies

Search

- Builder
- Files
- Tasks
- Workbench
- Overview
- Primary assets
- Suppliers
- Forms
- Timeline
- Risks
- KPIs
- Collections
- Distributions
- SoA
- Ideas/Roadmap
- Documentation
- Profile
- Settings
- Logout

Hierarchy List **Asset Management**

- Bob Sage accountings
- CISOMatic GRC Service
 - AWS Cloudfront
 - AWS Lambda
 - Clearview backend
 - CISOMatic tourist site service
 - Clearview service
 - Fiber consultation service
 - GOGO
 - PowerCrush service
 - Rockpush service
 - Sales to customers
 - Test item
 - tourist site mobile app service

Document Latest version Managed EDIT

Revisions Dependencies (7) Properties (5) Linked Documents (11) Linked As Property (0) Tasks (0) Comments (4)

Name of the asset.

CISOMatic GRC service

Description
Any relevant information on how the asset is used and why it has value to the business.

Our key product for GRC

Supporting location/medium
This can be a service, storage location or place of usage of the primary asset

- See attached assets

Asset type
What type of asset is it (Product & service, Physical, Sales/Marketing/Business, financial information, IPR, infrastructure, personal data, information processing devices, products & services, removable storage/hard drive, sales and marketing information, software applications, supply chain, commercial /contractual information, other information).

Once the asset is created you can add it to a dedicated checklist in the planning tab (eg primary assets, supporting assets) to manage them on the workbench

Online web service

Asset Classification
Public, confidential, sensitive, ... to help demonstrate the value of the information and its protection level required

Sensitive due to multiple confidential personal data

Financial value
You may optionally choose to add this to help illustrate financial value at risk and total value for the portfolio of assets;

Internal Asset Owner
Who is the final responsible for the asset within the company. You may also choose to specify the legal owner (eg organisation, employee for BYOD, supplier, ...)

CTO

Stakeholders
Who are the main stakeholders/interested parties that can influence or are most impacted by events on these assets.

- tourists
- Coachs
- Customer success
- CISO
- DPO
- CTO

Security requirements

ASK QUESTION

CISOMatic Switch Workspace

© BRAINFRAME TECHNOLOGIES s.r.l. PRIVACY POLICY 20240708-3715

User interface – Vendor management & dependencies

BRINFRAME TECHNOLOGIES INBOX

Search

Hierarchy List Suppliers Management

- Builder
- Files
- Tasks
- Workbench
- Overview
- Primary assets
- Suppliers**
- Forms
- Timeline
- Risks
- KPIs
- Collections
- Distributions
- SoA
- Ideas/Roadmap
- Documentation
- Profile
- Settings
- Logout

ASK QUESTION

CISOMatic Switch Workspace

© BRAINFRAME TECHNOLOGIES s.à.r.l. PRIVACY POLICY 20240708-3715

Amazon web services (AWS)

- AWS Autoscaling
 - AWS EC2
 - AWS Cloudformation
 - AWS Lambda
 - AWS CloudHSM
- Asana
- Atlassian
- Brainframe Technologies
- Canva
- Docker
- Github
- Google
- Slack
- Snyk
- Stripe
- Zendesk
- Zoho

Document Amazon web services (AWS) Latest version In renewal EDIT

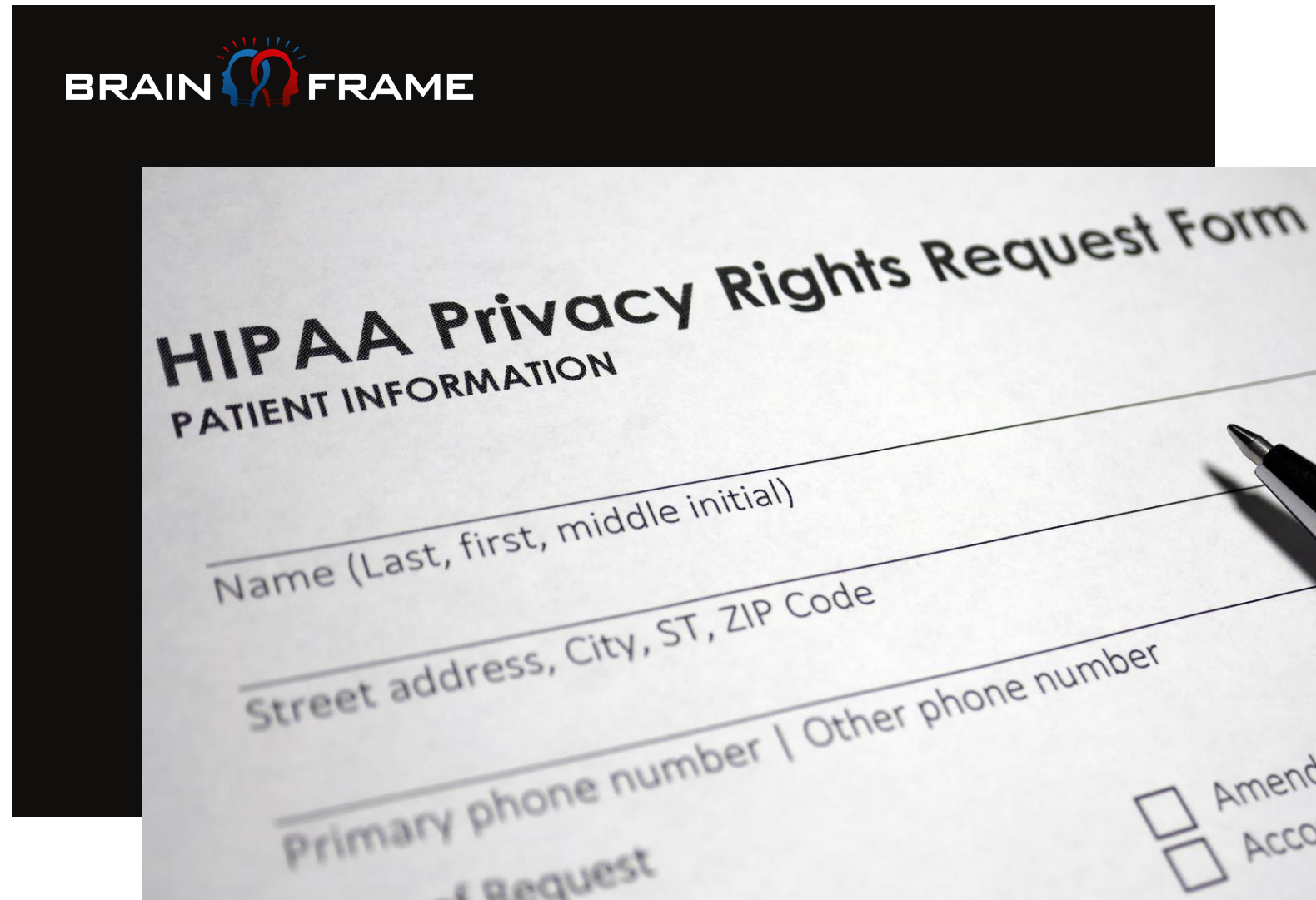
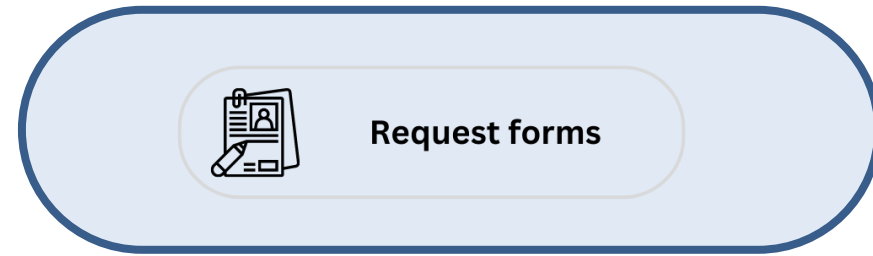
Revisions Dependencies (10) Properties (5) Linked Documents (15) Linked As Property (1) Tasks (2) Comments (5)

Company name	Amazon Web Services (AWS)
Address	Route de Luxembourg
Primary contact	Mr Jean Smith
VAT number	LU12345678
Services	Cloud service provider
Extra information	

Asset library

- AWS Autoscaling
- AWS Certificate manager
- AWS Cloudformation
- AWS Cloudfront

Automate Process Flows with Intelligent Forms



- Let others start workflows and processes using our online forms - don't chase them.
- Use your own Word/Excel documents as forms to be filled out or use simple Q&As.
- Embed forms into your own intranet/website.
- Auto-calculate risks based on replies received.
- Send out recurring document requests for your evidence collection.

User interface – Input forms

Search

- Files
- Tasks
- Workbench
- Overview
- Primary assets
- Vendors
- Forms**
- Timeline
- Risks
- KPIs
- Collections
- Distributions
- SoA
- Ideas/Roadmap
- Profile
- Settings
- Logout

Access request
Select Form

Show Form View Open Reply Folder Save

QUESTIONS SETTINGS

Form title
Access request

Form description

This form must be filled in for any access request

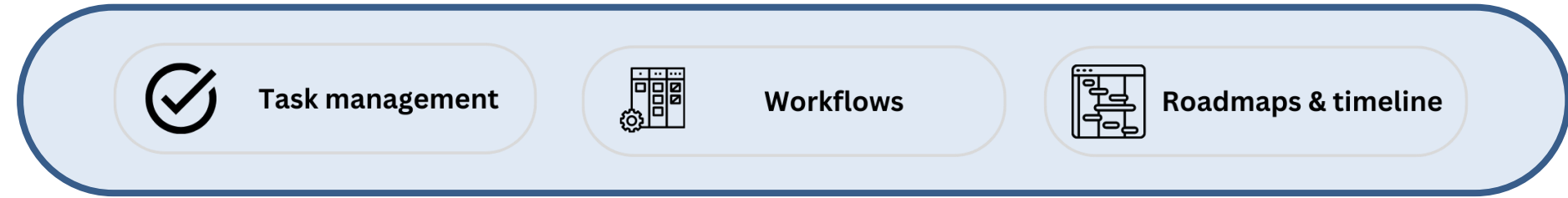
Placeholder text for initial document name filled in by form user

Free text Document property Risk Mapping

Question
What is the full name of the employee requesting the access change

Free text placeholder

All you Need to Plan your Mitigations



KANBAN BOARD



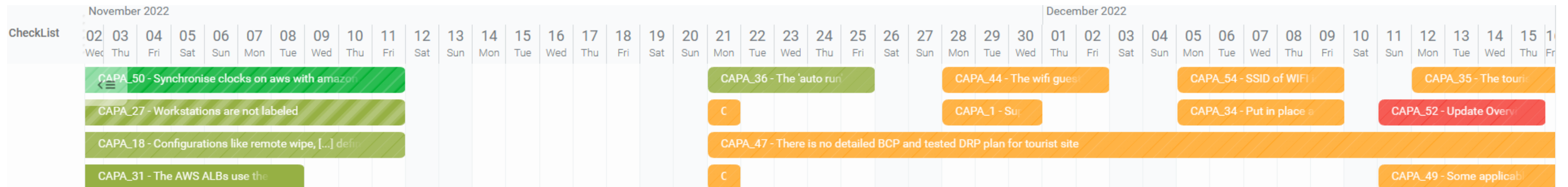
GANTT ROADMAPS



CHECKLISTS



REMINDERS



Track Your Audit Planning

Task management Workflows Roadmaps & timeline

Search document type

Action to take

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

Todo (5)

- AUD-2 - Initial ISO27001:2017 audit Stage 2 (0% progress)
- AUD-3 - GDPR audit by DPO 2023 (0% progress)
- Conduct internal audit
- Yearly Fiber consult audit
- AUD-4 - OWASP Pentest 2022 - tourist site and SkyPortPR

Doing (1)

- Yearly external pentest audit on key applications

Done (3)

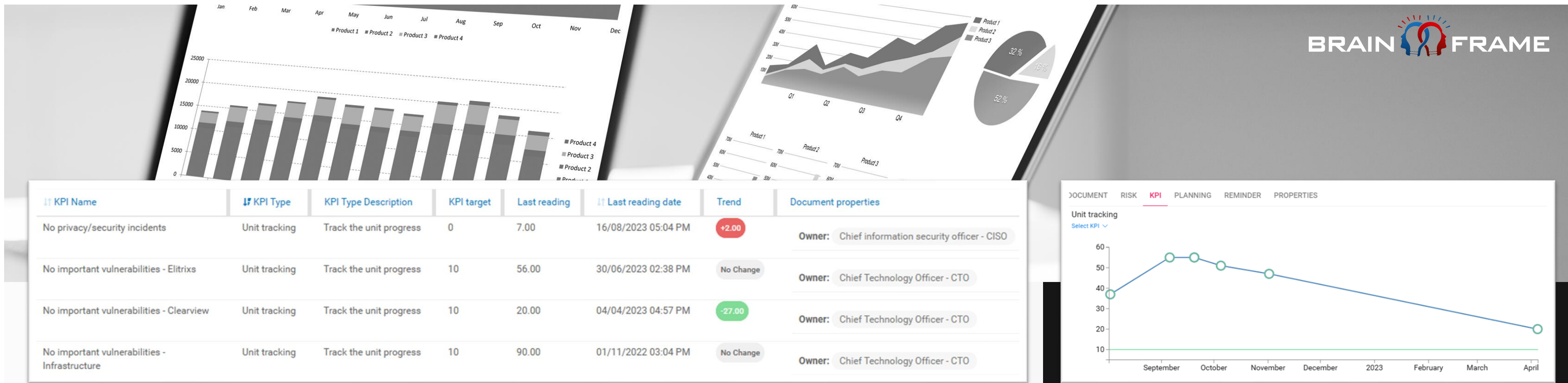
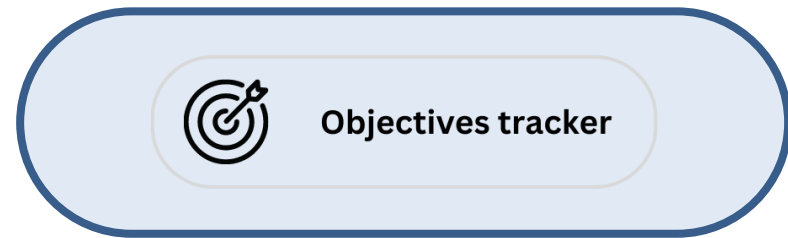
- Review of compliance with policies and procedures by managers (100% progress)
- AUD-1 ISO27001 Initial Blanc audit (100% progress)
- CISOMatic - ISO 27001 Rapport d'audit a blanc VD 10102022.docx (100% progress)

Timeline view showing a calendar for October 2022. A task titled "Review of compliance with policies and procedures by managers from 2022-10-13 to 2022-10-21" is highlighted with a green bar and a "Review" button.

