



RÉPUBLIQUE  
FRANÇAISE

*Liberté  
Égalité  
Fraternité*



REMPAR25

**REMPAR25**  
**MASS CYBER**  
**CRISIS EXERCISE:**  
**FEEDBACK**



# TABLE OF CONTENTS

<b>REMPAR25: a unique exercise carried out</b> _____	<b>3</b>
<b>on a national scale, open to all in order to promote collective cyber resilience</b>	
<b>REMPAR25, a new edition scaled up</b> _____	<b>5</b>
<b>to provide support across the entirety of the French territory</b>	
<b>1. A large-scale exercise to demonstrate</b> _____	<b>6</b>
<b>France's ability to practice countering a fictitious but plausible systemic cyberattack</b>	
<b>2. An exercise in which various</b> _____	<b>11</b>
<b>different industries from across the country were represented</b>	
<b>3. A large-scale exercise to assess</b> _____	<b>15</b>
<b>the country's level of preparedness</b>	
<b>4. Several courses of action to improve</b> _____	<b>24</b>
<b>the resilience of organisations over the next few years</b>	
<b>Going one step further</b> _____	<b>30</b>
<b>Appendix – List of partnerships</b> _____	<b>31</b>

---

# REMPAR25: A UNIQUE EXERCISE CARRIED OUT ON A NATIONAL SCALE, OPEN TO ALL IN ORDER TO PROMOTE COLLECTIVE CYBER RESILIENCE

---

On the 18th of September 2025, with the support of the national Cyber Campus, the Business Continuity Club (CCA), the French Information Security Club (CLUSIF), the Information and Digital Security Experts Club (CESIN), and 52 partners from across the territory, the French Cybersecurity Agency organised the mass exercise known as REMP25.

Close to 5,680 professionals participated in the exercise – 50% of which worked in neither the digital field nor the cybersecurity sector. Hailing from 1,263 different public and private organisations, spread across 13 regions and 9 overseas territories, participants were invited to respond to a simulated systemic cyberattack which, according to the scenario, led to the massive interruption of essential digital services, impacting several sectors and a multiplicity of actors. Central to every edition of the REMP25 exercise, this digital black-out scenario highlighted the importance of establishing business continuity plans, as well as the necessity for each organisation to integrate cyber-crisis management into their strategy – proactively and collaboratively with all of the organisation's functions.

---

After REMPLAR22, which had brought together 550 participants from 100 different entities located in the greater Paris area, this new edition was intended for all entities on the French territory, whatever their nature. The importance of pluridisciplinarity in the management of cyber crises was thereby emphasised.

In facilitating practice at both the operational and the strategic level, this exercise fell within the objectives provided by the NIS 2 Directive, as well as in the strategic objective set out in the National Strategic Review – which aims to ensure top-tier cyber resilience across the country.

REMPAR25 had five main complementary objectives:

