

Cybermap 360

Getting Started USER GUIDE



Cybermap 360 is intuitive and should not require too many explanations. We have therefore developed a very minimalist user guide. If you have questions, do not hesitate to contact us via our website.

To access Cybermap 360 go to www.cybermap360.ch.

Table of Contents

Introduction	4
FIRST STEP: Setup	4
<i>Cybermap 360 information.....</i>	<i>5</i>
<i>Entity</i>	<i>5</i>
<i>Data map.....</i>	<i>5</i>
<i>Country adequacy.....</i>	<i>6</i>
<i>Employee roles.....</i>	<i>6</i>
<i>Employees.....</i>	<i>6</i>
<i>Teams</i>	<i>7</i>
<i>Guarantees</i>	<i>7</i>
<i>Process owner roles.....</i>	<i>7</i>
<i>Purpose of processing.....</i>	<i>7</i>
<i>Reason for treatment</i>	<i>8</i>
<i>Regulation</i>	<i>8</i>
<i>Backup plans.....</i>	<i>8</i>
<i>Recovery hours</i>	<i>8</i>
<i>Contract renewal cycles.....</i>	<i>9</i>
SECOND STEP: Providers	9
THIRD STEP: Systems	9
<i>General tab.....</i>	<i>10</i>
<i>Provider tab.....</i>	<i>10</i>
<i>Onboarding tab</i>	<i>10</i>
<i>Ownership tab</i>	<i>11</i>
<i>Data maps tab.....</i>	<i>11</i>
<i>Hosting tab (scroll-down menu)</i>	<i>11</i>
<i>Business continuity tab.....</i>	<i>11</i>
<i>Compliance tab.....</i>	<i>11</i>
<i>Security parameters tab</i>	<i>11</i>
<i>Risk assessment tab.....</i>	<i>12</i>

FORTH STEP: Security checklist	14
<i>Structure of a security checklist.....</i>	<i>14</i>
FIFTH STEP: Data protection and compliance	17
<i>Process tab</i>	<i>17</i>
Automated individual decisions, including profiling.....	17
High risk process, requiring more attention	17
Purpose of processing.....	17
Justification	18
<i>Process owner tab</i>	<i>18</i>
<i>Systems and Data tabs</i>	<i>18</i>
<i>Users.....</i>	<i>18</i>
<i>Processor</i>	<i>18</i>
DPO - Data Protection Officer.....	18
The Dashboard	18
Maps	19
Risk analysis	19
<i>Risk assessment.....</i>	<i>19</i>
<i>Internet exposure</i>	<i>19</i>
<i>Cloud exposure</i>	<i>19</i>
<i>Vendor appliance exposure</i>	<i>20</i>
Business continuity.....	20
<i>Business continuity tests.....</i>	<i>20</i>
<i>Business continuity results.....</i>	<i>20</i>
Improvements	20
Troubleshooting	21
<i>Error message or system not displaying anything.....</i>	<i>21</i>
<i>System in not responding</i>	<i>21</i>
<i>Cannot log in anymore</i>	<i>21</i>
<i>Getting an invoice.....</i>	<i>21</i>

Introduction

Most organizations are more and more dependent on information technology, including the internet and cloud computing. If [some of] your systems are not available, you might not be able to serve customers and have to stop your production. You might face reputational damage, face regulatory fines, or lose money. In some cases, it can even be more dramatic, and you might go bankrupt. Or it could cost the lives of people if you are an emergency provider.

On the other hand, cyber incidents are more and more frequent, from technical failures to cyber-attacks. To be ready to face a cyber incident, the first step is to know and understand your cyber footprint. That is, for example, understanding where your systems are hosted, which data they store, if they are securely set up, how much you are depending on the internet, if you have sufficient business continuity capabilities in place. Our experience shows that most companies, especially small and mid-size companies, do not have a good understanding of their cyber footprint or believe they do, but as soon as one starts asking more detailed questions, they either do not know the answers or give you approximative answers. Approximation is never good for protecting yourself against cyber incidents. You need to know and be ready.