User interface – Gantt Timeline/Planning

The screenshot displays the BrainFrame Gantt Timeline/Planning interface. The top navigation bar includes the BrainFrame logo, a search bar, and a dropdown menu with 'INBOX'. Below this, there are toggle switches for 'Include Subfolders' and 'Show archived documents', and dropdown menus for 'Checklist Timeline', 'Employee lifecycle', and 'Day'. The main area is a Gantt chart for June and July 2024. The chart shows a 'Risk register' with several risks represented by horizontal bars of different colors and patterns. The risks are: R-028 (black bar, 'Non E2E encrypted confidential tourist/Coach data stored on our systems can be breached'), R-054 (black bar with diagonal lines, 'Insufficient cooling of production servers'), R-017 (orange bar with diagonal lines, 'Breaches of legal, contractual, statutory, regulatory or contractual obligations related to information security'), R-009 (orange bar with diagonal lines, 'Outdated frameworks resulting in unfixable security issues'), R-048 (orange bar with diagonal lines, 'Dreaming'), R-036 (orange bar with diagonal lines, 'Non-timely correction of tourist site vulnerabilities'), R-027 (yellow bar with diagonal lines, 'Support teams have full access to SkyPorts if they want'), and R-053 (green bar with diagonal lines, 'Multiple vulnerabilities in the Panthe...'). The 'Timeline' menu item in the left sidebar is highlighted. The bottom left corner shows the 'DC CISOMatic Switch Workspace' logo and the copyright notice '© BRAINFRAME TECHNOLOGIES s.r.l.'. The bottom right corner has the website URL 'WWW.BRAINFRAME.COM'.

Define, Document & Track your Objectives



KPI OVERVIEW

$f(x)$

COMPLEX FORMULA



TARGETS & TRENDS

User interface – Objectives/KPIs

Search

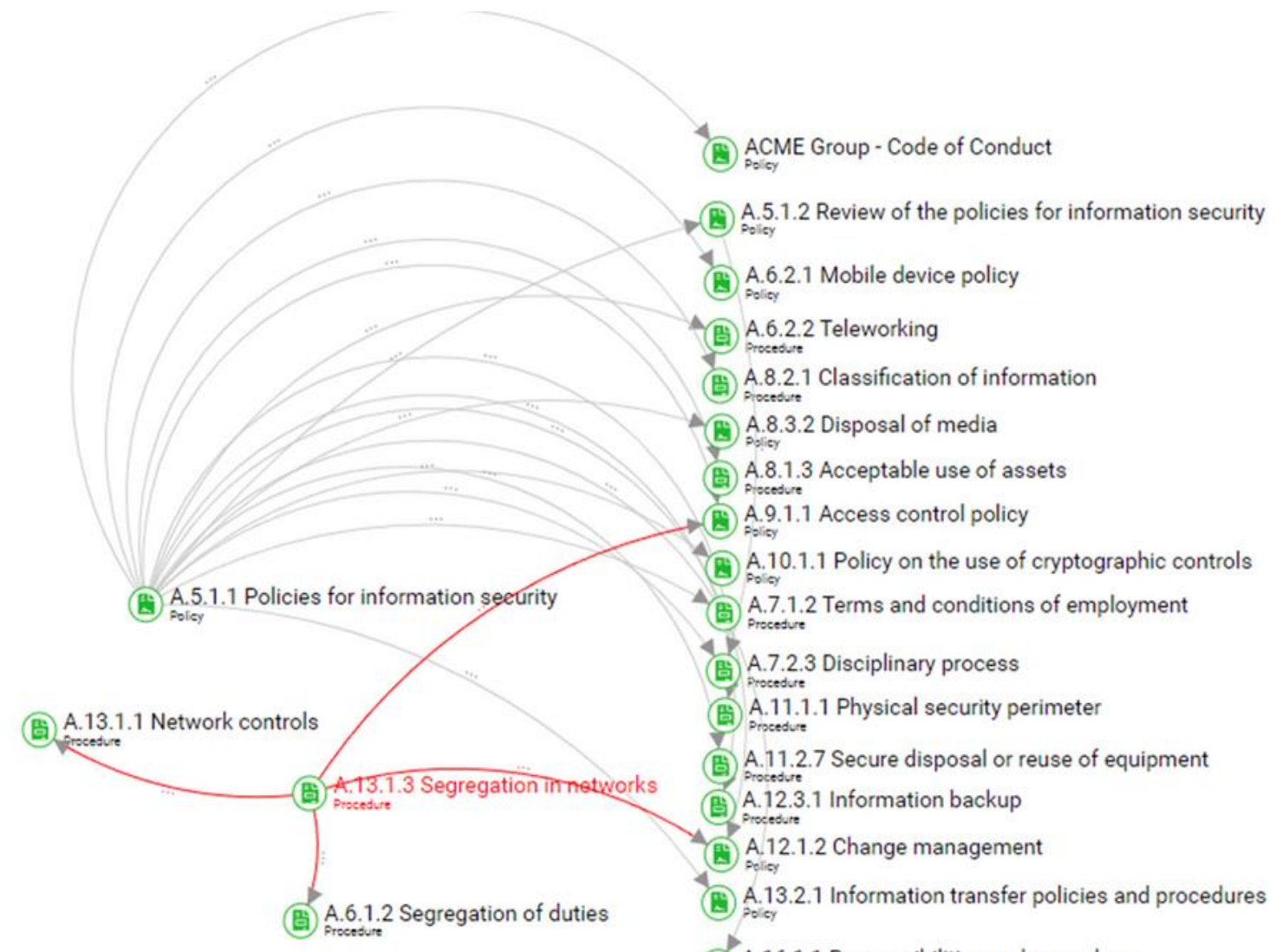
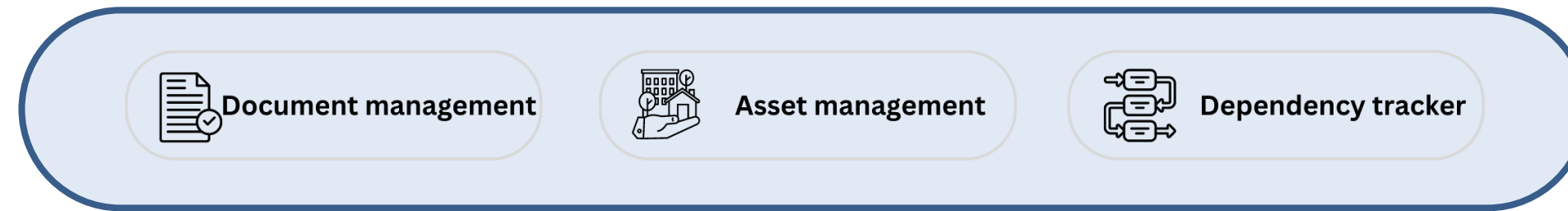
- Files
- Tasks
- Workbench
- Overview
- Primary assets
- Vendors
- Forms
- Timeline
- Risks
- KPIs**
- Collections
- Distributions
- SoA
- Ideas/Roadmap
- Profile
- Settings
- Logout

KPI Name	KPI Type	KPI Type Description	KPI target	Last reading	Last reading date	Trend	Document properties
Secure workstations	Unit tracking	Track the unit progress	0	2.00	21/03/2024 03:06 PM	-3.00	Owner: Chief information security officer - CISO
Average Time to Detect	Unit tracking	Track the unit progress	10	58.00	19/11/2023 06:17 PM	+2.00	Owner: Chief Technology Officer - CTO
Compliance score	Percentage tracking	Track the progress in percentage	80	50.00	16/11/2023 02:48 PM	No Change	Owner: Chief information security officer - CISO
Security/Privacy awareness training	Percentage tracking	Track the progress in percentage	100	96.00	16/08/2023 03:14 PM	+1.00	Owner: HR Manager
Average Time to Respond	Unit tracking	Track the unit progress	10	20.00	04/04/2023 04:57 PM	-27.00	Owner: Chief Technology Officer - CTO
High web service availability	Percentage tracking	Track the progress in percentage	99.5	99.60	06/03/2023 09:55 AM	-0.40	Owner: Infrastructure manager
Timely resolution CRITICAL infrastructure vulnerabilities	Unit tracking	Track the unit progress	10	90.00	01/11/2022 03:04 PM	No Change	Owner: Chief Technology Officer - CTO
Timely resolution CRITICAL application vulnerabilities	Unit tracking	Track the unit progress	10	15.00	01/11/2022 03:02 PM	-30.00	Owner: Chief Technology Officer - CTO
Timely resolution CRITICAL workstation vulnerabilities	Unit tracking	Track the unit progress	10	17.00	01/11/2022 03:00 PM	-20.00	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	-3.00	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	+1.00	Owner: Chief Technology Officer - CTO
No important vulnerabilities - Commercial website	Unit tracking	Track the unit progress	10	186.00	01/11/2022 02:55 PM	-2.00	Owner: Chief Technology Officer - CTO
No privacy/security incidents	Unit tracking	Track the unit progress	0	5.00	01/11/2022 11:19 AM	+4.00	Owner: Chief information security officer - CISO

DC CISOMatic Switch Workspace

Visually Map Dependencies of Assets/Risks/Controls

A unique feature of Brainframe is the capability of offering a holistic and visual representation of dependencies and links between assets, risks and related controls.



\$	Accounting system
⚡	Action to take
X ²	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 o
🔧	Corrective or preventive action (CAPA)

User interface - Dependencies

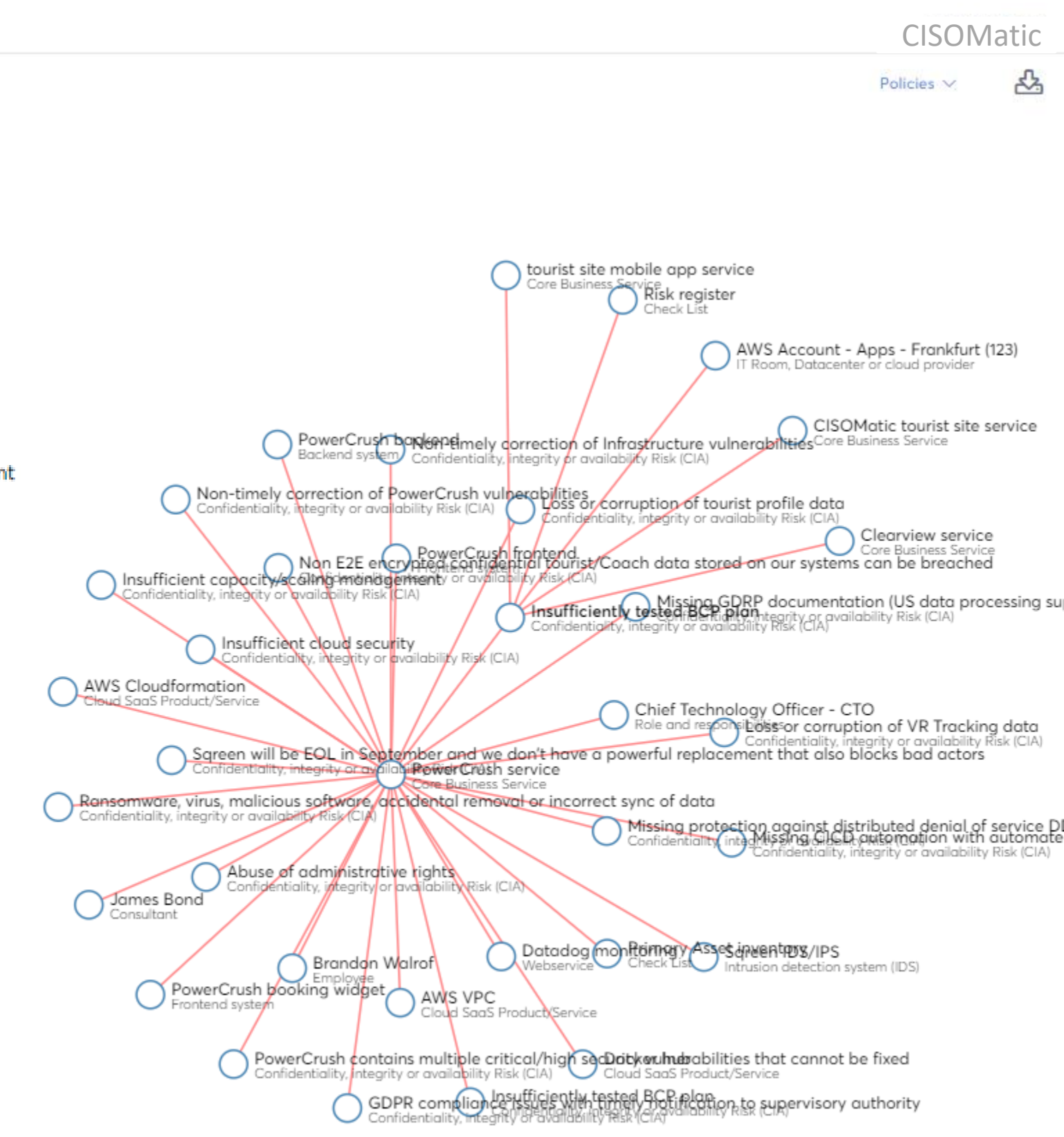
BRINFRAME TECHNOLOGIES

INBOX

Search

- Files
- Tasks
- Workbench
- Overview
- Primary assets
- Vendors
- Forms
- Timeline
- Risks
- KPIs
- Collections**
- Distributions
- SoA
- Ideas/Roadmap
- Profile
- Settings
- Logout