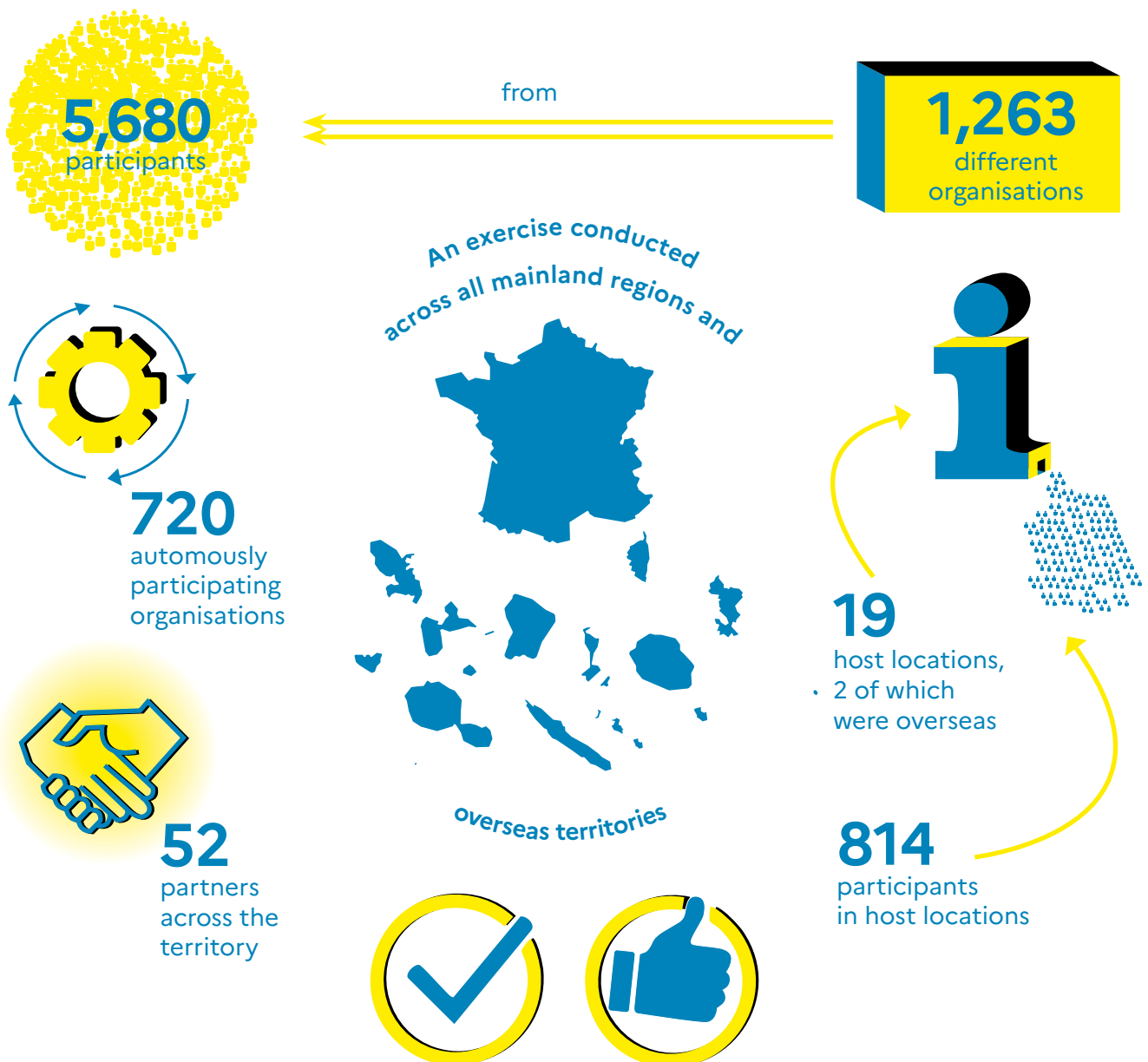
- **01** — Raising awareness amongst non-cybersecurity experts;
- **02** — Training the French ecosystem in cyber-crisis management;
- **03** — Testing the ability of organisations to react and endure over time;
- **04** — Addressing the question of anticipation;
- **05** — Introducing the notion of business continuity.

ANSSI encourages organisations to capitalise on this feedback and to utilise the ready-to-use kit to implement it. Crisis exercises are effective tools to develop a greater, shared understanding of the issues at hand amongst multidisciplinary teams. The best way to manage a cyber crisis is to prepare for it.

Organising an exercise of this magnitude – more than 5,000 participants from over 1,200 different organisations located across the country – was a challenge which we faced collectively. The cyber threat is a daily reality; France must prepare itself to handle various types of cyber crises. All organisations may someday be faced with a cyber crisis – as such, it is crucial to train and prepare for such an eventuality.

*Vincent Strubel, Director-General of ANSSI*

# REMPAR25: A NEW EDITION SCALED UP TO PROVIDE SUPPORT ACROSS THE ENTIRETY OF THE FRENCH TERRITORY



For over **95%** of participants, REMP25 provided an opportunity to implement crisis-management and/or ISS-related measures

REMP25 met the expectations of over **99%** of respondents

# **1. A LARGE-SCALE EXERCISE TO DEMONSTRATE FRANCE'S ABILITY TO PRACTICE COUNTERING A FICTITIOUS BUT PLAUSIBLE SYSTEMIC CYBERATTACK**

---



## 1.1 A realistic scenario based on the current state of the cyber threat

REMPAR exercise scenarios allow participants to practice handling a digital black-out. This experience provides an opportunity for participating entities to develop a deeper understanding of the risks associated with dependencies on the cyber supply chain, and to fully grasp the necessity of preparing the Nation to face cyber crises. At the national level, these scenarios are intended to facilitate the assessment of France's preparedness in the management of such crises.

