C4T
CYBER 4 TOMORROW

Cybersustainability Tool

How to set up the approach to measure the carbon footprint of your cybersecurity?

*Based on the V1 Methodology created and made available by Wavestone, the CyberSustainability V2 Methodology was produced by the Cyber Campus Working Group led by Wavestone in cooperation with Advens, Capgemini, Qorum Secur'Num, Sopra Steria Groupe and with the support of ADEME.

Soutenu par
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ADEME
AGENCE DE LA TRANSITION ÉCOLOGIQUE

Table of content

01. Methodology Presentation

02. How to set up the approach?

03. How to use the tool?

01. Methodology presentation

01. Methodology presentation

Cyber teams must play their part in the sustainability effort of the organisations, by questioning the way cybersecurity is ensured in order to reduce its impact without compromising on the risk level.

With this conviction, Cyber4Tomorrow is publishing this methodology to calculate the carbon impact of cybersecurity measures and set up an action plan to reduce this impact without reducing the risk coverage.

This methodology** was experimented in 2024-2025 during a pilot led by the Campus Cyber in cooperation with 5 consulting firms and with the support of Ademe. The tool was deployed in 7 organizations (5 large companies and 2 territorial collectivities) which contributed to its improvement thanks to their operational feedbacks.

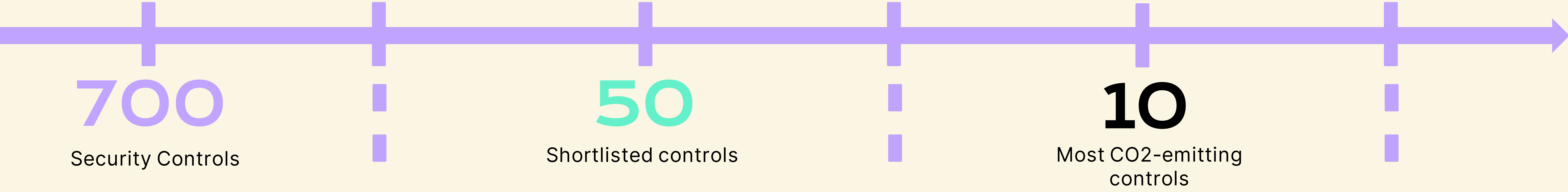
- Cyber represents a significant proportion of information systems (+/-5% of the IT budget*) and is growing rapidly to face new threats.
- Cybersecurity controls have a major impact on the way information systems are designed and operated, hence their strategic importance for overall carbon footprint.

* According to Wavestone's benchmark on 100+ organizations across all sectors, 5.3% of the IT budget is spent on cybersecurity on average.

*** The methodology is Open Source. Please, always credit the authors in the documents created based on this methodology by indicating the following : "Based on the V1 Methodology created and made available by Wavestone, the Cyber Sustainability v2 Methodology was produced by the Cyber Campus Working Group led by Wavestone in cooperation with Advens, Capgemini, Qorum Secur'Num, Sopra Steria Groupe and with the support of ADEME."*

01. Methodology presentation

The methodology based on NIST Cybersecurity Framework starting from 700 security controls. We shortlisted 50 shortlisted security controls, in which we identified the TOP 10 most emitting controls based on real data.



700
Security Controls

50
Shortlisted controls

10
Most CO2-emitting controls

Qualitative filtering

The 50 most emitting controls were selected if the answer was positive to one or more of the following questions (based on the ADEME/Arcep* breakdown of the carbon footprint of the digital world):

1. Does it require a significant number of endpoints?
2. Does it require a significant number of servers and computing power?
3. Does it require a large amount of network equipment and bandwidth?

Qualitative filtering

Among the 50 shortlisted controls, the TOP 10 most emitting controls was selected based on the calculation of the emissions using:

1. Real-life data from the pilot participants
2. Emission factors using benchmarked values of IT asset emissions*

Impact calculation

Methodology Emission Sources

Each company can focus its impact calculation on the most impactful emissions sources for cybersecurity