DC CISOMatic Switch Workspace



Make Document Distribution Easy and Automatic



- Send your policies and procedures to staff & suppliers per mail without login for online review & approval.
- Track multi-version auditable approvals per document.
- Centrally track progress.
- Continuously monitor document acknowledgment status.

User interface - Distributions

Search

- Files
- Tasks
- Workbench
- Overview
- Primary assets
- Vendors
- Forms
- Timeline
- Risks
- KPIs
- Collections
- Distributions**
- SoA
- Ideas/Roadmap
- Profile
- Settings
- Logout

ISMS - F3C Policies
Select Distribution

Show Distribution View Manage & Notify Contacts (0% Completed)

Introduction

intro Introduction to document approval	06/06/2024 10:48 PM	0%
is-policy Employee Handbook and Policy Quick Reference	06/06/2024 10:21 PM	0%

Policies

access Access Policy	1.0.0 - 03/06/2024 01:57 PM	0%
asset-mgmt Asset Inventory Management Policy	1.0.0 - 03/06/2024 01:54 PM	0%
risk-mgmt Risk Management Policy	1.0.0 - 03/06/2024 01:57 PM	0%
rar Roles, Responsibilities and Training Policy	1.0.0 - 03/06/2024 01:56 P...	0%
compliance-audit Compliance Audits and External Communications Policy	1.0.0 - 03/06/2024 01:55 PM	0%
vuln-mgmt Vulnerability Management	1.0.0 - 03/06/2024 01:55 PM	0%
hr HR and Personnel Security Policy	1.0.0 - 03/06/2024 01:56 P...	0%
data-mgmt Data Management Policy	1.0.0 - 03/06/2024 01:53 PM	0%
facility Facility Access and Physical Security Policy	1.0.0 - 03/06/2024 01:55 PM	0%
system-audit System Audits, Monitoring and Assessments Policy	1.0.0 - 03/06/2024 01:54 PM	0%
threat Threat Detection and Prevention Policy	1.0.0 - 03/06/2024 01:53 PM	0%
vendor Third Party Security, Vendor Risk Management and Systems/Services Acquisition Policy	1.0.0 - 03/06/2024 01:54 PM	0%
mdm Mobile Device Security and Storage Media Management Policy	1.0.0 - 03/06/2024 01:53 PM	0%
ccm Configuration and Change Management Policy	1.0.0 - 03/06/2024 01:54 PM	0%

User interface - Distributions

You will receive an invite per mail to read and formally approve all policies

ISMS - Policies (23.30 min remaining) 0%

Introduction Search document

- intro Introduction to document approval 1.89 min
- is-policy Employee Handbook and Policy Quick Reference < 1 min

Policies

- access Access Policy 1.97 min
- asset-mgmt Asset Inventory Management Policy < 1 min
- risk-mgmt Risk Management Policy < 1 min
- rar Roles, Responsibilities and Training Policy 2.20 min
- compliance-audit Compliance Audits and External Communications Policy 1.19 min
- vuln-mgmt Vulnerability Management < 1 min
- hr HR and Personnel Security Policy 1.30 min
- data-mgmt Data Management Policy 1.01 min
- facility Facility Access and Physical Security Policy 1.30 min
- system-audit System Audits, Monitoring and Assessments Policy < 1 min
- threat Threat Detection and Prevention Policy < 1 min
- vendor Third Party Security, Vendor Risk Management and Systems/Services Acquisition Policy 1.02 min
- mdm Mobile Device Security and Storage Media Management 1.06 min

intro Introduction to document approval

Mark As Read & Understood

Procedure

This is the first document you should read to understand how we want to communicate policies and procedures to you. A distribution is a grouping of multiple policies and/or procedures that Management decided on and would like you to carefully review, understand and apply.

Overview

- 1. On the left top you see all the distributions assigned to you.** We only require you to formally read and approve the policies, but we count on your best effort to understand and apply the related procedures in your day-to-day work.
- 2. On the left side of this text you see a list of documents from the current selected distribution (ISMS - policies).** Please open and read them one by one starting from the top.
- 3. For documents where we need your approval, you'll see a red button with "Mark as Read & understood" on the right top.** By clicking on it, you are providing auditable proof and confidence in your compliance with the content defined in that document.
- 4. As you will need to approve multiple documents, you'll see your overall progress in the top left.** The distribution with procedures does not require you to mark as read, so no progress is shown in that case.
- 5. Some people might get some additional department specific distributions assigned to them.** If this applies to you, you will see multiple distributions in the top left.

In case some links inside a document indicate that you have no permission, this means they are not part of distributions assigned to you. If so, you do not need to provide your explicit understanding/approval, so that you can proceed to ignore them.

Please note that policies and procedures are versioned and can evolve over time to align with the business evolution and new requirements. This means that you may receive new invites in the future to approve those new versions. They will be easy to identify, as you will see non-approved documents with a red dot in front.

At any time you can consult the latest version of our policies and procedures with the following links (please make sure to bookmark them):

- ISMS - Policies
- ISMS - Procedures

Your participation and thinking with us is essential for our continuous improvement, so if you identify non-compliance with our policies, or if you have improvement recommendations or special remarks regarding the policies and procedures, it is your duty to report this to your Manager and the Compliance Team, so that we can properly document it and implement a correction. Please do so by sending an email to [security@...com](mailto:security@...) with your Manager in CC.

We kindly ask you to **Read and Mark as Approved** all documents in the list on the left. Once you've done so, they show as green.

Thank you in advance for your time and cooperation,

The Compliance Team

Document comments & activity

● Add a comment

User interface - Distributions

You will receive an invite per mail to read and formally approve all policies

ISMS · Policies (23.30 min remaining) 0%

Introduction Search document

- intro Introduction to document approval 1.89 min
- is-policy Employee Handbook and Policy Quick Reference < 1 min

Policies

- access Access Policy 1.97 min
- asset-mgmt Asset Inventory Management Policy < 1 min
- risk-mgmt Risk Management Policy < 1 min
- rar Roles, Responsibilities and Training Policy 2.20 min
- compliance-audit Compliance Audits and External Communications Policy 1.19 min
- vuln-mgmt Vulnerability Management < 1 min
- hr HR and Personnel Security Policy 1.30 min
- data-mgmt Data Management Policy 1.01 min
- facility Facility Access and Physical Security Policy 1.30 min
- system-audit System Audits, Monitoring and Assessments Policy < 1 min
- threat Threat Detection and Prevention Policy < 1 min
- vendor Third Party Security, Vendor Risk Management and Systems/Services Acquisition Policy 1.02 min
- mdm Mobile Device Security and Storage Media Management 1.06 min

intro Introduction to document approval Mark As Read & Understood

Document content

Procedure

This is the first document you should read to understand how we want to communicate policies and procedures to you. A distribution is a grouping of multiple policies and/or procedures that Management decided on and would like you to carefully review, understand and apply.

Overview

- On the left top you see all the distributions assigned to you.** We only require you to formally read and approve the policies, but we count on your best effort to understand and apply the related procedures in your day-to-day work.
- On the left side of this text you see a list of documents from the current selected distribution (ISMS · policies).** Please open and read them one by one starting from the top.
- For documents where we need your approval, you'll see a red button with "Mark as Read & understood" on the right top.** By clicking on it, you are providing auditable proof and confidence in your compliance with the content defined in that document.
- As you will need to approve multiple documents, you'll see your overall progress in the top left.** The distribution with procedures does not require you to mark as read, so no progress is shown in that case.
- Some people might get some additional department specific distributions assigned to them.** If this applies to you, you will see multiple distributions in the top left.

In case some links inside a document indicate that you have no permission, this means they are not part of distributions assigned to you. If so, you do not need to provide your explicit understanding/approval, so that you can proceed to ignore them.

Please note that policies and procedures are versioned and can evolve over time to align with the business evolution and new requirements. This means that you may receive new invites in the future to approve those new versions. They will be easy to identify, as you will see non-approved documents with a red dot in front.

At any time you can consult the latest version of our policies and procedures with the following links (please make sure to bookmark them):

- ISMS - Policies
- ISMS - Procedures

Your participation and thinking with us is essential for our continuous improvement, so if you identify non-compliance with our policies, or if you have improvement recommendations or special remarks regarding the policies and procedures, it is your duty to report this to your Manager and the Compliance Team, so that we can properly document it and implement a correction. Please do so by sending an email to security@.com with your Manager in CC.

We kindly ask you to **Read and Mark as Approved** all documents in the list on the left. Once you've done so, they show as green.

Thank you in advance for your time and cooperation,

The Compliance Team

Document comments & activity

Add a comment

User interface - Distributions

You will receive an invite per mail to read and formally approve all policies

ISMS · Policies (23.30 min remaining) 0%

Introduction Search document

- intro Introduction to document approval 1.89 min
- is-policy Employee Handbook and Policy Quick Reference < 1 min

Policies

- access Access Policy 1.97 min
- asset-mgmt Asset Inventory Management Policy < 1 min
- risk-mgmt Risk Management Policy < 1 min
- rar Roles, Responsibilities and Training Policy 2.20 min
- compliance-audit Compliance Audits and External Communications Policy 1.19 min
- vuln-mgmt Vulnerability Management < 1 min
- hr HR and Personnel Security Policy 1.30 min
- data-mgmt Data Management Policy 1.01 min
- facility Facility Access and Physical Security Policy 1.30 min
- system-audit System Audits, Monitoring and Assessments Policy < 1 min
- threat Threat Detection and Prevention Policy < 1 min
- vendor Third Party Security, Vendor Risk Management and Systems/Services Acquisition Policy 1.02 min
- mdm Mobile Device Security and Storage Media Management Policy 1.06 min

Mark As Read & Understood

intro Introduction to document approval

Procedure

This is the first document you should read to understand how we want to communicate policies and procedures to you. A distribution is a grouping of multiple policies and/or procedures that Management decided on and would like you to carefully review, understand and apply.

Overview

- On the left top you see all the distributions assigned to you.** We only require you to formally read and approve the policies, but we count on your best effort to understand and apply the related procedures in your day-to-day work.
- On the left side of this text you see a list of documents from the current selected distribution (ISMS · policies).** Please open and read them one by one starting from the top.
- For documents where we need your approval, you'll see a red button with "Mark as Read & understood" on the right top.** By clicking on it, you are providing auditable proof and confidence in your compliance with the content defined in that document.
- As you will need to approve multiple documents, you'll see your overall progress in the top left.** The distribution with procedures does not require you to mark as read, so no progress is shown in that case.
- Some people might get some additional department specific distributions assigned to them.** If this applies to you, you will see multiple distributions in the top left.

In case some links inside a document indicate that you have no permission, this means they are not part of distributions assigned to you. If so, you do not need to provide your explicit understanding/approval, so that you can proceed to ignore them.

Please note that policies and procedures are versioned and can evolve over time to align with the business evolution and new requirements. This means that you may receive new invites in the future to approve those new versions. They will be easy to identify, as you will see non-approved documents with a red dot in front.

At any time you can consult the latest version of our policies and procedures with the following links (please make sure to bookmark them):

- ISMS - Policies
- ISMS - Procedures

Your participation and thinking with us is essential for our continuous improvement, so if you identify non-compliance with our policies, or if you have improvement recommendations or special remarks regarding the policies and procedures, it is your duty to report this to your Manager and the Compliance Team, so that we can properly document it and implement a correction. Please do so by sending an email to security@.com with your Manager in CC.