The 2025 edition of REMPAR was based on a scenario in which the update of a broadly used security solution (antivirus or EDR<sup>1</sup>) was compromised by a state-sponsored actor, allowing said actor to sabotage the infrastructure on which the solution was installed. In this scenario, the cyberattack also brought about mass data leaks, orchestrated by the state-sponsored actor, who relied on cybercriminal groups to obtain ransoms and thus obscure the source of this sabotage operation.

1. EDR: Endpoint Detection and Response software used by IT teams to detect, contain, and investigate cyberattacks.

To make REMPLAR25 a progressive and immersive exercise, the crisis scenario was broken down into three successive phases:

- **Phase 1 – Data exfiltration:** a week prior to the launch of the wiper attack, the attacker altered the security solution's behaviour in order to collect and exfiltrate sensitive data. Wherever the (fictitious) update had been installed (across all participating organisations), the countdown was initiated – ending at 5:00am on the day of the exercise and thereupon activating the crisis units;
- **Phase 2 – Data erasure:** the attack further intensified with the implementation of a destructive mode (irreversible erasure), resulting in major malfunctions and in the urgent mobilisation of crisis unit teams. This phase provided an opportunity to test business continuity, anticipation, and detection and response measures;
- **Phase 3 – Data disclosure:** the data exfiltrated during phase 1 was shared with a cybercriminal group, then published progressively alongside ransom demands to avoid their total disclosure. This phase provided an opportunity to test the resilience of organisations with regards to both the communication – notably in the face of simulated media pressure – and the legal aspects of crisis management, given the publication of data and the declarations which must follow.

Common to all participating organisations, this scenario was conceived to be adapted to local contexts, guaranteeing the coherence of the exercise while taking into account the specific realities of each participant. It provided an opportunity for participants to test their ability to detect, analyse, and manage a complex cyber crisis, all the while ensuring business continuity as well as internal and external communication.

It provided for height distinct roles – “human resources”, “legal”, “finance”, “communication”, “business”, “decision”, “IT”, and “cyber” – to emphasise the necessity of multidisciplinary and coordination in the resolution of cyber crises.

Several different versions of the same scenario were provided, to allow participants to select the most appropriate sectorial variant and implement any necessary alterations. Territorial prefectures and CSIRTs<sup>2</sup> were also supplied a specific scenario which reflected the main scenario and allowed them to practice establishing departmental operational centres, for prefectures, and, for CSIRTs, issuing a request for mass support at the operational level.

<sup>2</sup> Territorial CSIRTs (Computer Security Incident Response Team) are cyber incident response centres which work closely with the entities located on their territory. They handle assistance requests from medium-sized actors (SMEs, mid-caps, local governments, and associations) and connect them to local partners: incident response service providers and state partners.

## 1.2 A uniquely designed exercise, drawing on the experience of the 2024 Olympic and Paralympic Games, with support intended to empower its participants...

To promote extensive and inclusive mobilisation, two different modes of participation were offered:

- **Mode 1 – Autonomous participation on the organisation’s own premises:** participants partook in the exercise from within their own environment, with their own teams and tools, and tested their crisis management mechanism (option favoured by organisations wishing to draw tangible lessons to implement in their specific context);
- **Mode 2 – Participation in a fictitious crisis unit:** up to three of the organisation’s representatives joined a fictitious crisis unit established at a given location (option favoured by organisations wishing to better understand the process of a cyber crisis management exercises and to discuss with their peers).

This dual format was conceived to facilitate shared learning and to promote greater maturity in the face of cyber challenges.