Examples of questions you should be able to answer (the list is far from being exhaustive):

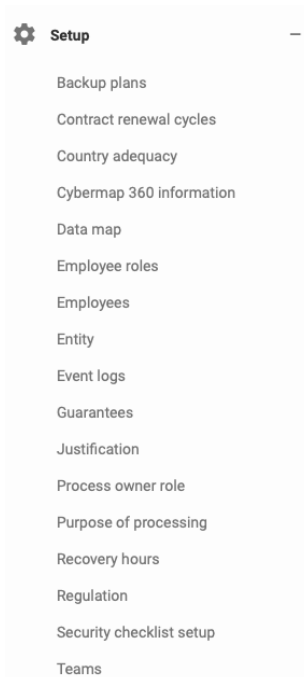
- Which systems are well set up and secure, and which have deficiencies that need fixing? By when will these deficiencies be fixed, and by whom?
- What systems will stop functioning if you lose access to the internet because of a denial of service attack?
- How much are you depending on the public cloud?
- How good are your business continuity capabilities? Have they been successfully tested?

Cybermap 360 will help you to define and understand your cyber footprint, assess the related cyber risks, and take appropriate actions to improve your cyber posture. Obviously, Cybermap 360 is not the silver bullet that will protect you against cyber events. You still need to deploy appropriate cyber defenses, like firewalls and anti-malware tools, to name two types of solutions. But with Cybermap 360 you will be better prepared to react to a cyber incident and know what to do.

FIRST STEP: Setup

Please note that in Cybermap 360, fields marked with a red asterisk are mandatory. Even if the other fields are not mandatory we strongly recommend to fill in as much information as possible.

First step is to go through the Setup menu and configure Cybermap 360:



While the menu is in alphabetical order, we present the different features to set up in a different order here.

Cybermap 360 information

You can define a main and deputy contact person. This is the name and email that are going to be used as people to contact in case of questions or problems. You should at least define a main contact person, ideally a Cybermap 360 administrator.

Entity

Many companies have multiple entities, and Cybermap 360 can manage your cyber footprint by entities. For example, you can have Company ABC, which has 4 entities, Switzerland, UK, USA, Japan.

If you only have one entity, just create your main entity. You can name it as you wish, either using the name of the country, calling it Headquarters, or anything else. You must at least have one entity.

The DPO is the Data Protection Officer.

Data map

The data map is where you define the types of data you store and work with in your business. A financial institution would have clients, positions, transactions, risk factors, etc. A retailer might have clients, providers, buying habits, products, etc.

You can create as many data types as you wish in your data map. The purpose of the data map is NOT to manage the hundreds or thousands of data elements you store in your systems but to define the main types of data you store. **Do not try to use Cybermap 360 to manage your full enterprise data schema.**

You can modify your data map at any time. But modifying your data map after having already created many systems in Cybermap 360 might be cumbersome, as you will have to go through each system again. **We encourage you to give your data map some serious thoughts upfront.**

Personal data is usually elements like a client's name, a client's address, a client's phone number.

Sensitive data is usually elements like religion, healthcare information.

Depending on the level of granularity you want to have in your data map, once suggestion is to use the following format:

data type: data element

For example, you could have

Employee: name
Employee: address
Employee: phone number

Country adequacy


The country adequacy is used to inform you about how much it is adequate to store data or not in a given country. The prefilled country adequacy reflects the view of Switzerland as of 2022.

Note: The user and the company using Cybermap 360 are responsible to ensure that the adequacy of countries is correct in regard to the legal and regulatory environments that apply to them. Cybermap360 SA is not responsible and cannot be liability for any incorrect country adequacy.

Employee roles

Before creating your employees and users, you need to define employee roles.

By default, Cybermap 360 has 5 roles that you can use, but cannot change: DPO (Data Privacy Officer), CCO (Chief Compliance Officer), CISO (Chief Information Security Officer), CIO/CTO (respectively Chief Information Officer and Chief Technology Officer), and CEO (Chief Executive Officer).


You can add as many employee roles as you wish using the .

We suggest that you create a *Generic* role, for all employees where their specific role does not really matter.

You might have multiple people on your compliance team. If you want all of them to be able to handle compliance activities, declare them as CCO. That will give them access to all compliance features.