We kindly ask you to **Read and Mark as Approved** all documents in the list on the left. Once you've done so, they show as green.

Thank you in advance for your time and cooperation,
The Compliance Team

Comments

Document comments & activity

● Add a comment

User interface - Distributions

You will receive an invite per mail to read and formally approve all policies

ISMS · Policies (23.30 min remaining) 0%

Introduction Search document

- intro Introduction to document approval 1.89 min
- is-policy Employee Handbook and Policy Quick Reference < 1 min

Policies

- access Access Policy 1.97 min
- asset-mgmt Asset Inventory Management Policy < 1 min
- risk-mgmt Risk Management Policy < 1 min
- rar Roles, Responsibilities and Training Policy 2.20 min
- compliance-audit Compliance Audits and External Communications Policy 1.19 min
- vuln-mgmt Vulnerability Management < 1 min
- hr HR and Personnel Security Policy 1.30 min
- data-mgmt Data Management Policy 1.01 min
- facility Facility Access and Physical Security Policy 1.30 min
- system-audit System Audits, Monitoring and Assessments Policy < 1 min
- threat Threat Detection and Prevention Policy < 1 min
- vendor Third Party Security, Vendor Risk Management and Systems/Services Acquisition Policy 1.02 min
- mdm Mobile Device Security and Storage Media Management 1.06 min

intro Introduction to document approval

Procedure

This is the first document you should read to understand how we want to communicate policies and procedures to you. A distribution is a grouping of multiple policies and/or procedures that Management decided on and would like you to carefully review, understand and apply.

Overview

- On the left top you see all the distributions assigned to you.** We only require you to formally read and approve the policies, but we count on your best effort to understand and apply the related procedures in your day-to-day work.
- On the left side of this text you see a list of documents from the current selected distribution (ISMS · policies).** Please open and read them one by one starting from the top.
- For documents where we need your approval, you'll see a red button with "Mark as Read & understood" on the right top.** By clicking on it, you are providing auditable proof and confidence in your compliance with the content defined in that document.
- As you will need to approve multiple documents, you'll see your overall progress in the top left.** The distribution with procedures does not require you to mark as read, so no progress is shown in that case.
- Some people might get some additional department specific distributions assigned to them.** If this applies to you, you will see multiple distributions in the top left.

In case some links inside a document indicate that you have no permission, this means they are not part of distributions assigned to you. If so, you do not need to provide your explicit understanding/approval, so that you can proceed to ignore them.

Please note that policies and procedures are versioned and can evolve over time to align with the business evolution and new requirements. This means that you may receive new invites in the future to approve those new versions. They will be easy to identify, as you will see non-approved documents with a red dot in front.

At any time you can consult the latest version of our policies and procedures with the following links (please make sure to bookmark them):

- ISMS - Policies
- ISMS - Procedures

Your participation and thinking with us is essential for our continuous improvement, so if you identify non-compliance with our policies, or if you have improvement recommendations or special remarks regarding the policies and procedures, it is your duty to report this to your Manager and the Compliance Team, so that we can properly document it and implement a correction. Please do so by sending an email to security@.com with your Manager in CC.

We kindly ask you to **Read and Mark as Approved** all documents in the list on the left. Once you've done so, they show as green.

Thank you in advance for your time and cooperation,

The Compliance Team

Document comments & activity

● Add a comment

Approval

[Mark As Read & Understood](#)

User interface - Distributions

You will receive an invite per mail to read and formally approve all policies

ISMS · Policies (23:30 min remaining) 0%

All documents & status

Introduction Search document

intro Introduction to document approval	1.89 min
is-policy Employee Handbook and Policy Quick Reference	< 1 min

Policies

access Access Policy	1.97 min
asset-mgmt Asset Inventory Management Policy	< 1 min
risk-mgmt Risk Management Policy	< 1 min
rar Roles, Responsibilities and Training Policy	2.20 min
compliance-audit Compliance Audits and External Communications Policy	1.19 min
vuln-mgmt Vulnerability Management	< 1 min
hr HR and Personnel Security Policy	1.30 min
data-mgmt Data Management Policy	1.01 min
facility Facility Access and Physical Security Policy	1.30 min
system-audit System Audits, Monitoring and Assessments Policy	< 1 min
threat Threat Detection and Prevention Policy	< 1 min
vendor Third Party Security, Vendor Risk Management and Systems/Services Acquisition Policy	1.02 min
mdm Mobile Device Security and Storage Media Management	1.06 min

intro Introduction to document approval

Mark As Read & Understood

Procedure

This is the first document you should read to understand how we want to communicate policies and procedures to you. A distribution is a grouping of multiple policies and/or procedures that Management decided on and would like you to carefully review, understand and apply.

Overview

- On the left top you see all the distributions assigned to you.** We only require you to formally read and approve the policies, but we count on your best effort to understand and apply the related procedures in your day-to-day work.
- On the left side of this text you see a list of documents from the current selected distribution (ISMS · policies).** Please open and read them one by one starting from the top.
- For documents where we need your approval, you'll see a red button with "Mark as Read & understood" on the right top.** By clicking on it, you are providing auditable proof and confidence in your compliance with the content defined in that document.
- As you will need to approve multiple documents, you'll see your overall progress in the top left.** The distribution with procedures does not require you to mark as read, so no progress is shown in that case.
- Some people might get some additional department specific distributions assigned to them.** If this applies to you, you will see multiple distributions in the top left.

In case some links inside a document indicate that you have no permission, this means they are not part of distributions assigned to you. If so, you do not need to provide your explicit understanding/approval, so that you can proceed to ignore them.

Please note that policies and procedures are versioned and can evolve over time to align with the business evolution and new requirements. This means that you may receive new invites in the future to approve those new versions. They will be easy to identify, as you will see non-approved documents with a red dot in front.

At any time you can consult the latest version of our policies and procedures with the following links (please make sure to bookmark them):

- ISMS - Policies
- ISMS - Procedures

Your participation and thinking with us is essential for our continuous improvement, so if you identify non-compliance with our policies, or if you have improvement recommendations or special remarks regarding the policies and procedures, it is your duty to report this to your Manager and the Compliance Team, so that we can properly document it and implement a correction. Please do so by sending an email to [security@...com](mailto:security@...) with your Manager in CC.

We kindly ask you to **Read and Mark as Approved** all documents in the list on the left. Once you've done so, they show as green.

Thank you in advance for your time and cooperation,

The Compliance Team

Document comments & activity

Add a comment

User interface - Distributions

You will receive an invite per mail to read and formally approve all policies

ISMS - Policies

Procedures
(23.30 min remaining) 0%

Introduction
Search document

●
intro Introduction to document approval
1.89 min

●
is-policy Employee Handbook and Policy Quick Reference
< 1 min

Policies
Search document

●
access Access Policy
1.97 min

●
asset-mgmt Asset Inventory Management Policy
< 1 min

●
risk-mgmt Risk Management Policy
< 1 min

●
rar Roles, Responsibilities and Training Policy
2.20 min

●
compliance-audit Compliance Audits and External Communications Policy
1.19 min

●
vuln-mgmt Vulnerability Management
< 1 min

●
hr HR and Personnel Security Policy
1.30 min

●
data-mgmt Data Management Policy
1.01 min

●
facility Facility Access and Physical Security Policy
1.30 min

●
system-audit System Audits, Monitoring and Assessments Policy
< 1 min

●
threat Threat Detection and Prevention Policy
< 1 min

●
vendor Third Party Security, Vendor Risk Management and Systems/Services Acquisition Policy
1.02 min

●
mdm Mobile Device Security and Storage Media Management Policy
1.06 min

intro Introduction to document approval

Mark As Read & Understood

Procedure

This is the first document you should read to understand how we want to communicate policies and procedures to you. A distribution is a grouping of multiple policies and/or procedures that Management decided on and would like you to carefully review, understand and apply.

Overview

1. **On the left top you see all the distributions assigned to you.** We only require you to formally read and approve the policies, but we count on your best effort to understand and apply the related procedures in your day-to-day work.
2. **On the left side of this text you see a list of documents from the current selected distribution (ISMS - policies).** Please open and read them one by one starting from the top.
3. **For documents where we need your approval, you'll see a red button with "Mark as Read & understood" on the right top.** By clicking on it, you are providing auditable proof and confidence in your compliance with the content defined in that document.
4. **As you will need to approve multiple documents, you'll see your overall progress in the top left.** The distribution with procedures does not require you to mark as read, so no progress is shown in that case.
5. **Some people might get some additional department specific distributions assigned to them.** If this applies to you, you will see multiple distributions in the top left.

In case some links inside a document indicate that you have no permission, this means they are not part of distributions assigned to you. If so, you do not need to provide your explicit understanding/approval, so that you can proceed to ignore them.

Please note that policies and procedures are versioned and can evolve over time to align with the business evolution and new requirements. This means that you may receive new invites in the future to approve those new versions. They will be easy to identify, as you will see non-approved documents with a red dot in front.

At any time you can consult the latest version of our policies and procedures with the following links (please make sure to bookmark them):

- [ISMS - Policies](#)
- [ISMS - Procedures](#)

Your participation and thinking with us is essential for our continuous improvement, so if you identify non-compliance with our policies, or if you have improvement recommendations or special remarks regarding the policies and procedures, it is your duty to report this to your Manager and the Compliance Team, so that we can properly document it and implement a correction. Please do so by sending an email to [security@... .com](mailto:security@...) with your Manager in CC.

We kindly ask you to **Read and Mark as Approved** all documents in the list on the left. Once you've done so, they show as green.