More than a simple exercise, REMP25 was a veritable support programme which, between March and September of 2025, allowed 720 organisations to prepare for the deployment of the exercise across their structure *via*:

- The preparation and provision of a detailed documentary exercise kit which could be adapted to the specificities of participating organisations;
- Between March and September of 2025, invitations to an opening webinar, four implementation webinars, and a general briefing to present the REMP25 project, the stakes at hand, and a method to facilitate acculturation and the appropriation of the documentary kit;
- Follow-up, in the form of weekly question-and-answer sessions from June of 2025, to answer the organisers' questions and to promote acculturation and the appropriation of issues addressed by REMP25.

Each participating organisation thus benefited from support and follow-up in the adaptation of REMP25 to their specific context and maturity level.

The fictitious crisis unit mode of participation was selected by 814 individuals (from 555 different organisations), spread across 19 host locations (17 in mainland France and 2 overseas) established by territorial Cyber campuses, prefectures, CCIs, and metropolises. This experience was a first introduction to cyber-crisis management and provided an opportunity for organisations to develop first reflexes.

Local project teams were assembled across the country, led by ANSSI's regional delegates and assisted by the local ecosystem, to organise, moderate, and observe the exercise at each location.

Media pressure was simulated to allow all participating structures to practice implementing cyber-crisis communication measures. This pressure platform sustained the collective nature of the experience and was commended for its realism, as well as for the links it successfully established between the participants. It notably provided a greater level of visibility with regards to the public communication decisions taken by participants in the context of the exercise.

REMP25 was an opportunity for France to present its know-how to the francophone international partners who had been invited for the occasion. Beyond the simple presentation of the exercise and its logistics, guests were able to partake in the exercise and immerse themselves fully in the simulation by taking on their own fictitious roles.

---

## **2. AN EXERCISE IN WHICH VARIOUS DIFFERENT INDUSTRIES FROM ACROSS THE COUNTRY WERE REPRESENTED**

---



Feedback from participating organisations was overwhelmingly positive: 99.54% of respondents asserted that REMP25 overall met their expectations, and 99.08% expressed their desire to participate in future editions of the exercise. 94.95% stated that the support programme was suitably adapted to their needs, and 98.62% judged that the resources provided had been sufficient to ensure the smooth conduct of the exercise.

Over 80% of respondents who believed themselves to possess low levels of maturity in cyber-crisis management prior to the exercise claimed to have progressed to moderate or aware<sup>3</sup> maturity levels. Similarly, over 70% of respondents estimated to possess moderate levels of maturity prior to the exercise now claim to be either aware or experts.