→ These results have to be calculated for each company

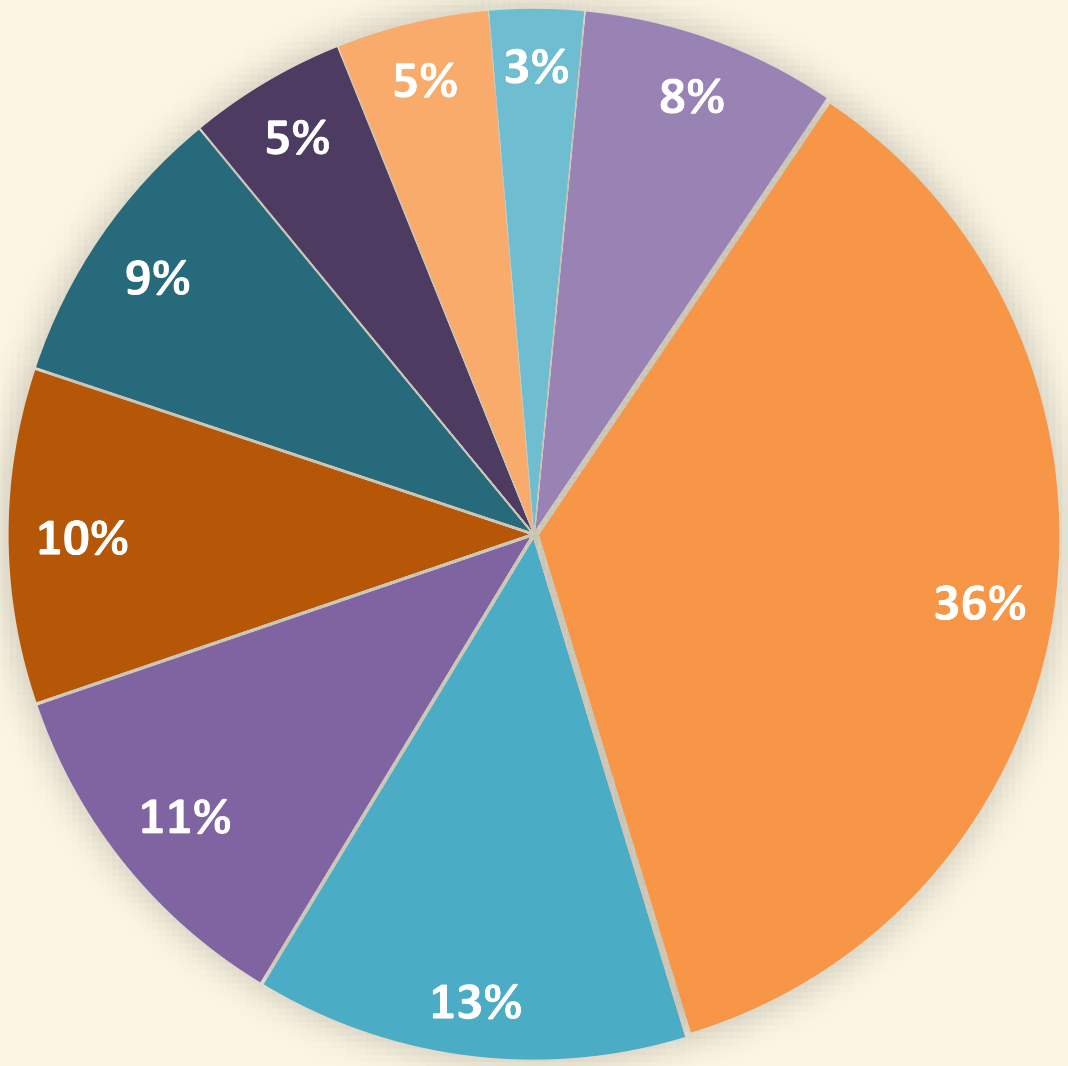
→ These initial results enable us to identify the first paths of action

*Based on government and Workgroup data

01. Methodology presentation

Through this first impact assessment, we debunked cybersecurity emissions' myth.
2 security topics generate 50% of cybersecurity-related emissions…

Emissions % by NIST topic



■ Resilience (36%)
Redundancy capabilities in different regions (Backup servers, Backup PCs)

■ Endpoints (13%)
Contractor workstations, Administrator workstations and VDIs

■ Detect (11%)
Log generation, collection and storage, analysis

■ IAM (10%)
Authentication, Vaults, PAM

■ Data (5%)
Data in motion, at rest protection, Cryptography

■ Governance (3%)
Cyber staff workstations, Travel

■ Vulnerability (9%)
Vulnerability scans, Pentests, Antiviruses, Patch management

■ Network (5%)
Network mapping and segmentation, Anti DDoS

■ Other topics (8%)
Incident management, risk, etc.