Thank you in advance for your time and cooperation,

The Compliance Team

Document comments & activity
●

●

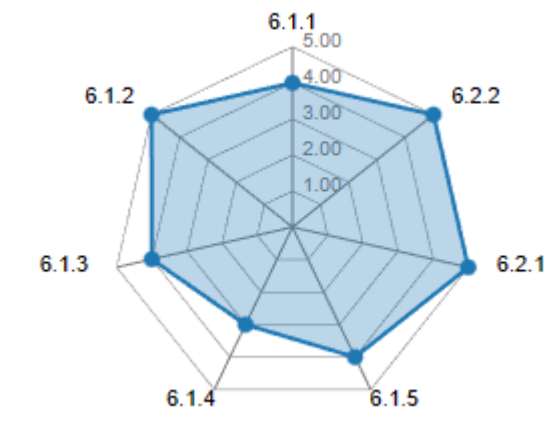
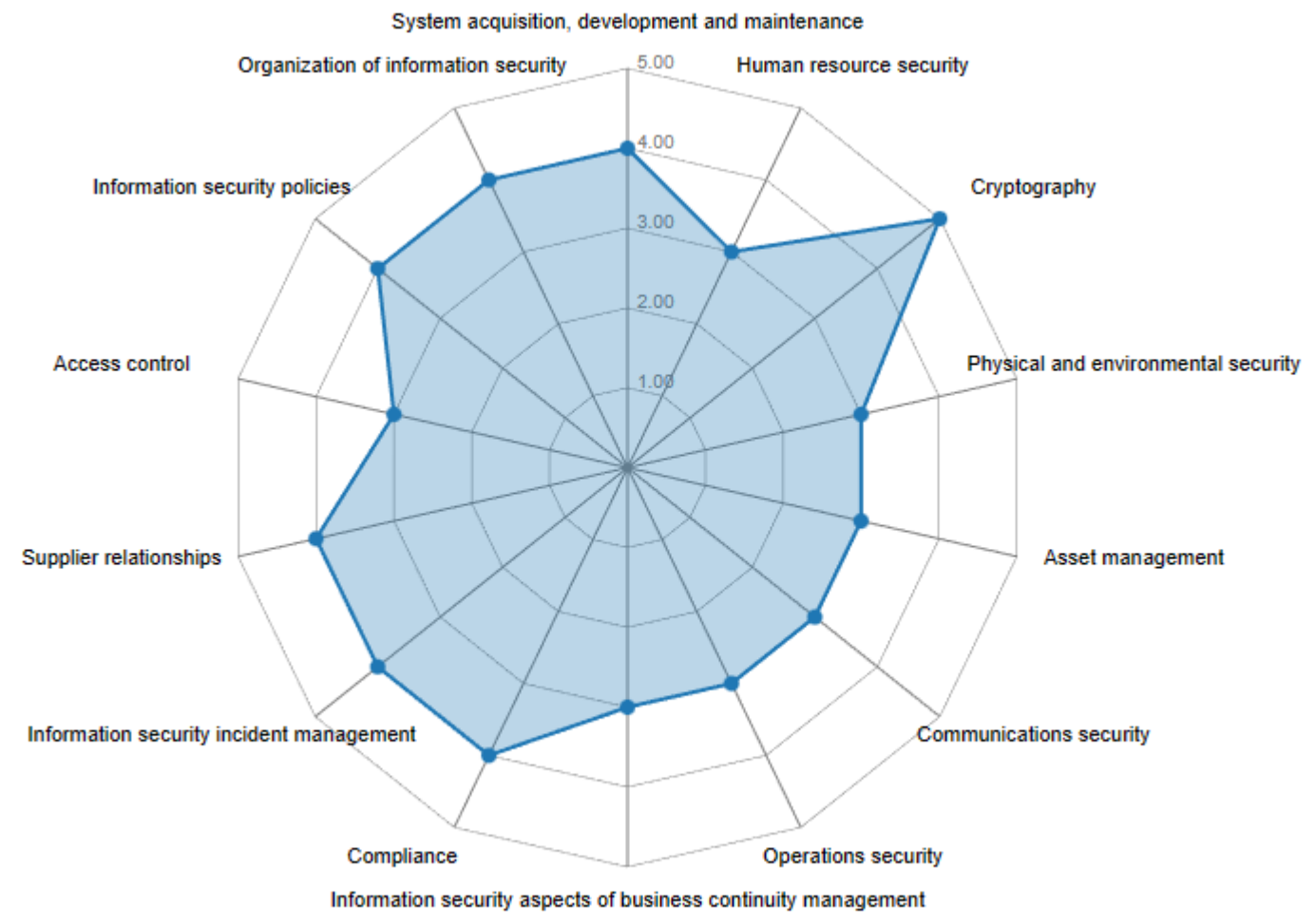
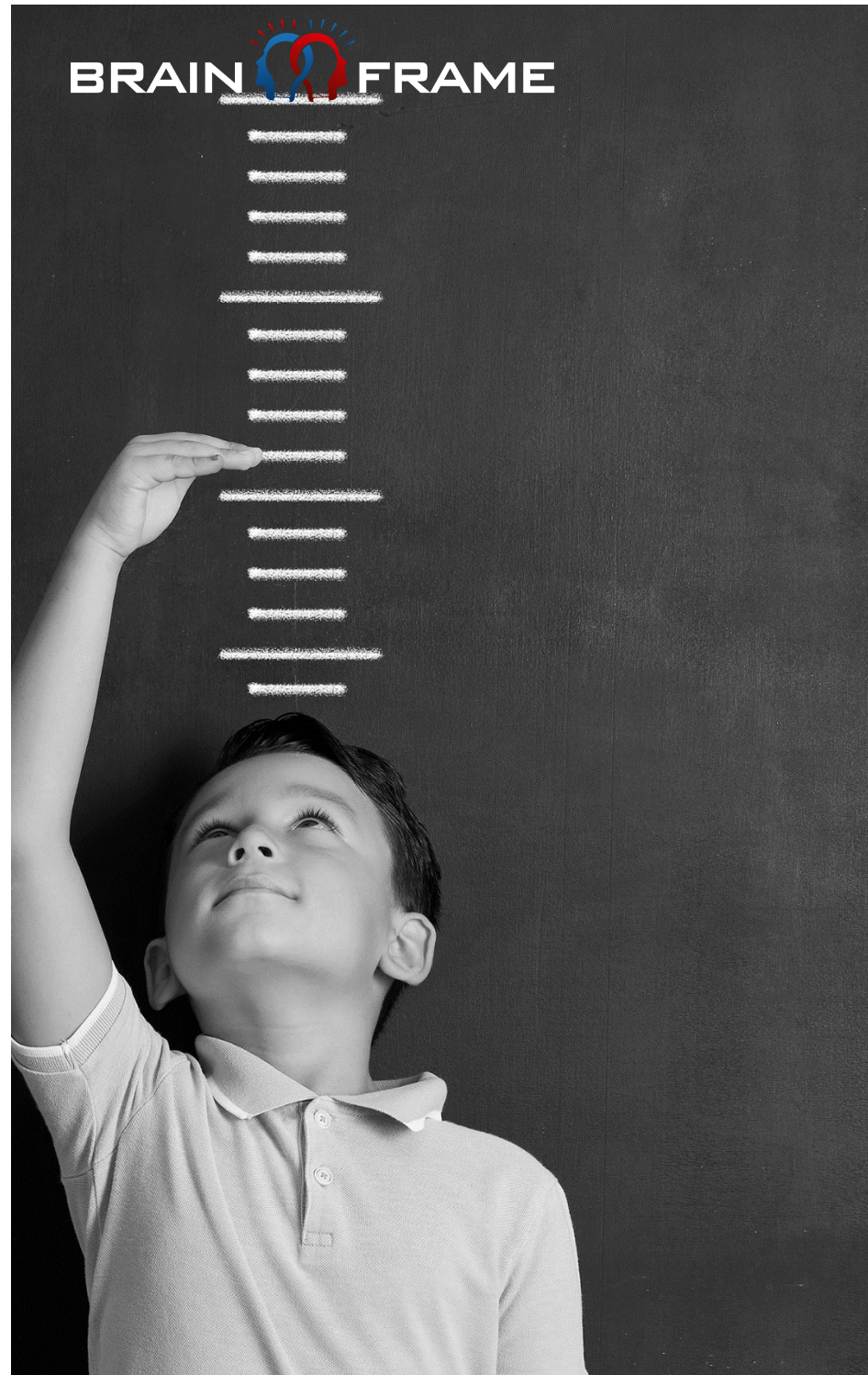
Works with Any Standard or Framework



- Perfect for multi-standard mapping
 - *ISO27001*
 - *ISO9001*
 - *NIS, NIS2*
 - *ISO27017*
 - *ISO13485*
 - *GDPR*
 - *ISO27701*
 - *FSSC CSSF PSF*
 - *NIST*
 - *SOC 2*
 - *DORA*
 - *HIPAA, ...*
- Build your own framework/requirements
- Track policy & procedure relations
- One central place to store all your evidences
- Link your requirement applicability to risks



Easily Track your Compliance Maturity Visually



- 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

User interface - Frameworks

Search

- Files
- Tasks
- Workbench
- Overview
- Primary assets
- Vendors
- Forms
- Timeline
- Risks
- KPIs
- Collections
- Distributions
- SoA**
- Ideas/Roadmap
- Profile
- Settings
- Logout

ISO/IEC 27002:2022

+ Add SOA



A.5.1 Policies for information security

Applicable and implemented - MANAGED

Linked controls

POL-ALL-01 Policies for information security

Applicable and implemented - MANA...

Evidence of implementation

Commitment on Confidentiality.docx

Related risks

R-001 Missing protection against distributed denial of service DDoS attacks

Linked Tasks

Review information security policy

JB

Configure planning

Edit Task

A.5.2 Information security roles and responsibilities

Applicable and being implemented

Linked controls

cp-role-assignment Assignment of Roles and the Security Committee

Applicable and implemented - DEFIN...

Notes

A.5.3 Segregation of duties

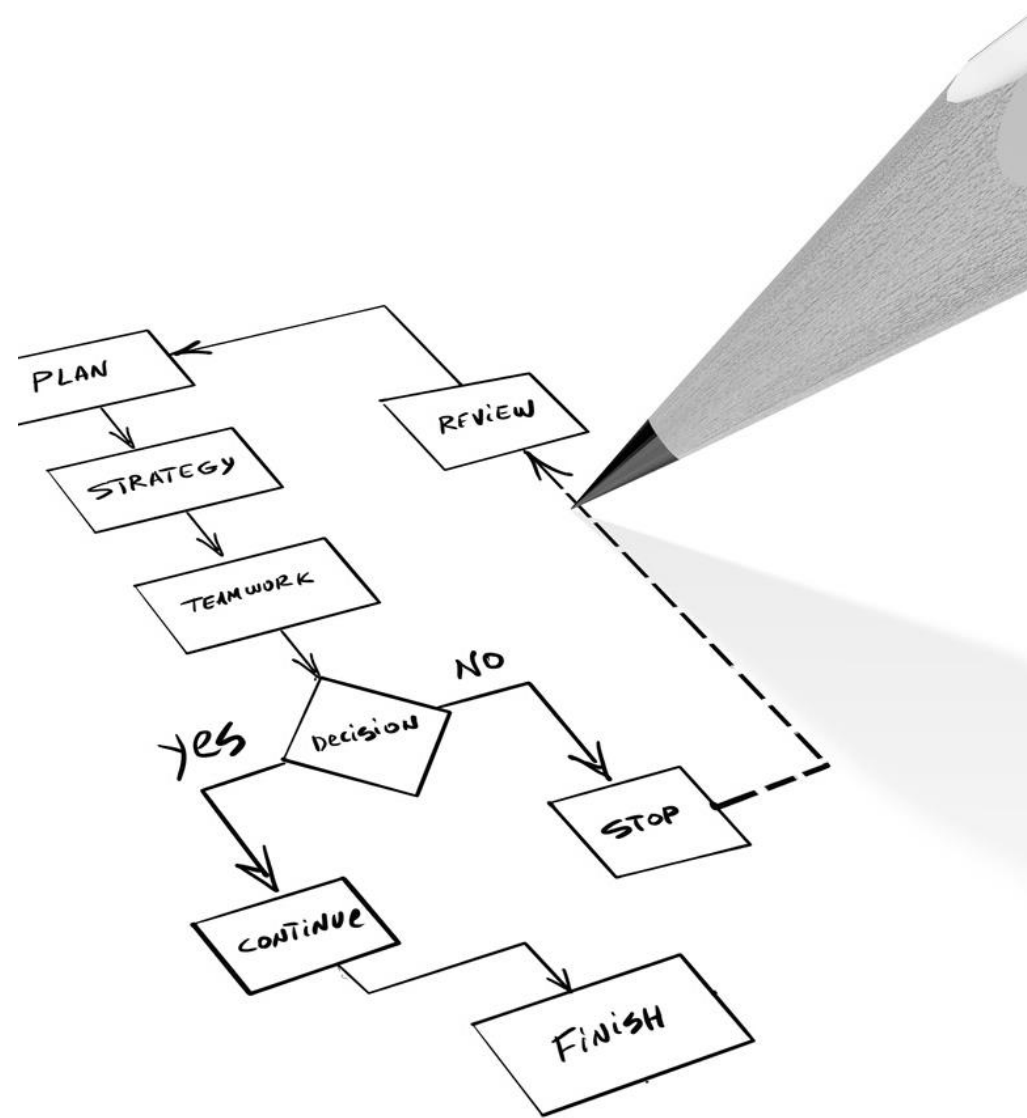
Applicable but not implemented

Linked controls

cp-role-assignment Assignment of Roles and the Security Committee

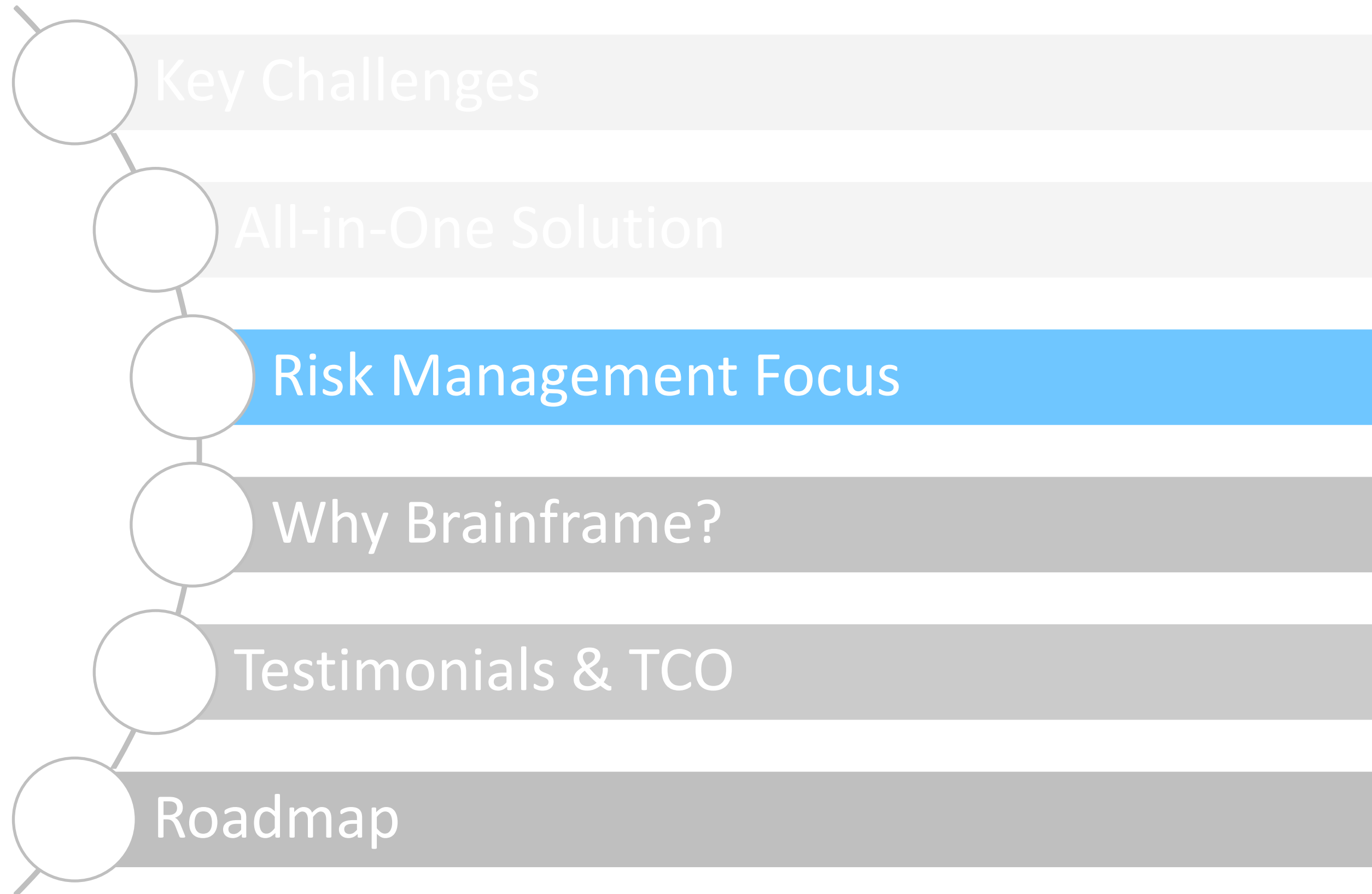
Applicable and implemented - DEFIN...