Employees

Define all the employees that have a role with your cyber footprint. For instance, those who are system owners, or who have a responsibility towards cybersecurity.


Create your employees by using the .

An employee can or cannot be a user of cybermap. If you define an employee as a user, he will receive an email to activate his/her account. If they do not receive the email, ask them to check their spam folder.

Each user must have a user role:

- **Administrator:** has access to all features of Cybermap 360. Should be limited to 2-3 people;
- **Power user:** can access most features but not access some setup functions and user creation;
- **Viewer:** can only access Cybermap 360 in read-only and cannot make any changes.

For users who have a pending status, you can re-send an invitation email by clicking on the small icon in front of their "Pending for Verification".

User Status
Active
Pending for Verification 
Active

Teams

Teams are used in the *Data protection and compliance process*, where you can associate teams to processes.

Guarantees

Guarantees are used in the *Data protection and compliance process*, where you can associate guarantees to providers. Examples of guarantees are

- Legally binding instrument between public bodies;
- Binding corporate rules (BCR);
- Standard data protection clauses;
- Approved code of conduct;
- Approved certification mechanism;

Process owner roles

Process owners are used in the *Data protection and compliance process*. Examples of process owner roles are

- Main responsible
- Co-responsible
- Provider

Purpose of processing

The purpose of processing is the business reason for processing certain information. Examples of purpose of processing can be

- Conducting business
- Managing HR

- Managing financials
- Maintaining files


Reason for treatment

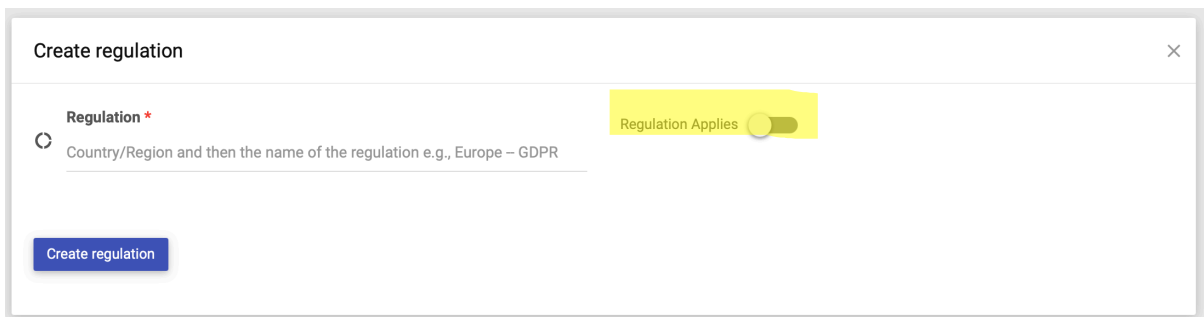
The reason for treatment is the legal justification for treating certain information. Typical reasons for treatments are

- Legal requirement
- Business Necessity
- By consent

Regulation

You can define all the regulations your systems must potentially comply with. We suggest you use the schema *Country name-Regulation*, e.g., in France, for GDPR, you would create the regulation *FR-GDPR*.

For each regulation you create, you can define if it must apply or not to new systems by default. I.e., if you turn it on Regulation Applies , the regulation will automatically be applied for any new system. You can still change it when you create new systems.



Backup plans

You can define the type of backup plans your systems must follow, e.g., *High retention, Low retention*. Or "7 days, 5 weeks, 5 months, 12 years" for 7 days in a row, 5 weeks in row, 5 months in a row, 12 years in a row. You can have as many retention plans as you wish but we suggest to have maximum 3 to 5.

Recovery hours

You can define your recovery hours for your business continuity plans. If you have a business continuity team, ask them to help you with the right recovery hours.

Standard recovery hours:

- 2 hours
- 4 hours
- 12 hours
- 24 hours
- 1 week

They will be used for your Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

The RTO defines for how long your business can sustain not having access to a system. For example, if you are a trading company, your RTO for your trading system would be between 0 and 2 hours. The RTO for your HR system would be anything between 2 to 5 days.

The RPO defines how much data you can afford to lose in case of an incident. We also measure the RPO in time. The RPO for your trading system would be between 0 and 2 hours. The RTO for your HR system would be 1-2 days.