It emits less than we may think

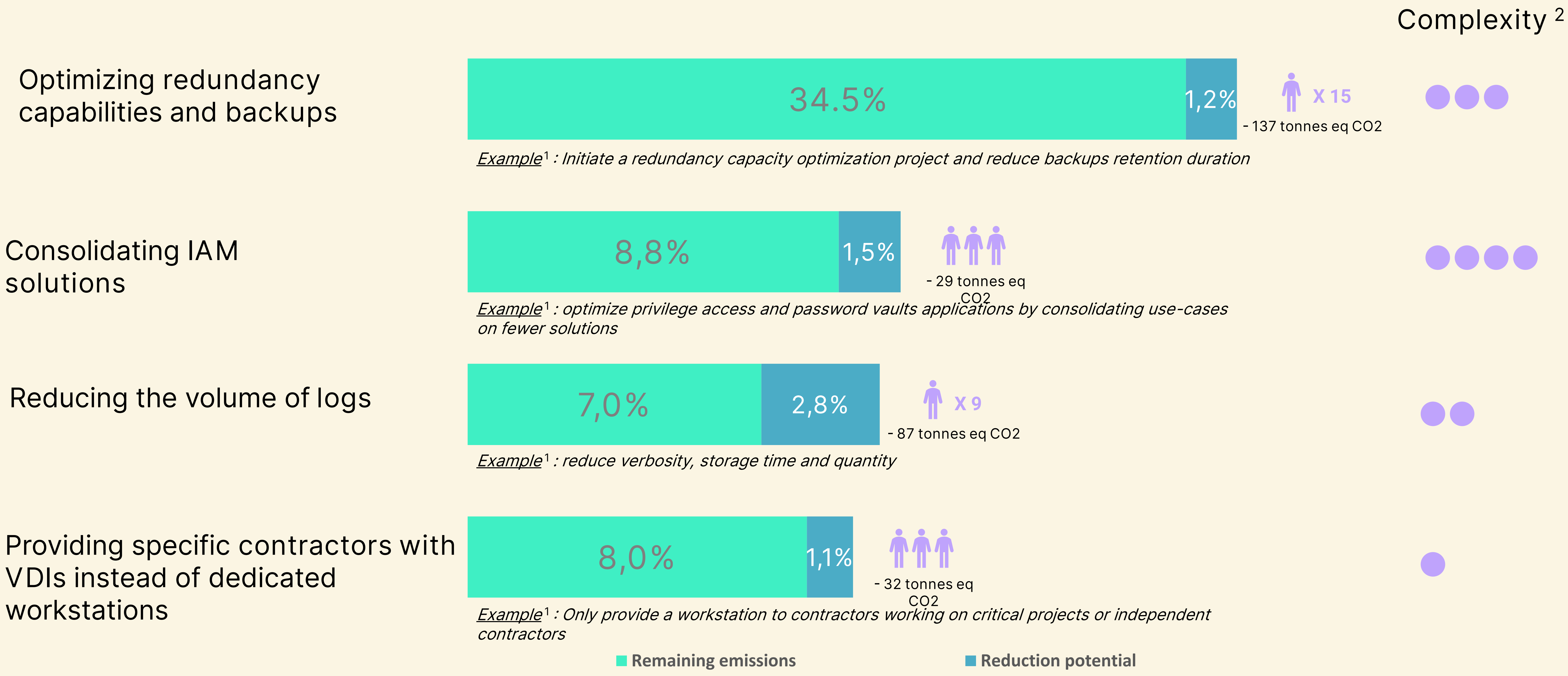
- Cyber threat intelligence
  Less than 2% of cyber emissions
- Encryption
  Less than 1% of cyber emissions

It emits more than we may think

- Resilience capabilities
  36% of cybersecurity emissions
- Contractor workstations
  9% of cybersecurity emissions

Beyond contributing to mitigating climate change, decreasing the carbon footprint of cybersecurity comes with many co-benefits

Optimizing security controls to decrease emissions by 5% to 10%, with a constant level of risk



Optimizing redundancy capabilities and backups

Example[1] *: Initiate a redundancy capacity optimization project and reduce backups retention duration*

Consolidating IAM solutions

Example[1] *: optimize privilege access and password vaults applications by consolidating use-cases on fewer solutions*

Reducing the volume of logs

Example[1] *: reduce verbosity, storage time and quantity*

Providing specific contractors with VDIs instead of dedicated workstations

Example[1] *: Only provide a workstation to contractors working on critical projects or independent contractors*

[1] *Depends on each organization and context.* [2] *This is an estimation and depends on each organization and context.*

Beyond contributing to mitigating climate change, decreasing the carbon footprint of cybersecurity comes with many co-benefits

Decreasing cyber emissions comes with significant co-benefits

1. Reducing operational costs by optimizing the IT infrastructure (duplicated servers, cyber servers, workstations, etc.)

3. Be at the forefront of innovation in cybersecurity and attract talents

2. Comply with and anticipate legal requirements (including SDS in the UK and CSRD in the EU)

02. How to set up the approach?

02. How to set up the approach?

Tips to increase your chances of success

On study management

From the start, identify and **mobilize a high-level sponsor** and secure a **dedicated budget.**

Place the study within a cross-functional, **long-term** strategy: **integrate sustainability-by-design** into the ISP process, into risk analyses, add digitally responsible criteria to calls for tender, etc.

Identify long-term operational contact points, to anticipate action plan updates at N+1/2/3

Build a study team of both cyber and green IT members. The study can be the opportunity to reduce silos between teams.

Put the **study into perspective** with the implementation of **regulations, standards and certifications** (e.g. NIS2, RGPD, DORA, CSRD).

Methodologic levers

Improve the readability of your results by presenting them with equivalences in euros, or in material.