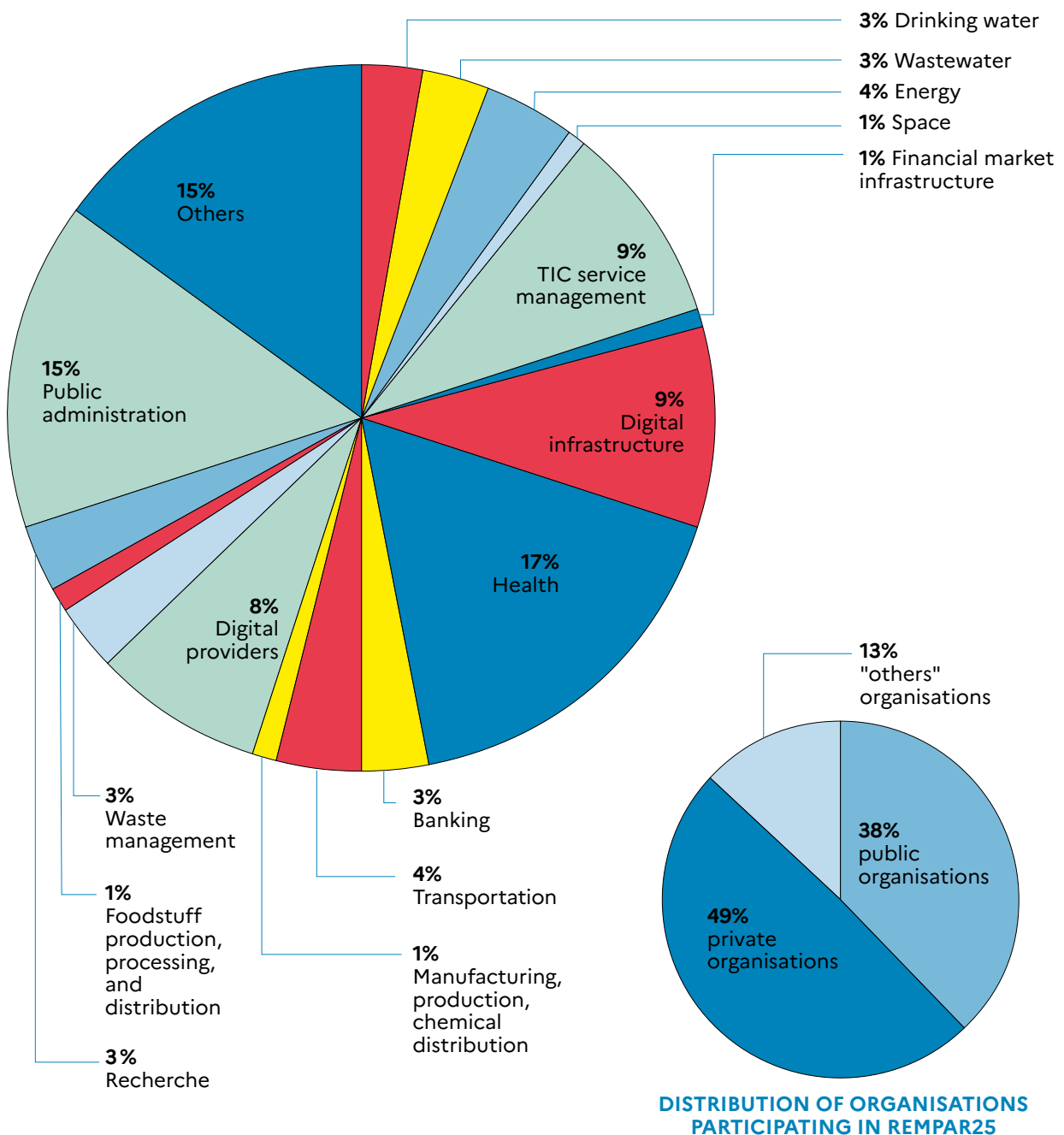
This experience promoted greater awareness of the fact that cyber crises, much like other types of crises, impact all strata of an organisation. Efforts must however be sustained to further involve industries as, in spite of the diverse make-up of the different units, the digital field was noticeably over-represented (around 50% of participants, as opposed to the 20% expected). The next edition of REMP25 will need to focus on mobilising non-cyber relays and thus reach a broader population.

The consideration of cyber risks when establishing business continuity plans remains low. The NIS 2 Directive, which notably insists on this point, should lay the groundwork for improvement over the upcoming years. In the same way, if greater attention is given to communication in the management of cyber crises, significant improvement may also be expected.