Contract renewal cycles

You can define your contract renewals. This is useful if you want to manage your contract renewals in Cybermap 360. Ask your legal team to help you with contract renewal cycles.

Standard contract renewals:


- Yearly
- Every 2 years
- Every 3 years
- 4 Years
- 5 Years

SECOND STEP: Providers

It is now time to create your systems' providers. We strongly recommend managing your providers if you want to be accurate about understanding your cyber footprint and its associated risks.

ATTENTION: This is not about managing all your providers, e.g.: your office cleaning provider or your office furniture provider. This is ONLY about providers of IT systems in relation to your data and processes.

When creating a provider, you should give it a name. We strongly recommend also indicating the country and an email address.


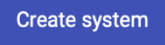
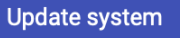
Once you have created a provider, you can create the provider's key contacts you have, using .

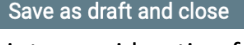
From a cyber security perspective, you should have a key cybersecurity contact for each provider you have. E.g., whom to contact to get help and support in case of a cyber incident.

THIRD STEP: Systems

It is now time to start mapping your cyber footprint, which is entering all the systems you are using. An **information system** is a formal, organizational system designed to collect, process, store and distribute information. The most frequent systems in companies are, for example, an ERP, an Email system, an HR-Management solution, a CRM system. You want to be as exhaustive as possible. The information to provide is really straightforward in most cases, even for non-technical people. We are only documenting the information that requires more technical knowledge.

Our experience is that this exercise is very revealing. Initially, most people believe they have a solid view of their cyber footprint. When going through the questions and mapping all their systems, it often turns out NOT to be the case!

To add a new system, click on . You will now have to go through several tabs. When you are finished click on button  to save your data. If you need to add some changes within your system once it's created, you can do it. Use for this purpose button .

If you need to break during entering your systems, use button . All data will be saved as draft, but won't be active, which means won't be taken into consideration for the risk calculation. You will find your draft-system in your overview marked "light blue". You may come back later and continue fill in. Remember that until you don't click on "create system" button your system won't be active!

General tab

System status

The system status is important because only systems that are decommissioned are not included in risk assessments. Active, Testing, and Inactive systems are considered as they potentially expose your company to cyber risks.

Entity

You'll find a scroll-down menu corresponding to the entities you created under setup/entity.

Business criticality (scroll-down menu)

Cybermap 360 uses an industry standard business criticality ranking.

Business criticality	Explanation	Unavailability acceptable
Crown jewel	Most critical systems to run your business. If they are not available or compromised, it can have dramatic implications on your business	2-4 hours
Business critical	Critical systems to run your business. If they are not available or compromised, it can have important implications on your business	4-8 hours
Business crucial	Systems that are necessary but you cannot do without them for a day or two	24-48 hours
Not critical	Systems you could live without for multiple days, potentially a week or more	>48 hours

Data criticality (scroll-down menu)

Cybermap 360 uses an industry standard data criticality ranking.

Provider tab

The provider tab is optional but we strongly recommend that you fill in it. It enables you to have a higher reactivity in case of cyber incident.

ATTENTION: You'll find a scroll-down menu corresponding to the provider and provider employees you created under setup/provider.

Onboarding tab

Normally, before starting to use a new system, whether it is installed on premises, in the public cloud or at a provider, you should onboard it. Cybermap does not provide any specific template to onboard systems but enable you to store all onboarding documents, e.g., your own onboarding

template, ISO certifications, and any other documents you might have asked and/or received from the provider.

If you do not have an onboarding template, contact us and we will be happy to share one with you. That you can customize.

Ownership tab

Each system must have a system owner (it's the only mandatory field). A system owner must be an employee and a user of Cybermap 360.

You can also associate teams to systems here, that is what teams are using that system.

Data maps tab

That's where you select which type of data the system stores. So that you can know what data is in which system. You'll find a scroll-down menu corresponding to the data map you created under setup/data map.

Hosting tab (scroll-down menu)

Once again, even if all fields are not mandatory, we strongly recommend that you always complete all the hosting fields.