Adapt the tool according to your organisation size and maturity in terms of data collection and of your **collection and results priorities.**

Build your action plan and prioritise the actions with a risk-based approach : obsolescence, dependency, vulnerability, etc.

Simplify study scope: you can **limit your study to one representative Business Unit** to reduce data collection needs and then generalise to the entire company

Operational levers

Organise a kick-off meeting with all stakeholders to launch the dynamic.

Identify "must have" and "nice to have" data to prioritize efforts, follow the collect with KPIs.

Accept approximations via monetary ratios and accept to stop the collect when your main collection goals are achieved. Indicate the choices made to dig in later on.

Capitalize on and **maintain relationships with identified reactive contacts.**

Involve the stakeholders in the long term with regular feedbacks on actions set-up progress following the study.

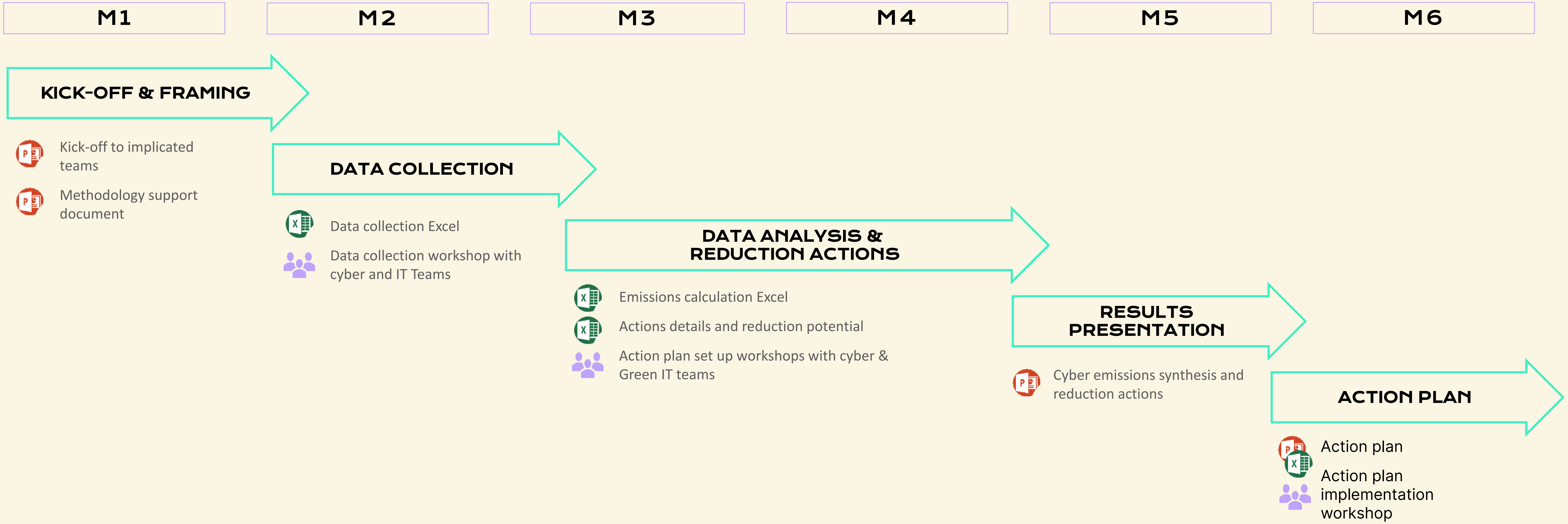
Communication levers

When contacting teams to collect data, **demystify the work required**: the data is often already available, the intervention of each contact may be very limited in time (e.g.: 1-hour call). If possible, include the workload in their work schedule.

Communicate on the objectives and benefits of the approach**, by producing communication elements adapted to the stakeholders** (CSR, CISOs, COMEX). For CISOs : possibility of a better knowledge of assets, equipment, SAAS applications, reduction of the CO2eq. impact of cyber activities and of maintenance costs.

02. How to set up the approach?

Approximately 30 to 45 days are required to deploy the methodology.
This estimate varies according to the organization's size, complexity and level of maturity.



M1 | M2 | M3 | M4 | M5 | M6

KICK-OFF & FRAMING

- Kick-off to implicated teams
- Methodology support document

DATA COLLECTION

- Data collection Excel
- Data collection workshop with cyber and IT Teams

DATA ANALYSIS & REDUCTION ACTIONS

- Emissions calculation Excel
- Actions details and reduction potential
- Action plan set up workshops with cyber & Green IT teams

RESULTS PRESENTATION

- Cyber emissions synthesis and reduction actions

ACTION PLAN

- Action plan
- Action plan implementation workshop

03. How to use the tool?

Introduction and Methodology

Excel Calculator goal

The goal is to calculate an estimate of the carbon footprint of cybersecurity.

The calculator focuses on greenhouse gases (in CO2e) – impacts on biodiversity, natural resources, soil and water pollution are not taken into account.