Internal Tool for Process Flow or Diagram Design



- Quickly draw any process/diagram flow.
- Duplicate or Adapt Existing flows.
- Allow Draft and Published versions.
- Officially Track diagram versions.
- No more external tools needed.

Agenda



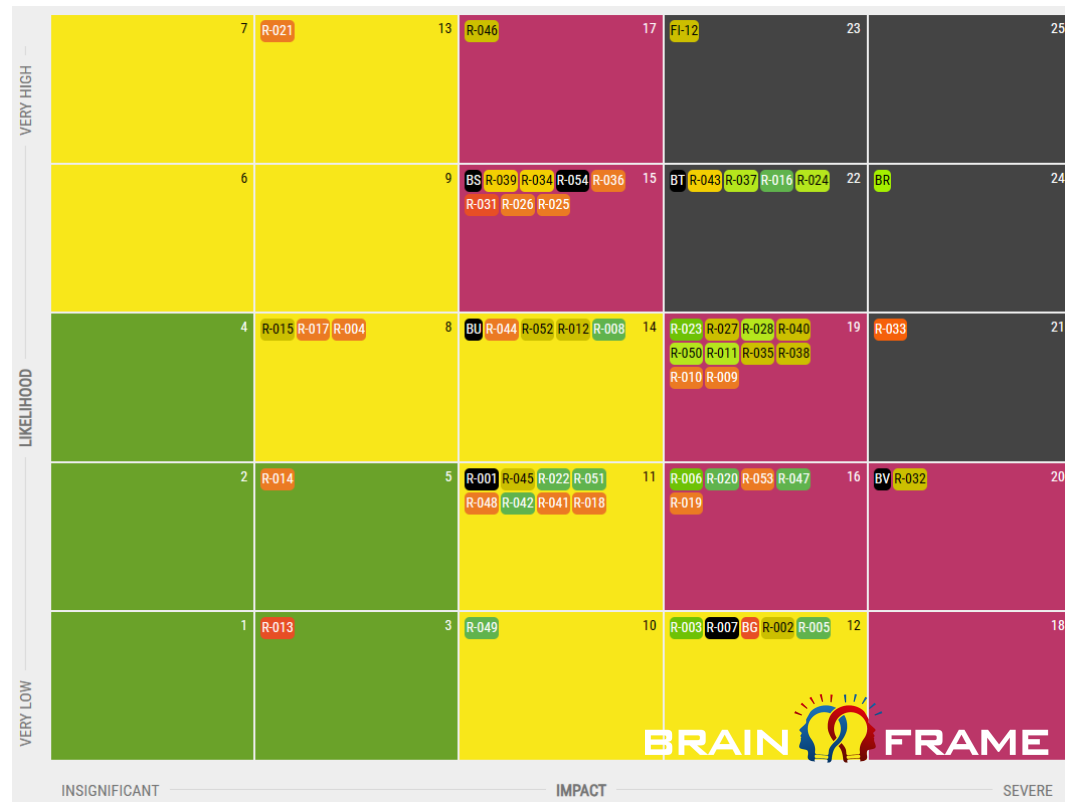
We Help You Keep the Focus on Actual Risks

The ultimate purpose of a GRC solution is to **efficiently identify, reduce and/or eliminate actual risks** that can impact your business. Using our **visual asset dependency representation and auto-documentation**, combined with **context aware risk views** (per product/department/...) and a **built-in task management with automatic risk evolution/prediction**, we bring a new approach on how to efficiently manage risks.



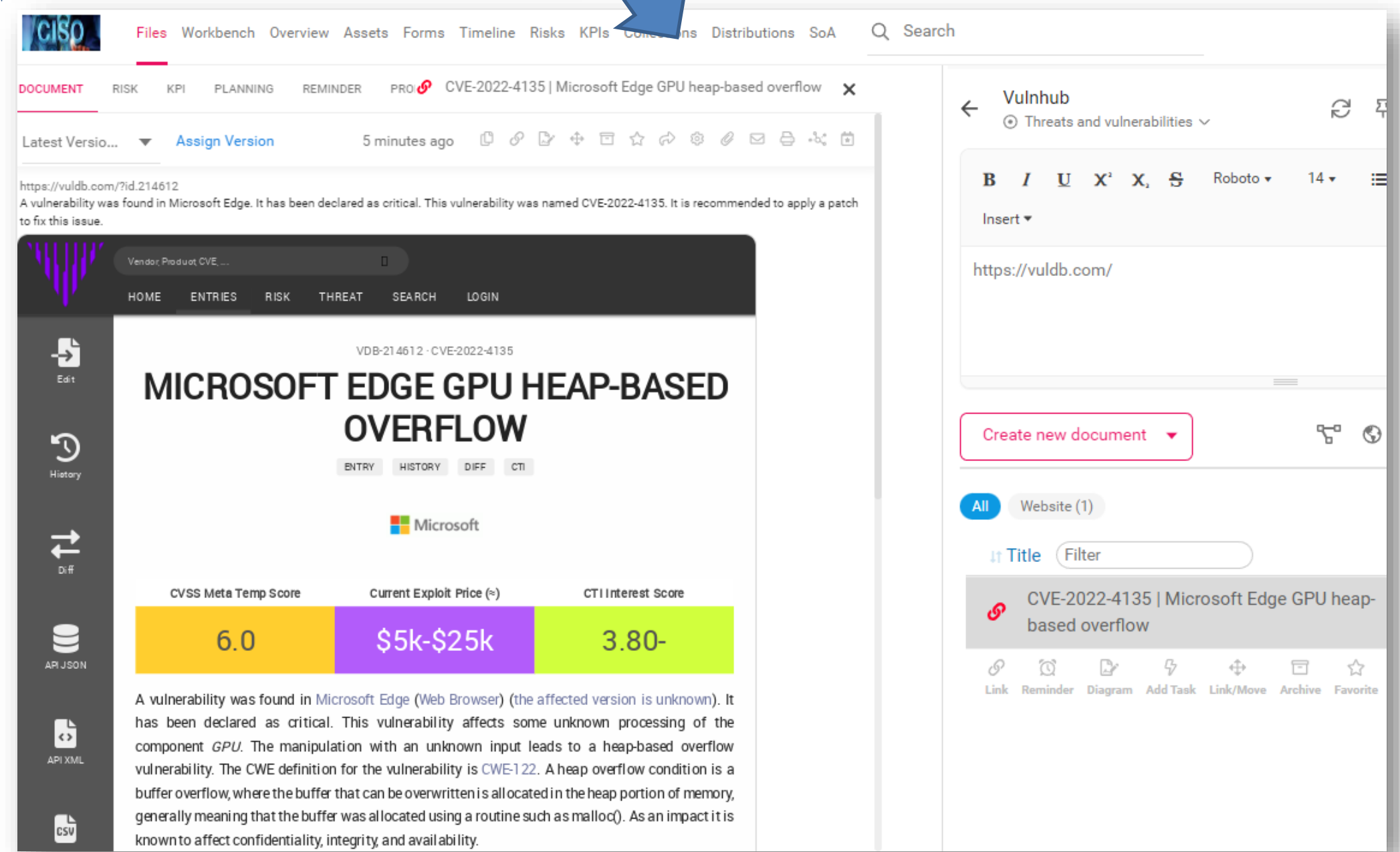
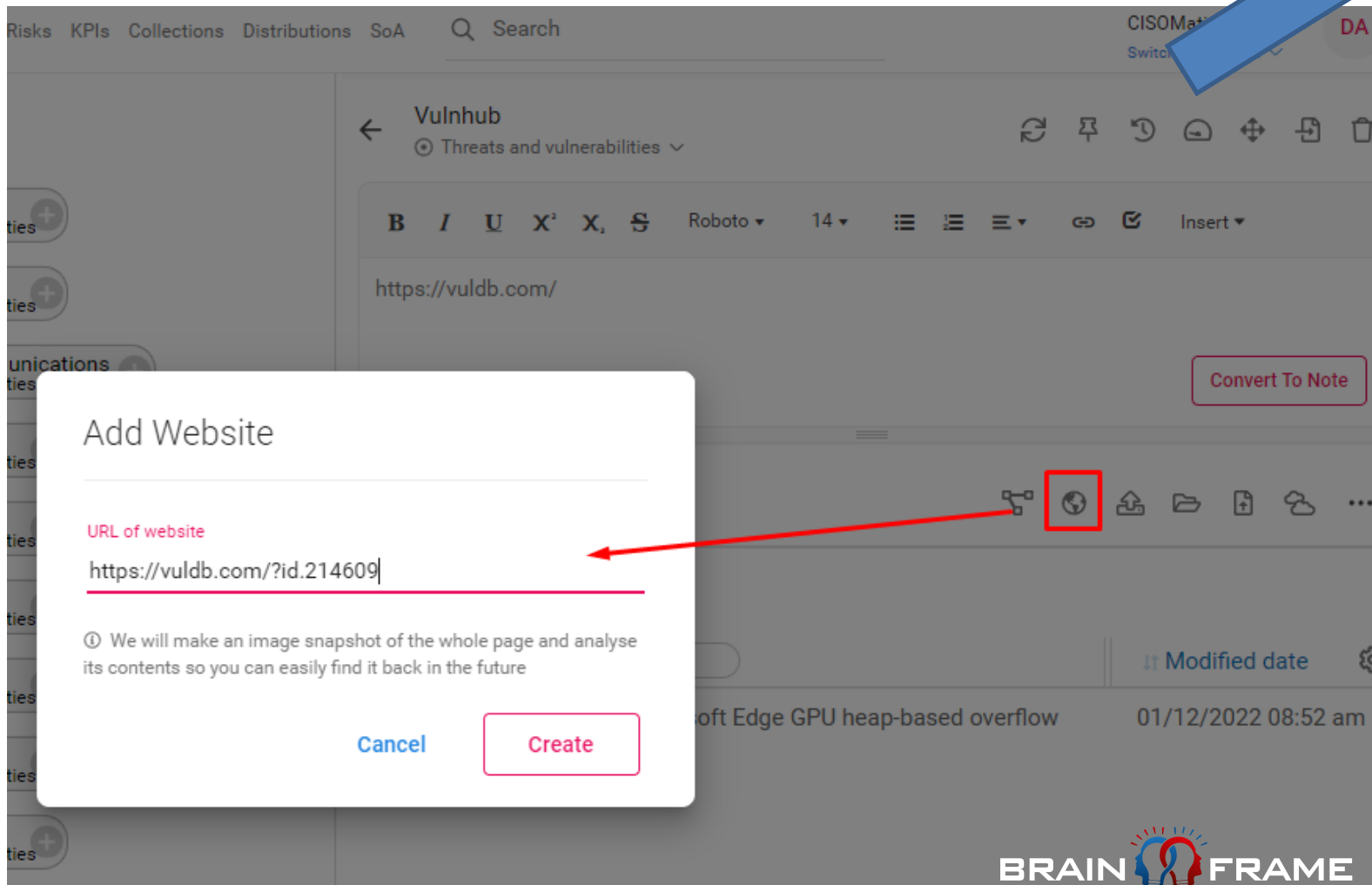
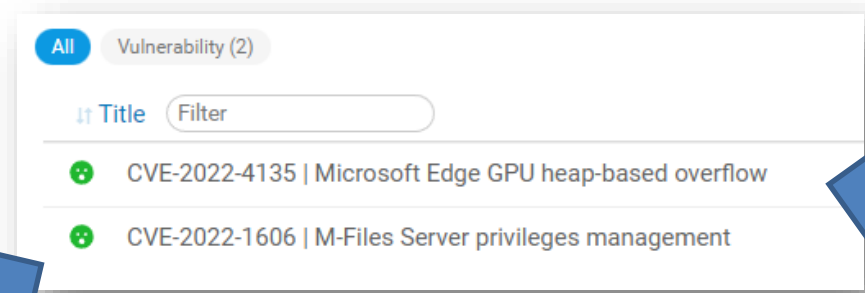
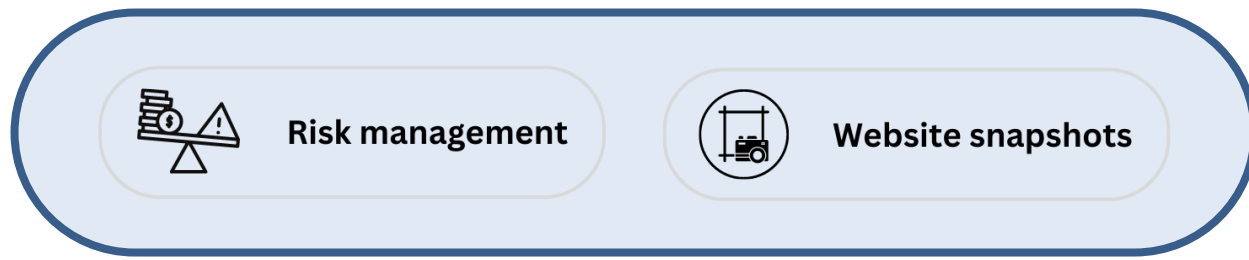
Simple & Effective

On our roadmap



- Manage multiple risks types (eg CIA, Suppliers, Employees, Non-conformities, Stakeholders, ...) with self defined measures/properties.
 - Intuitive risk matrix with quick view on remaining work and risks that need to be reviewed.
 - Directly map your risks to framework requirements.
 - Track risks and related work on Kanban boards that can be fully aligned with your process.
 - Automatically calculate risks based on questionnaire form replies.
- Financial/Quantitative risk management.
 - AI assisted risk identification & documentation.
 - Cyber defense matrix mapping of controls to quickly identify gaps on your assets.
 - Automated replies to security questionnaires you receive.