The hosting type can be:

- **Internal DC**, that is, in your own data centers
- **Cloud** for any public cloud provider like Microsoft Azure, AWS or Google Cloud
- **Third Party Hosted** when the solution provider hosts the solution for you like Bloomberg would
- Or **SaaS** (solution as a service) and in that case you might not know where it is hosted (you should ask during your onboarding process)

Business continuity tab

Your business continuity capabilities are fundamental in case of cyber incident. Document them properly.

Recovery Time Objective (RTO) defines for how long your business can sustain not having access to a system. For example, if you are a trading company, your RTO for your trading system would be between 0 and 2 hours. The RTO for your HR system would be anything between 2 to 5 days.

Recovery Point Objective (RPO) defines how much data you can afford to lose in case of an incident. We also measure the RPO in time. The RPO for your trading system would be between 0 and 2 hours. The RTO for your HR system would be 1-2 days.

Compliance tab

In the compliance tab, you define if a system must or not be compliant with the defined regulations (through turn-on/off button).

Security parameters tab

2FA

For 2-factor-authentication. For example through authenticator app, a code via SMS, an RSA key, or any other 2FA solution or equivalent.

Signon method

That's the one parameter where you might need help from a more technical person. In case your setup is not represented within the available options but you believe you have a solid setup, choose **Strong signon**.

If you access an application with 2FA, you can choose **Strong signon**.

Need internet in/out?

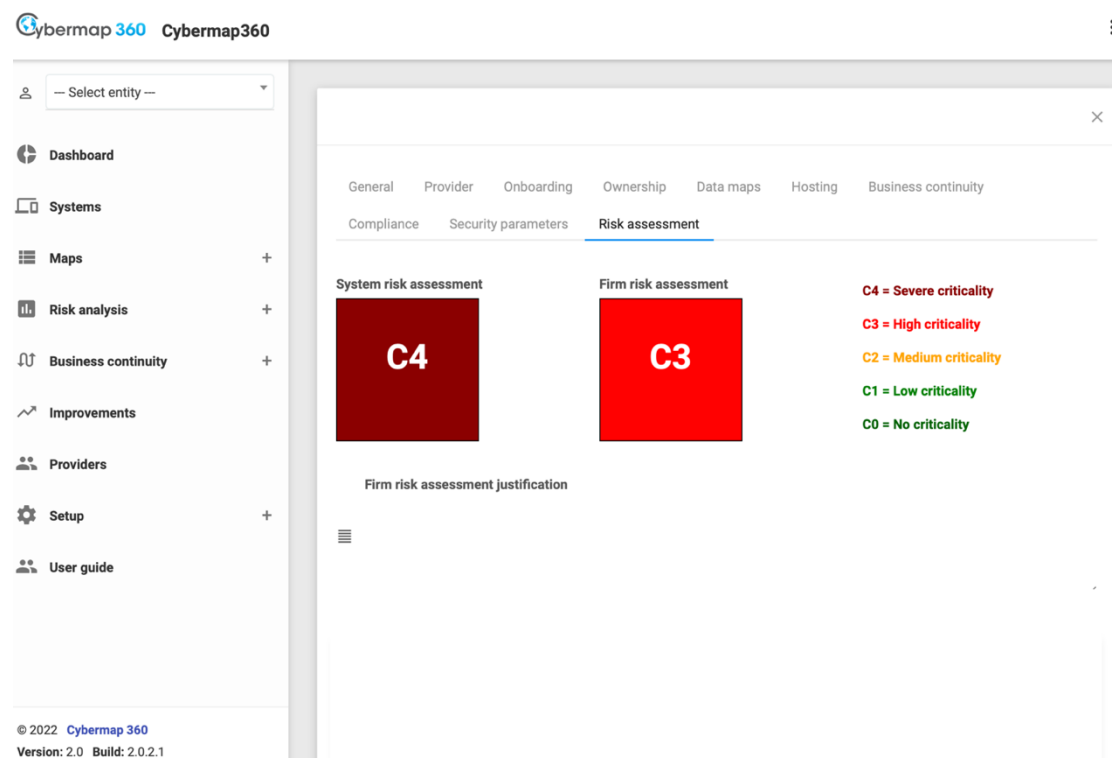
Does the system require internet in and/or out to work? And what's the impact if it's not available? If the answer to need internet in/out is "no", the impact must be **No impact**. Most systems will need internet in and out.