Emissions of cybersecurity are defined as the emissions that are the consequence of a cybersecurity control.

Recommendation for large companies: calculate the emissions of a large entity that is representative of the information system, then extend the results to the whole company thanks to a customized multiplication factor.

GHG emissions methodology

The calculator takes scope 1, 2 and 3 into account (scope 1 through certain emission factors). The goal is to be comprehensive enough to be able at the end to come up with impactful actions to decrease the carbon footprint of cyber measures.

Emissions are calculated over 1 year, with a stock vision (it calculates emissions of the existing infrastructure and divides it by its lifetime).

Emissions linked to electricity consumption are taken into account with the location-based method (the carbon intensity depends on the electricity mix of the country where electricity is consumed), not with the market-based method.

03. How to use the tool?

Overview of the Data Collection Excel workbook. This document focuses on data collection.
It can be shared between all participants allowing you to centralize the needed data.

01. Introduction and read me

Understand how the methodology is built (NIST controls, pilot and test realized…) and how to use the calculator

02. Data collection

Collect data from the organization's IS (e.g., endpoints, server locations, external services).

03. Security control and organisation mapping

Map each collected date type (Devices, Cyber solutions, Travels, etc.) and each type of external service with the security controls to obtain the measure you wish

04. Emission factors and assumptions

Track emissions factors based on country, hardware and define assumptions to estimate the carbon footprint.

03. How to use the tool?

The Emissions Calculator Excel workbook is designed to calculate carbon emissions. It is based on the data collected in the Data Collection Document, from which you can report the data and on emission factors from Ademe or Boavizta. It includes dashboards and graphs to present the results, as well as a section to build your action plan to reduce the emissions of your cybersecurity.

01. Introduction and read me

Understand how the methodology is built (NIST controls, pilot and test realized…) and how to use the calculator

02. Data collection

Gather data from the organization’s IS (e.g., endpoints, server locations, external services).

03. Security control mapping

Link each data type (Devices, Cyber Solutions, Travel, etc.) and external services to the relevant security controls.

04. Emission factors and assumptions

Track emissions factors based on country and hardware, and define assumptions to estimate the carbon footprint.

05. Dashboard

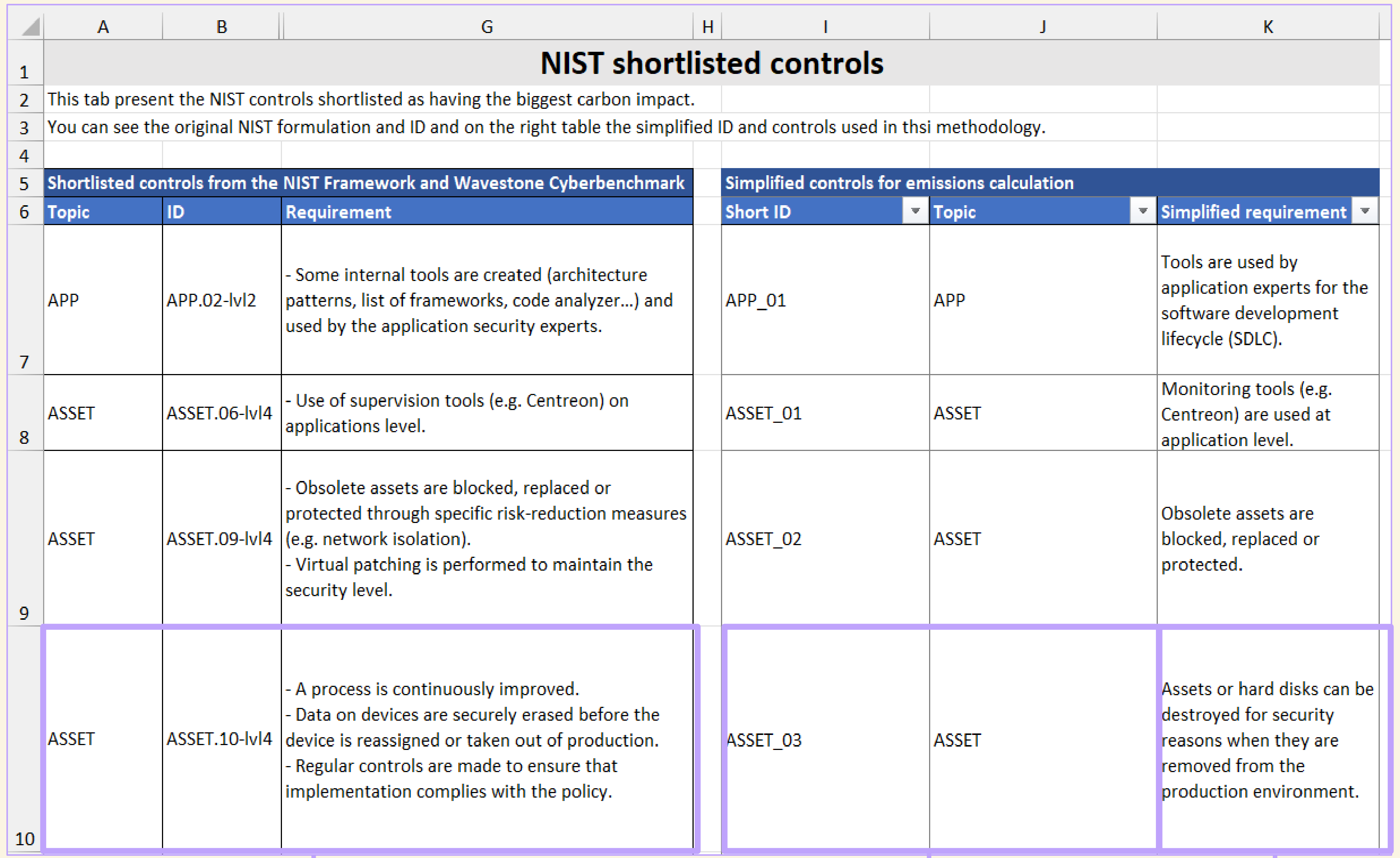
Present a summary of cyber emissions by security control, topic and IT domain