Quickly Document New Vulnerabilities



User interface – Risk management

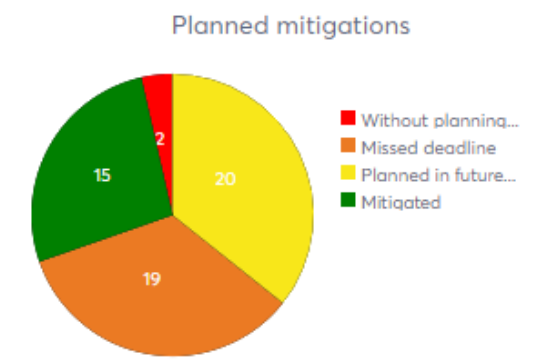
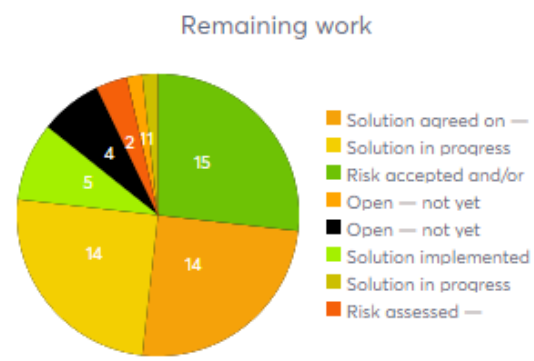
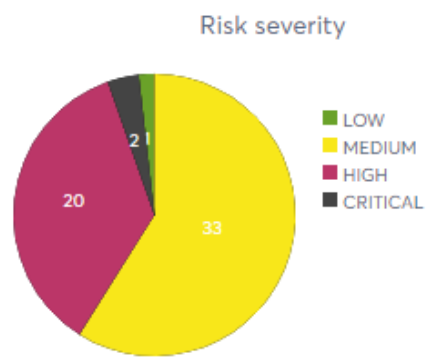
Search

Create New Risk

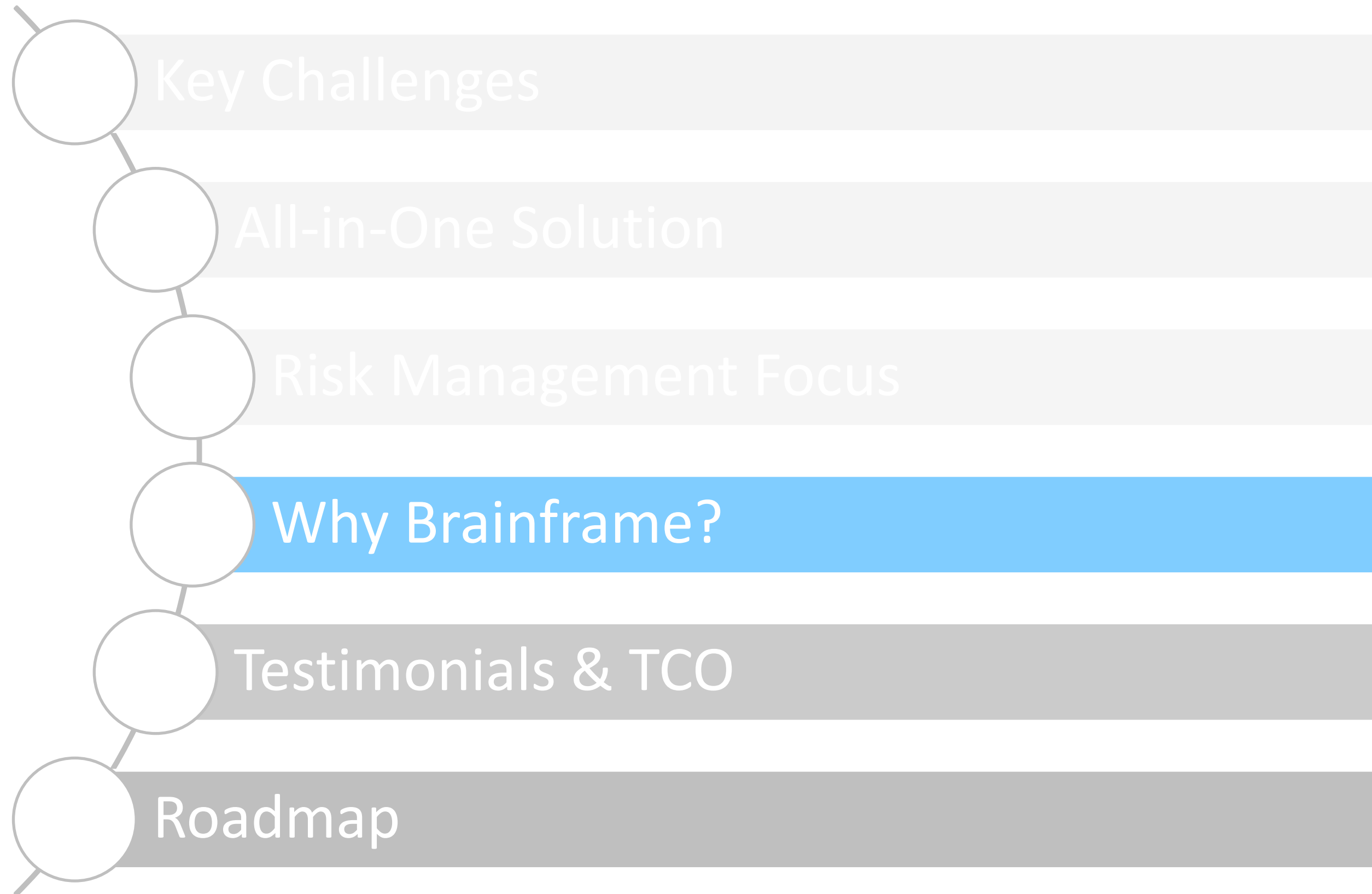
Filter risks

Confidentiality, integrity and availability Risk

- Builder
- Files
- Tasks
- Workbench
- Overview
- Primary assets
- Suppliers
- Forms
- Timeline
- Risks**
- KPIs
- Collections
- Distributions
- SoA
- Ideas/Roadmap
- Documentation
- Profile
- Settings
- Logout



Agenda



Why Brainframe?

Brainframe takes away the complexity - and anxiety - of GRC tasks with an operational implementation that puts the user experience and ease-of-use first. User benefits come directly from an embedded intelligence (continuously adapted from field experience and regulations), process automation with templates and AI-driven logic. Onboarding services are strongly reduced via straightforward integration embedding existing available documentation and connecting to existing platforms.

Brainframe empowers CISO and risk management professionals in their duties and assures GRC success across the entire organization from day one.



Customer is Gold

- Small company = 100% customer focus. ALWAYS!
- Any type/size/compliance state is readily supported
- You define our agile roadmap
- Non-Disruptive onboarding (come as you are!)
- Cloud or self-hosted for more control

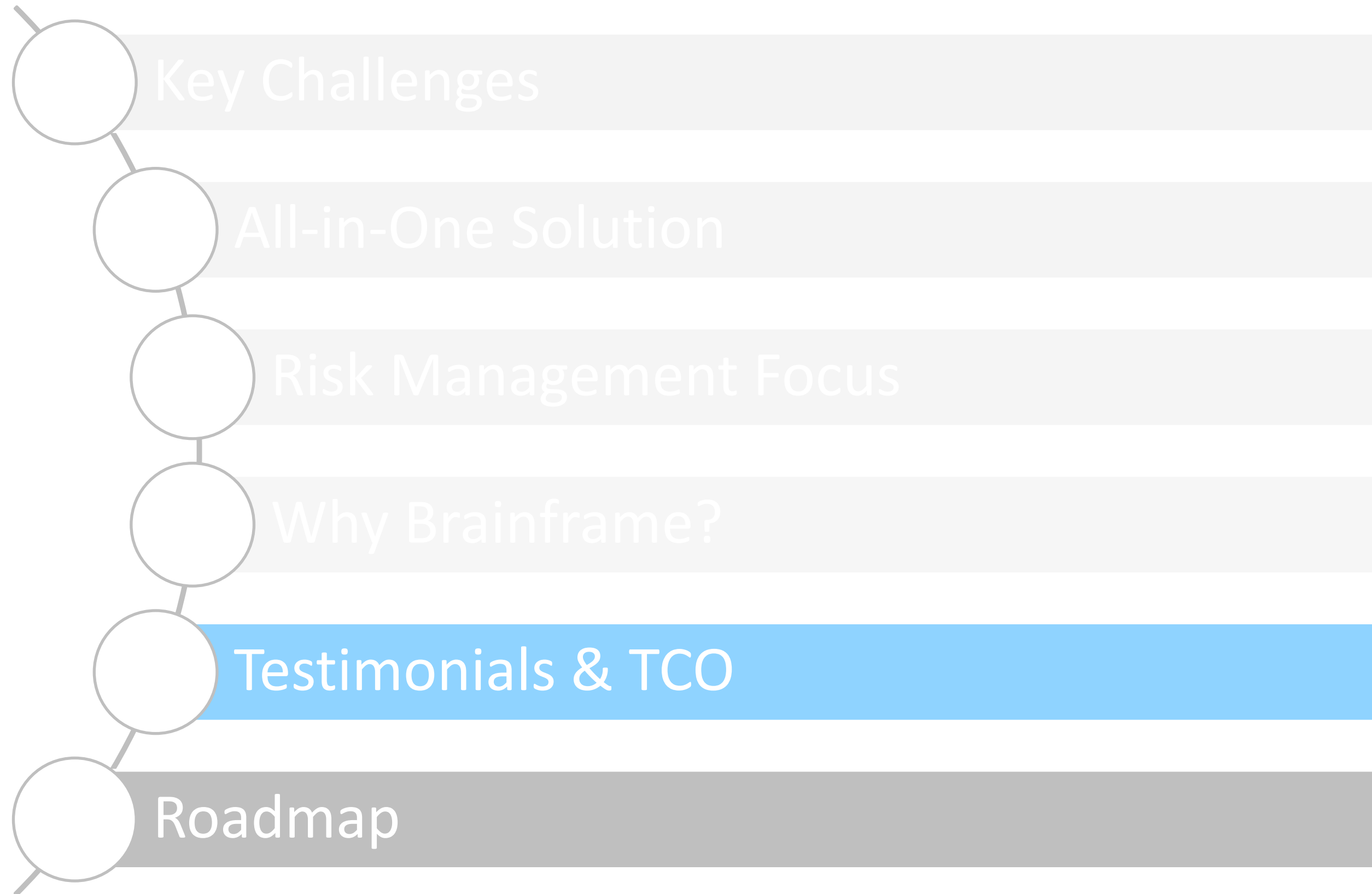
Cost Effective

- Integrated All-in-one solution
- All modules included (don't compromise on security/quality)
- Company based pricing (no user pricing)
- Focus on saving time, reducing costs and minimize risks

Value Focus

- Feature-Rich product with intuitive navigation
- Focus on risk reduction
- Value for In-house specialists AND Consultants
- Knowledge retention
- Keep all corporate and functional levels close to the IT security and compliance reality

Agenda



Brainframe Customer Testimonials

Brainframe is on the market since early 2022 and is proud of its growing customer base of **30+ companies in different domains** (fintech, governments, insurance, healthcare, MSP, consulting, IOT, security, ...) with **ZERO CHURN** to-date!