Appliance from vendor

Some vendors deploy some physical hardware within your network. This is the case for Bloomberg in some cases. Physical hardware is potentially an additional risk within your infrastructure that must be tracked. You can then describe the appliance deployed with **Appliance description**.

For instance, if you are a financial institution, the regulator, internal audit or external auditors would ask you if you have third-party providers' appliances within your network.

Risk assessment tab



System risk assessment

The system risk assessment is the risk calculated by Cybermap 360. You cannot change it. The categories are self-explanatory and defined on the right.

Any C4 and C3 requires immediate actions to reduce the risk exposure. A C2 is less critical but also requires actions.

If you look below the risk assessments, Cybermap 360 provides tailored recommendations on how to improve your systems' risk assessment.

Risk category	Recommendations
Two factor authentication	C4 - Assess alternative to 2FA
Data encryption at rest - Hosting type Cloud	C3 - Encrypt your confidential data at rest
Data encryption in transit - Hosting type Cloud	C3 - Encrypt your confidential data in transit

And you can define improvement actions that you can assign to people.

Firm risk assessment

Cybermap 360 might not know everything and overestimate or underestimate the risk assessment. You can modify the Firm risk assessment by clicking on it.

FORTH STEP: Security checklist

Cybermap 360 allows you to create a security checklist to ensure proper security measures are in place. This feature can be particularly helpful when preparing for audits or security certifications.

The first thing to do is to configure the security checklist in the setup menu.

Name your security checklist

Description: Put a description for your security checklist

Intervals **Green** : [1 - 1] **Orange** : [0.8 - 0.9] **Red** : [0 - 0.8]

Domains

Controls

Questions

To give a name and description to your checklist, click on the icon. You can also define intervals that will determine the color (red, orange, green) of the score displayed. It's important to ensure that your intervals do not overlap.

You can use the sharing icon to share the structure of your security checklist with any other company that uses Cybermap 360. This feature allows you to share your checklist without revealing your answers. To get the URL, simply click on the sharing icon. Then, provide the URL to the company with whom you want to share your checklist. To import it, the enterprise simply needs to click on the link.

Structure of a security checklist

A security checklist can include various domains, and each domain can have several controls. Each control can contain a set of questions, and some of these questions can be marked as "red flag" questions. Red flags are counts that indicate potential security vulnerabilities. The goal is to have no red flags in a secure company.

Define your domains:

Domains

Search:

Action	Domain
	Data center security
	End-user security









Showing 1 to 2 of 2 entries

Previous **1** Next















Controls

Questions

Define your controls:

Domains		
Controls		
  Search: _____		
Action	Domain	Controls
 	Data center security	Access controls
 	Data center security	Data center physical security
 	End-user security	End-user hardware
Showing 1 to 3 of 3 entries		
		Previous 1 Next
Questions		

Define your questions:

Domains				
Controls				
Questions				
  Search: _____				
Action	Domain	Controls	Questions	Red flag
 	Data center security	Access controls	Access controls are reviewed quarterly at minimum	<input checked="" type="checkbox"/>
 	Data center security	Data center physical security	Doors locked at all time	<input checked="" type="checkbox"/>
 	Data center security	Data center physical security	Surveillance camera	<input type="checkbox"/>
 	End-user security	End-user hardware	Accesss to devices is controlled via strong password	<input checked="" type="checkbox"/>
 	End-user security	End-user hardware	All computers have an anti-virus/malware installed	<input checked="" type="checkbox"/>
 	End-user security	End-user hardware	Anti-virus/malware are updated at minimum once a month	<input checked="" type="checkbox"/>
Showing 1 to 6 of 6 entries				
				Previous 1 Next

Which gives the following security checklist:

Name your security checklist

Description : Put a description for your security checklist

0 Score

0 Red flags

Calculate score Certify Compare with previous Certified checklists

Data center security : Assess the security of internal and external data centers, including public cloud providers.