06. Actions

Calculate the emissions reduction potential of specific actions (tab to be customized and replicated for each action)

03. How to use the tool?

How are NIST controls used in the tool?



NIST shortlisted controls

This tab present the NIST controls shortlisted as having the biggest carbon impact.

You can see the original NIST formulation and ID and on the right table the simplified ID and controls used in thsi methodology.

Shortlisted controls from the NIST Framework and Wavestone Cyberbenchmark			Simplified controls for emissions calculation		
Topic	**ID**	**Requirement**	**Short ID**	**Topic**	**Simplified requirement**
APP	APP.02-lvl2	- Some internal tools are created (architecture patterns, list of frameworks, code analyzer...) and used by the application security experts.	APP_01	APP	Tools are used by application experts for the software development lifecycle (SDLC).
ASSET	ASSET.06-lvl4	- Use of supervision tools (e.g. Centreon) on applications level.	ASSET_01	ASSET	Monitoring tools (e.g. Centreon) are used at application level.
ASSET	ASSET.09-lvl4	- Obsolete assets are blocked, replaced or protected through specific risk-reduction measures (e.g. network isolation). - Virtual patching is performed to maintain the security level.	ASSET_02	ASSET	Obsolete assets are blocked, replaced or protected.
ASSET	ASSET.10-lvl4	- A process is continuously improved. - Data on devices are securely erased before the device is reassigned or taken out of production. - Regular controls are made to ensure that implementation complies with the policy.	ASSET_03	ASSET	Assets or hard disks can be destroyed for security reasons when they are removed from the production environment.

Original NIST code and description.

Generic ID and topic to allocate the emissions.