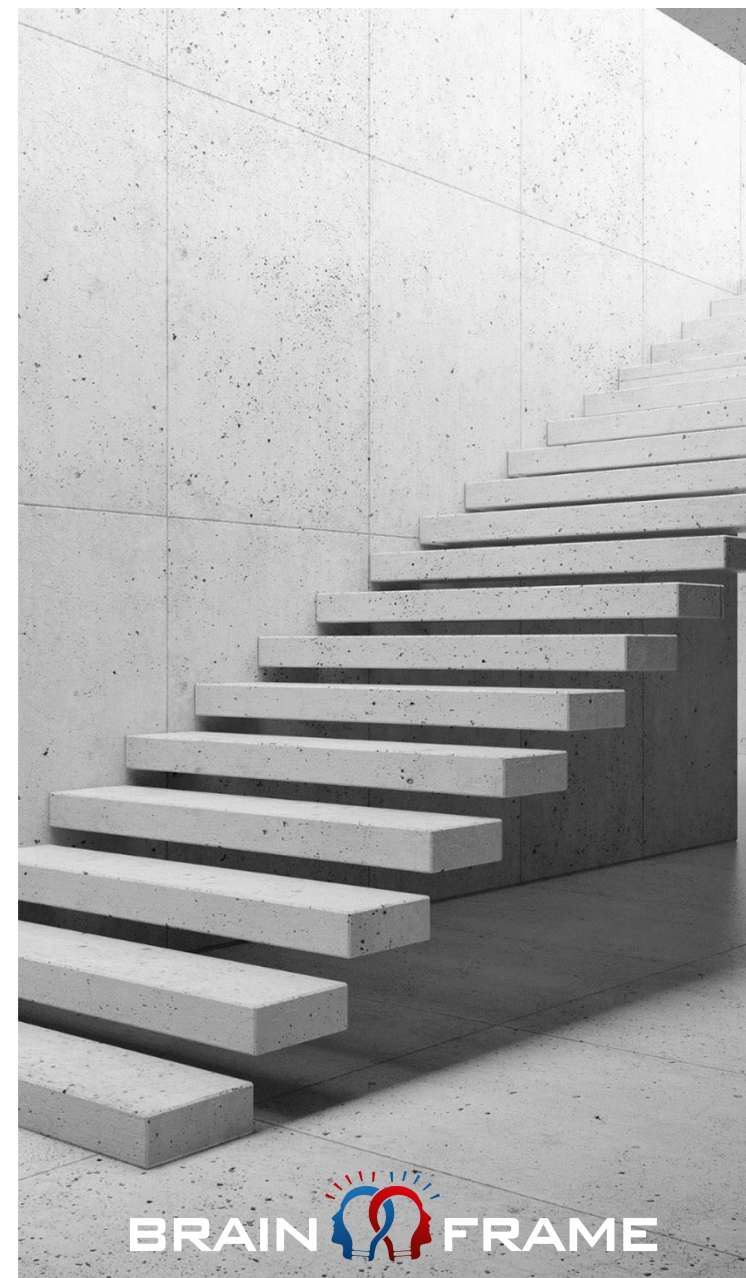
This accounts for **more than 500 satisfied and successful users that interact with our service on regular basis to improve and control their GRC.**

*“Brainframe is the solution I wanted to work with at the start of my career, because it allows me to **easily manage all the tasks that fall to a CISO**. In terms of compliance, the controls carried out and the evidence of these controls, all our assets and the risks associated with these assets, are **all in one place**.*

*Thanks to the **flexibility** of this solution, I've been able to continue using and centralizing my existing documents. This centralization has enabled me to **save many hours in managing our GRC program**.*

*The **Brainframe team listens to our needs and thinks along with us at a management level**, providing advice on best practice while implementing the new features we request very quickly.”*

Jean-Yves MATHIEU
CISO NATIXIS BANK



*“As a consultant, time is money. Using Brainframe **saves many hours per week** by centralizing all the management in one place.*

*We were able to **implement our own methodology** and way of working into the platform allowing us to keep a strong competitive edge while at the same time standardizing our way of working with all customers and significantly **reducing the onboarding time** for new clients.*

*I love how quickly the product is evolving, constantly **adding new features** that make sense **without additional costs/upselling.**”*

Luc COTTIN
CISO Rcube, CEO Rsecure

Use Case – Natixis Bank

Brainframe was chosen by Natixis in early 2022, with the main aim to fully digitalize the GRC program of the bank.

In less than 30 days their key GRC processes were migrated to Brainframe thanks to the support of our GRC experts



Targeted issue(s)

Missing digitalization

- Difficult to manage multiple certifications/standards/regulations COST ↑
- Challenging to align management teams COST/RISK ↑
- No clear view on risk/compliance status RISK ↑
- Time consuming document approvals and other process implementations in the field COST ↑
- Difficult to manage/delegate/track tasks, risks and non-conformities COST/RISK ↑
- Challenging to properly document/understand assets and their dependencies COST/RISK ↑

Solution

Brainframe GRC platform

- Holistic GRC management solution
- All you need to manage in one Digitalization
- Compliancy visibility & Maturity Level
- Unique everything-is-a-document approach

Value for Natixis bank

Risk & cost reduction

Direct benefits

- Fast import and integration of existing documentation COST ↓
- Context aware view of tasks/risks/non-conformities RISK ↓
- Simple + effective risk management & prediction RISK/COST ↓
- Easy-to-use tool for internal/external managers COST ↓

Indirect Benefits

- Self hosted allowing us to fully protect the way we want RISK ↓
- Top-notch DMS system COST ↓
- Automation with forms to bring information to CISO/DPO RISK ↓

Use Case – Rcube, R carré & Rsecure Luxembourg

Brainframe was chosen by Rcube, R carré and Rsecure consulting in early 2022, to help scale the management of multiple customers

Today they manage the GRC work/documentation for whole Rcube and many customers in a standardized way using Brainframe



<p>Targeted issue(s)</p> <ul style="list-style-type: none"> • Missing standardization among customers • Challenging to switch context between multiple complex customers • No central view for customer and us to track progress on tasks/risks/non-conformities and other works • Onboarding of new customers is time consuming • We had no “continuous link” with our end customers • Difficult Evidence collection and audit traceability 	<p>Missing digitalization</p> <p>COST ↑</p> <p>COST ↑</p> <p>COST/RISK ↑</p> <p>COST ↑</p> <p>COST/RISK ↑</p> <p>COST/RISK ↑</p>	<p>Solution</p> <ul style="list-style-type: none"> • Multi entity GRC management solution • All you need to manage in one Digitalization • Compliancy visibility & Maturity Level • Unique everything-is-a-document approach 	<p>Brainframe GRC platform</p>
		<p>Value for Natixis bank</p> <p>Direct benefits</p> <ul style="list-style-type: none"> • Low time to value for our customers due to fast onboarding • Clear view on risks/non-conformities per customer • Easy delegation/follow-up of tasks to customer • Standardization of compliance work <p>Indirect Benefits</p> <ul style="list-style-type: none"> • Ability to self host with our own domain name • Constant evolving DMS system with new free features • Easy adaptability of Brainframe to our customer’s needs 	<p>Risk & cost reduction</p> <p>COST ↓</p> <p>RISK ↓</p> <p>RISK/COST ↓</p> <p>COST ↓</p> <p>RISK ↓</p> <p>COST ↓</p> <p>COST ↓</p>

TCO: Maximize Savings and more Value over Time

At Brainframe, we realize GRC-related TCO is much more than just licensing or infrastructure costs.

With Brainframe, you will comprehensively address and **minimize all your GRC related costs, incorporating onboarding and constant value addition while reducing your risks.**



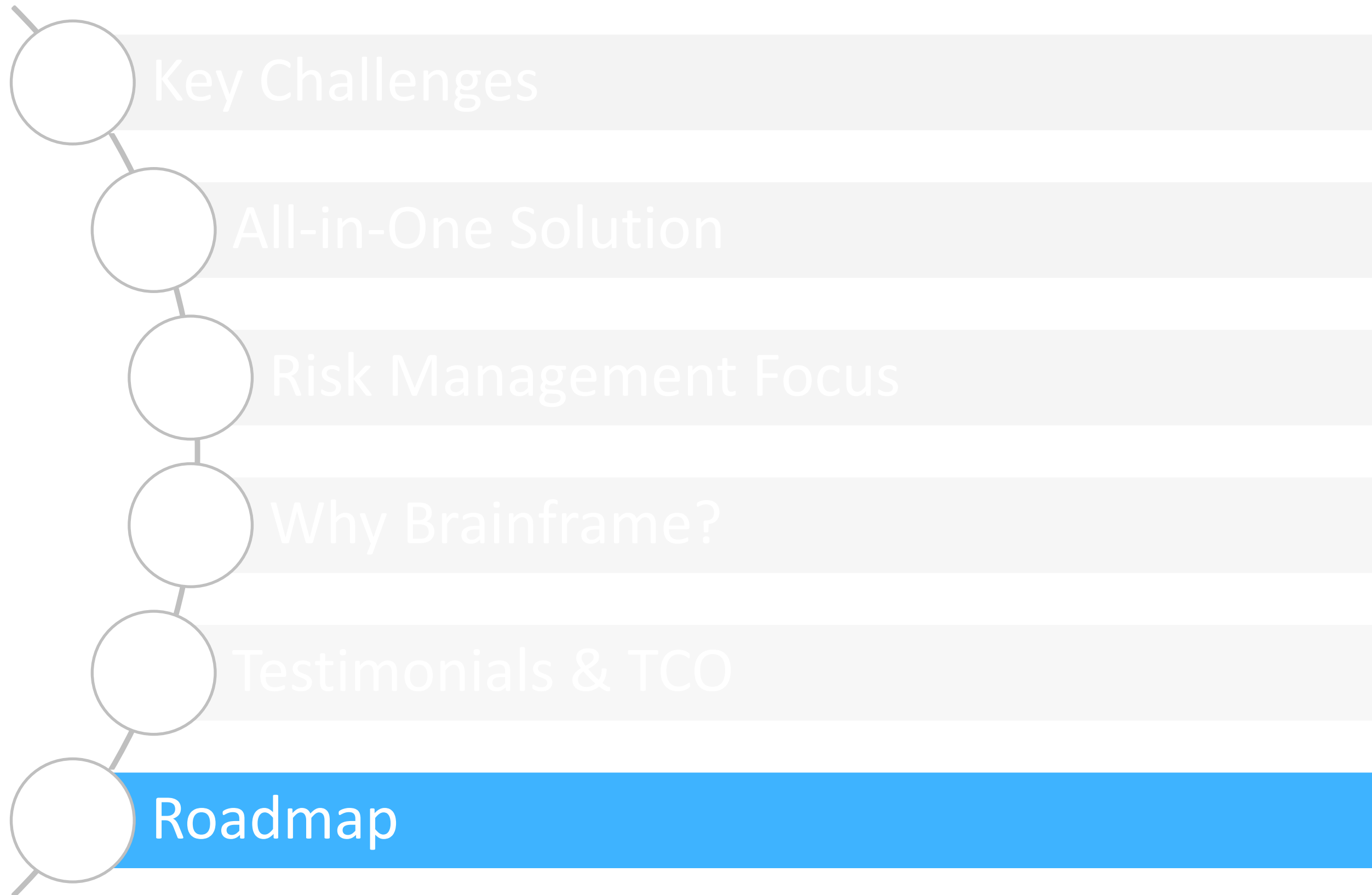
Some of the features that Brainframe implements to keep **your TCO** under control:

- AI power guiding you with best practices, document reviews, auto-documentation
- No development costs for new common features
- No hardware costs (*using cloud solution for optimized infrastructure*)
- No additional maintenance costs
- Just-In-Time access to specialists*
- Community driven knowledge and expertise sharing*
- Consulting & professional services for best practice onboarding
- Standardization of your compliance
- Integrated auditable trace & document storage
- Corporate Knowledge retention with constant auto-documentation
- No additional tools are needed for GRC management



Reduced governance, risk and compliance costs

Agenda



Brainframe Roadmap

You as a customer help define our roadmap by using the integrated ideas/voting system that allows us to keep **focused on your needs**. **Weekly cloud updates** are done using automated agile methods that never impact your operations. The **self-hosted solution receives monthly updates** including all cloud delivered improvements.

Y2024-Q2/Q3

Y2024-Q4

Functionality

- Document headers and revision tables
- Improvements on risk management
- AI copilot (automated onboarding, risks, policies, procedures, T&C review, DPAs, ...)
- Define review policies for document types (assets, vendors, workbench, risks, ...)
- Allow external contacts to do document approvals
- SOA audit & versioning
- Build your own compliance packages to share with community/customers including flexible rollout planner linked to deadline

- Multiple Integrations (Azure Devops, Google Docs, Monarc.lu, Serim, API, Snyk, ...)
- AI powered agents (document review/collection, report generation, automation)

- External auditor view integration
- Business continuity management
- Quantitative risk management
- Live content updates using plugins
- Self-service backups restores
- Custom report builder
- Gamification
- Cyber defence matrix mapping
- Threat intelligence integration
- Additional Integrations

Community

- Consultant directory
- Security software directory

- Auditor directory

- Security/Compliance events



(*) *DISCLAIMER: Brainframe Technologies reserves the right to change feature content or timing of this roadmap if customer priorities, industry standards or technology evolutions require so.*

OUR CONTACTS



+352 27867914

WWW.BRAINFRAME.COM

INFO@BRAINFRAME.COM

Luxembourg



<https://www.facebook.com/BrainframeCom>



<https://twitter.com/brainframecom>



<https://www.linkedin.com/company/brainframecom>



MADE IN
LUXEMBOURG
since 2016