- **Data center physical security :**
Assessment of the overall security of data centers.
 - **Doors locked at all time?**
 Yes Partially No
 - **Surveillance camera?**
 Yes Partially No
- **Access controls :**
Assess the access controls.
 - **Access controls are reviewed quarterly at minimum?**
 Yes Partially No


End-user security : Assess the security of end-user computing devices.

- **End-user hardware :**
Assess the security of end-user hardware.
 - **All computers have an anti-virus/malware installed?**
 Yes Partially No
 - **Anti-virus/malware are updated at minimum once a month?**
 Yes Partially No
 - **Access to devices is controlled via strong password?**
 Yes Partially No

FIFTH STEP: Data protection and compliance

Please note that Cybermap360 SA does not provide any legal or non-legal advice on data protection laws. Cybermap 360 is a tool to support companies with data protection and compliance, but just using the tool might not be sufficient in some cases and in some jurisdictions. Cybermap360 SA is not responsible and cannot be liable for any incorrect data protection and compliance matters.

Data protection refers to the safeguarding of personal information to ensure its privacy, security, and responsible handling. It involves protecting individuals' data from unauthorized access, use, disclosure, and destruction. By implementing appropriate measures and controls, organizations can ensure that personal data is collected and processed lawfully, transparently, and for specific purposes. Data protection aims to uphold individuals' rights and freedoms, promoting trust and accountability between individuals and organizations that handle their data. Through robust data protection practices, individuals can have confidence that their information is handled with care and protected against potential misuse or breaches.

To create a new process, click on . The information to be provided is straightforward. We will describe only specific fields.

Process tab

In the process tab, you can define the process by giving it a name, a description, and associating it to an entity.

Automated individual decisions, including profiling

Refers to the use of automated processes or algorithms to make decisions about individuals that have legal or significant effects on them. This involves the analysis and evaluation of personal data, often on a large scale, to predict or assess certain characteristics, behaviors, preferences, or performance of individuals.

High risk process, requiring more attention

Refers to processing activities that are likely to pose significant risks to individuals' rights and freedoms due to the nature, scope, context, or purposes of the processing. These high-risk processes may involve the handling of sensitive personal data, large-scale processing, systematic monitoring, or the use of new technologies.

Purpose of processing

The purpose of processing is the business reason for processing certain information. Examples of purpose of processing can be

- Provision of services
- Marketing and advertising
- Compliance with legal requirements
- User account management
- Analytics and research
- Consent management
- Employment-related purposes
- Security and fraud prevention

Justification

The justification for treatment is the legal justification for treating certain information. Typical reasons for treatments are

- Consent from data subject
- Legal obligation of the controller
- Protection of the vital interests of the data subject
- Public interests or official authority vested in the controller
- Current or future competitive economic relationship with another person
- Legitimate interests of the data controller

Process owner tab

The process owner can be a team, an employee, a provider or a mix of them. Each process owner must have a role.

Systems and Data tabs

Select the systems that are involved in the given process. By default, it associates the data that are part of the process.

Note: in this version, it is not possible to change the data involved.

Users

Define which teams and employees within your organization are involved in the given process.

Processor

Identify the different processors being involved, which are directly selected from your providers. If you want to add a processor, you need to add it to your providers.

DPO - Data Protection Officer

The DPO is the Data Protection Officer. It is not always necessary to have a DPO.

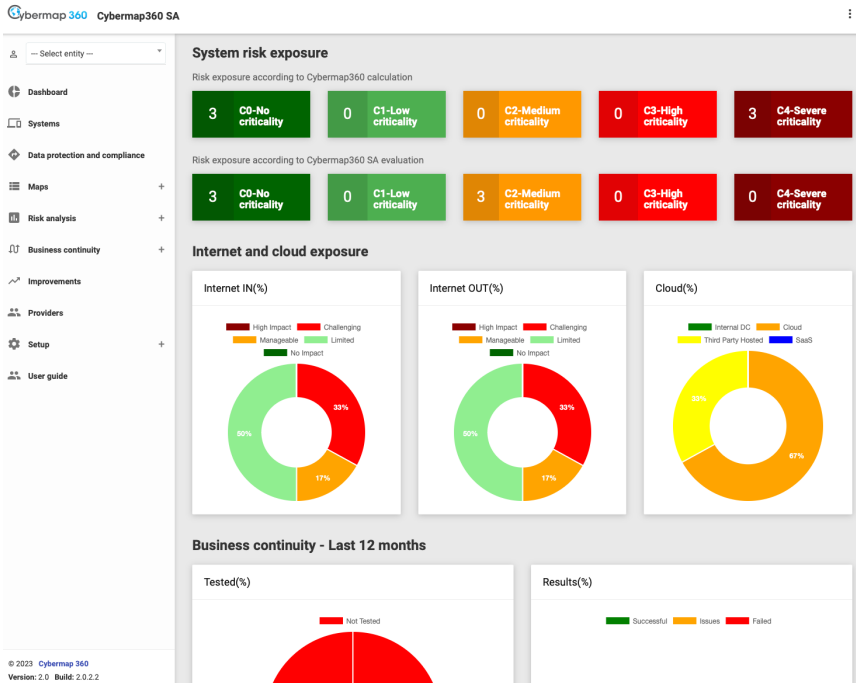
Providers can be any third party involved in the process.