Security control description to map with cyber solutions or servers' description

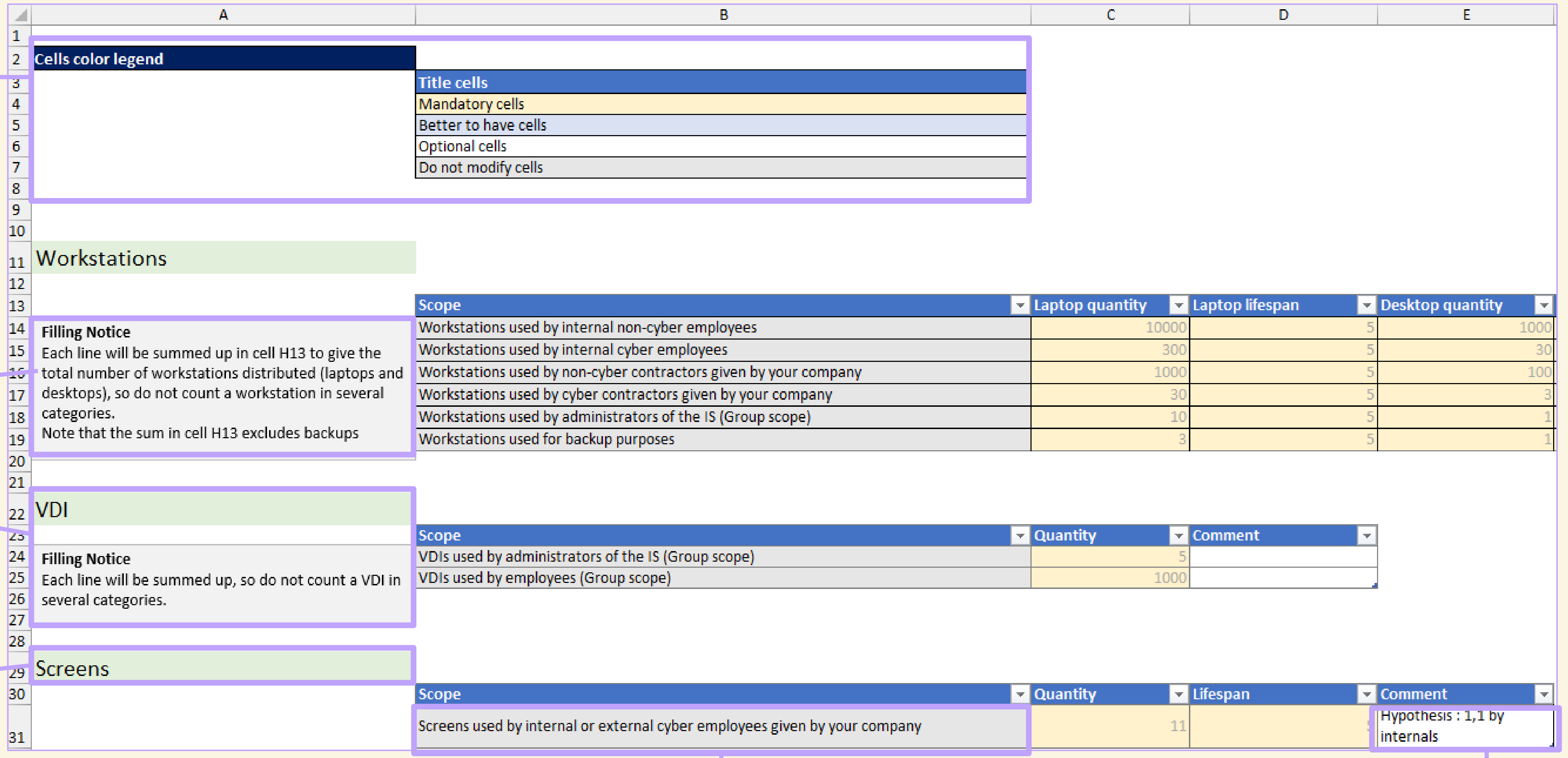
The most emitting NIST controls have been shortlisted thanks to experts (72 security controls).

Each control phrasing has been simplified in the methodology to be easier to apply to various environments.

Each control has been attributed a generic ID to be able to allocate cyber-related emissions to a security control.

03. How to use the tool?

How is the "Data Collection Document" tab constructed?



Cells color legend

Title cells
Mandatory cells
Better to have cells
Optional cells
Do not modify cells

Workstations

Filling Notice
Each line will be summed up in cell H13 to give the total number of workstations distributed (laptops and desktops), so do not count a workstation in several categories.
Note that the sum in cell H13 excludes backups

Scope	Laptop quantity	Laptop lifespan	Desktop quantity
Workstations used by internal non-cyber employees	10000	5	1000
Workstations used by internal cyber employees	300	5	30
Workstations used by non-cyber contractors given by your company	1000	5	100
Workstations used by cyber contractors given by your company	30	5	3
Workstations used by administrators of the IS (Group scope)	10	5	1
Workstations used for backup purposes	3	5	1

VDI

Filling Notice
Each line will be summed up, so do not count a VDI in several categories.

Scope	Quantity	Comment
VDIs used by administrators of the IS (Group scope)	5	
VDIs used by employees (Group scope)	1000	

Screens

Scope	Quantity	Lifespan	Comment
Screens used by internal or external cyber employees given by your company	11	5	Hypothesis : 1,1 by internals

The legend indicates what to fill-in and what to avoid modifying. "Better to have" cells will allow a more precise measure and to create specific dashboards.

The notice gives indications about what is expected in the cells and elements to pay attention to.

The topic or category is indicated for each table in green.