In the Systems tab, you can select which systems are involved in the process. It will then automatically link the data available in that system (see the Data tab).

The Summary tab gives you the content that your data register

The Dashboard

The dashboard gives you the big picture on your current cyber posture. You can click on every item to get more details.



Maps

Cybermap 360 provides 3 maps: the **Systems map**, which is basically a massive table with all the systems and all their information. The **Locations map**, which tells you how many systems you have in which country. And the **Data map** that tells you which data types are stored in which systems.

Risk analysis

Risk assessment

The risk assessment gives you an overview of the risk level of all your systems. Click on the system's name to see its details.

Internet exposure

This risk analysis is very important in case of (Distributed) Denial of Service attack (DDoS). Because you will know exactly what systems are going to be impacted. Through your Business Continuity Plan you can define your ability to keep your operations running in case of DDOS.

The internet exposure only displays systems that have an exposure. It calculates an **Internet risk** that can be "High Impact / Challenging / Manageable / Limited / No Impact". And then provides information about readiness, and the impacts in and out.

Cloud exposure

This risk analysis is very important to understand how much you rely on the public cloud and how much you are ready in case of difficulties with accessing the cloud.

The Cloud exposure gives you a view by country. Focus on the third column.

Cloud exposure

Search: _____

Country	Internal DC	Cloud	Third party hosted	SaaS
United States	0	1	0	0

Showing 1 to 1 of 1 entries

Vendor appliance exposure

This enable you to track all vendor appliances you might have within your infrastructure. This is not very frequent anymore to have vendor appliances but in case you have some, you need to be sure they are well managed as they create an additional potential cyber risk.

Business continuity

Your business continuity capabilities are very critical to your ability to go through any IT incident, whether it is a disaster, failure, cyber-attack, or any type of incident. Your business continuity capabilities should be tested at least once a year.

Business continuity tests

Here you can create an entry for each system tested. You must select the **System**, the **Date** of the test, the **Result** of the test.

Then you should mention if the system has been **Tested during BCP**. It can happen that for some reasons the test cannot be conducted.

The **RTO** – Recovery Time Objective is an industry standard, define as the targeted duration of time within which a business process must be restored after a disaster failure, or comparable event. You can define if your RTO has been achieved during your BCP.

The **RPO** – Recovery Point Objective is an industry standard, define as the maximum amount of data that can be lost after a recovery from a disaster, failure, or comparable event. You can define if your RPO has been achieved during your BCP.

We would suggest that systems' owners are responsible for their systems' tests.

Business continuity results

This gives you an overview of your test results.

Improvements

You can define improvement measures and manage them as to do's that are assigned to employees. Don't be afraid to have many improvement actions, give yourself enough time to implement them, but make sure they get done!

Troubleshooting

Error message or system not displaying anything

Reload the page. If it does not work, empty the cache of your browser, close your browser and start again.

System in not responding

Empty the cache of your browser, close your browser, and start again.

Cannot log in anymore

Empty the cache of your browser, close your browser, and start again.

Getting an invoice

Connect to Cybermap 360, click on the three dots on the top-right of the screen and select Account. You'll find your invoice there.

Do not hesitate to contact us at info@cybermap360.com