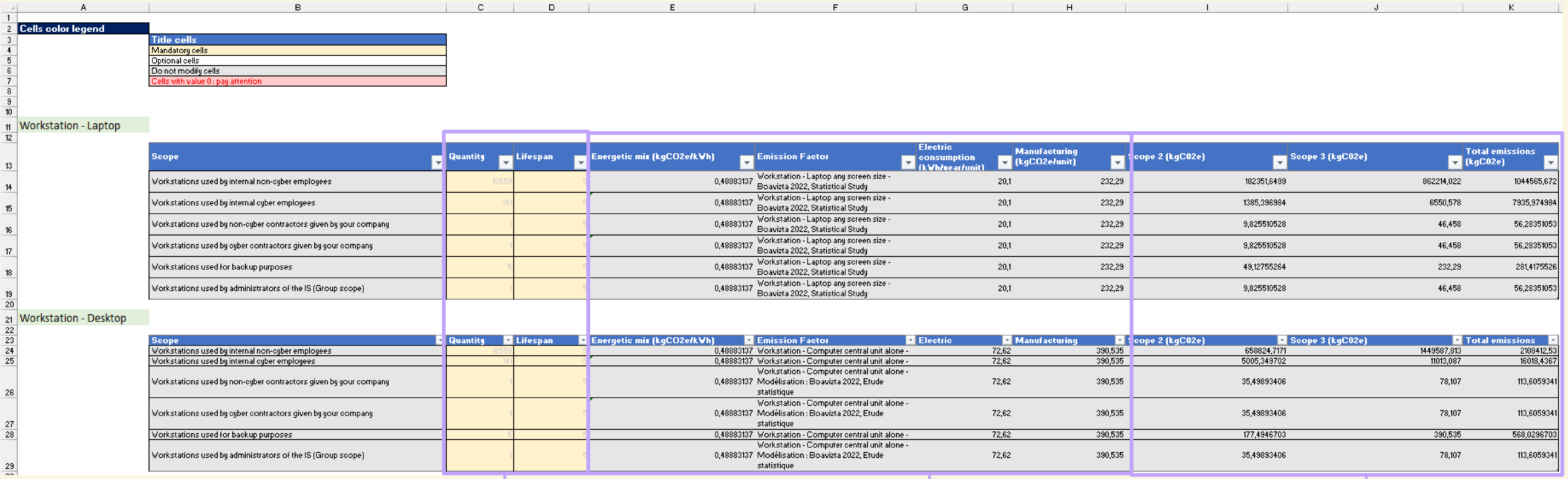
The scope of expected data is indicated in grey.

You can add comment as needed. *E.g.* it can be used to indicate the reliability of your data.

03. How to use the tool?

CYBER 4 TOMORROW

How is the "Emissions Calculator" tab constructed?



Cells color legend

- Title cells
- Mandatory cells
- Optional cells
- Do not modify cells
- Cells with value 0 : pay attention

Workstation - Laptop

Scope	Quantity	Lifespan	Energetic mix (kgCO2e/kWh)	Emission Factor	Electric consumption (kWh/year/unit)	Manufacturing (kgCO2e/unit)	Scope 2 (kgC02e)	Scope 3 (kgC02e)	Total emissions (kgC02e)
Workstations used by internal non-cyber employees	18559	5	0,48883137	Workstation - Laptop any screen size - Boavizta 2022, Statistical Study	20,1	232,29	182351,6499	862214,022	1044565,672
Workstations used by internal cyber employees	141	5	0,48883137	Workstation - Laptop any screen size - Boavizta 2022, Statistical Study	20,1	232,29	1385,396984	6550,578	7935,974984
Workstations used by non-cyber contractors given by your company	1	5	0,48883137	Workstation - Laptop any screen size - Boavizta 2022, Statistical Study	20,1	232,29	9,825510528	46,458	56,28351053
Workstations used by cyber contractors given by your company	1	5	0,48883137	Workstation - Laptop any screen size - Boavizta 2022, Statistical Study	20,1	232,29	9,825510528	46,458	56,28351053
Workstations used for backup purposes	5	5	0,48883137	Workstation - Laptop any screen size - Boavizta 2022, Statistical Study	20,1	232,29	49,12755264	232,29	281,4175526
Workstations used by administrators of the IS (Group scope)	1	5	0,48883137	Workstation - Laptop any screen size - Boavizta 2022, Statistical Study	20,1	232,29	9,825510528	46,458	56,28351053

Workstation - Desktop

Scope	Quantity	Lifespan	Energetic mix (kgCO2e/kWh)	Emission Factor	Electric	Manufacturing	Scope 2 (kgC02e)	Scope 3 (kgC02e)	Total emissions
Workstations used by internal non-cyber employees	18559	5	0,48883137	Workstation - Computer central unit alone -	72,62	390,535	658824,7171	1449587,813	2108412,53
Workstations used by internal cyber employees	141	5	0,48883137	Workstation - Computer central unit alone -	72,62	390,535	5005,349702	11013,087	16018,4367
Workstations used by non-cyber contractors given by your company	1	5	0,48883137	Workstation - Computer central unit alone - Modélisation : Boavizta 2022, Etude statistique	72,62	390,535	35,49893406	78,107	113,6059341
Workstations used by cyber contractors given by your company	1	5	0,48883137	Workstation - Computer central unit alone - Modélisation : Boavizta 2022, Etude statistique	72,62	390,535	35,49893406	78,107	113,6059341
Workstations used for backup purposes	5	5	0,48883137	Workstation - Computer central unit alone -	72,62	390,535	177,4946703	390,535	568,0296703
Workstations used by administrators of the IS (Group scope)	1	5	0,48883137	Workstation - Computer central unit alone - Modélisation : Boavizta 2022, Etude statistique	72,62	390,535	35,49893406	78,107	113,6059341

Report here the data you have collected for each category and scope.

The emission factors used in the calculations are indicated here.

When you add your data, the results of emissions calculation appear here.

C4T

CYBER 4 TOMORROW

To learn more about the Methdology and/or about Cyber4Tomorrow !

contact@cyber4tomorrow.fr