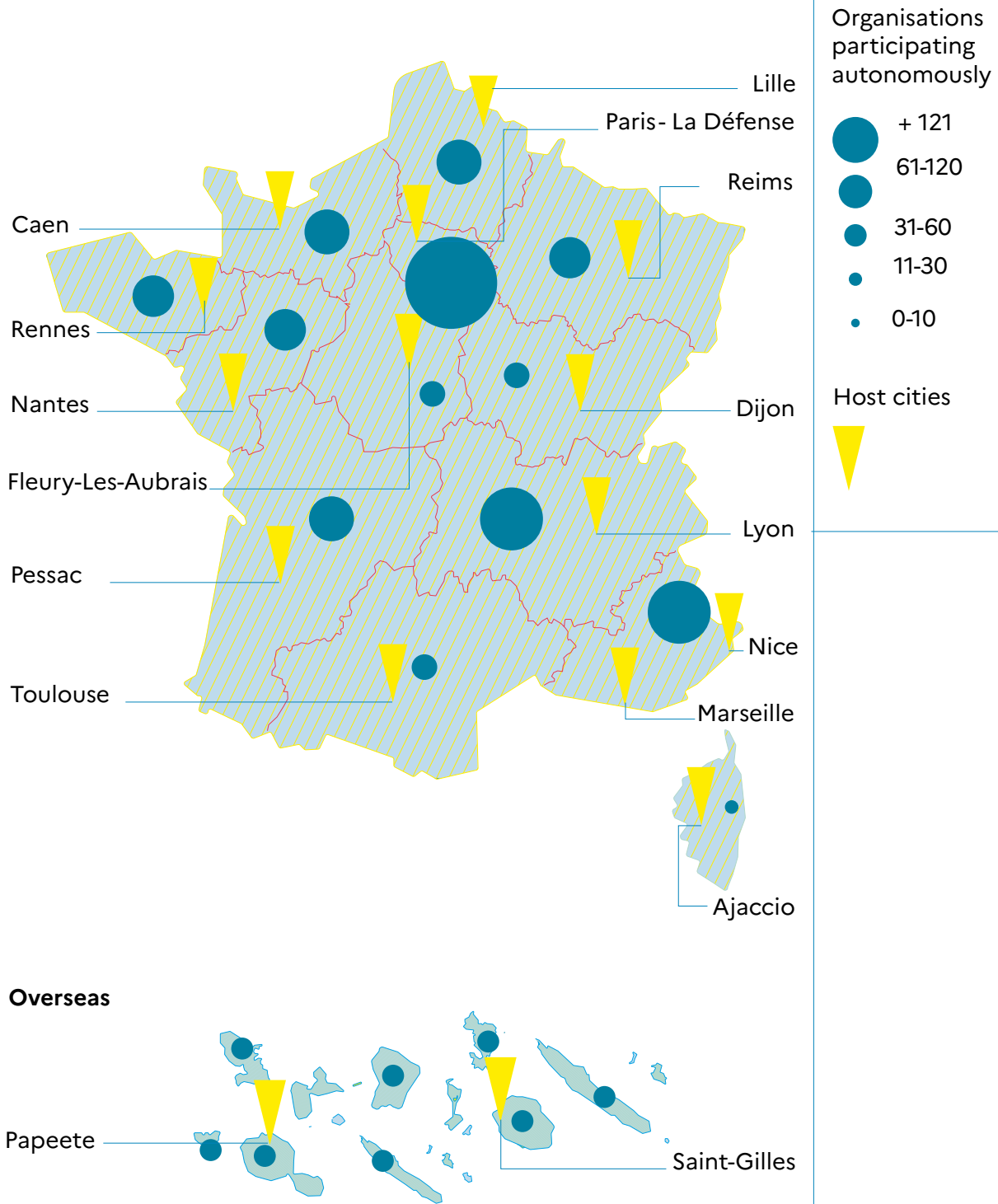
Participating organisations were also able to capitalise on – and sometimes discover – a rich cyber ecosystem with territorial coverage on which they could rely. This ecosystem must now be reinforced to fully mobilise non-cyber relays, growing increasingly dense and structured.

3. Suggested levels: weak, moderate, aware, expert.

## 2.1 Sectorial distribution of organisations participating in REMP25



## 2.2 Regional distribution of organisations participating in REMP25



---

# **3. A LARGE-SCALE EXERCISE TO ASSESS THE COUNTRY'S LEVEL OF PREPAREDNESS**

---



Following the end of the REMP25 exercise, on the 18th of September 2025, all involved parties – whatever their mode of participation – were invited to respond to a feedback survey. This feedback was then collected and analysed to concatenate and summarise the results.

To gain an operational appreciation of the observations provided by organisations which selected mode 1 of participation, these results were broken down into three levels of preparedness in cyber-crisis management, defined according to the following criteria:

- > The size of the organisation;
- > The proportion of non-IT/ISS participants;
- > The proportion of decision-makers amongst the participants;
- > Prior participation in a cyber crisis exercise;
- > The total number of players involved.

This categorisation distinguishes between the following levels of preparedness:

- > **Level 1 (L1)** – limited maturity;
- > **Level 2 (L2)** – intermediate maturity;
- > **Level 3 (L3)** – advanced maturity;

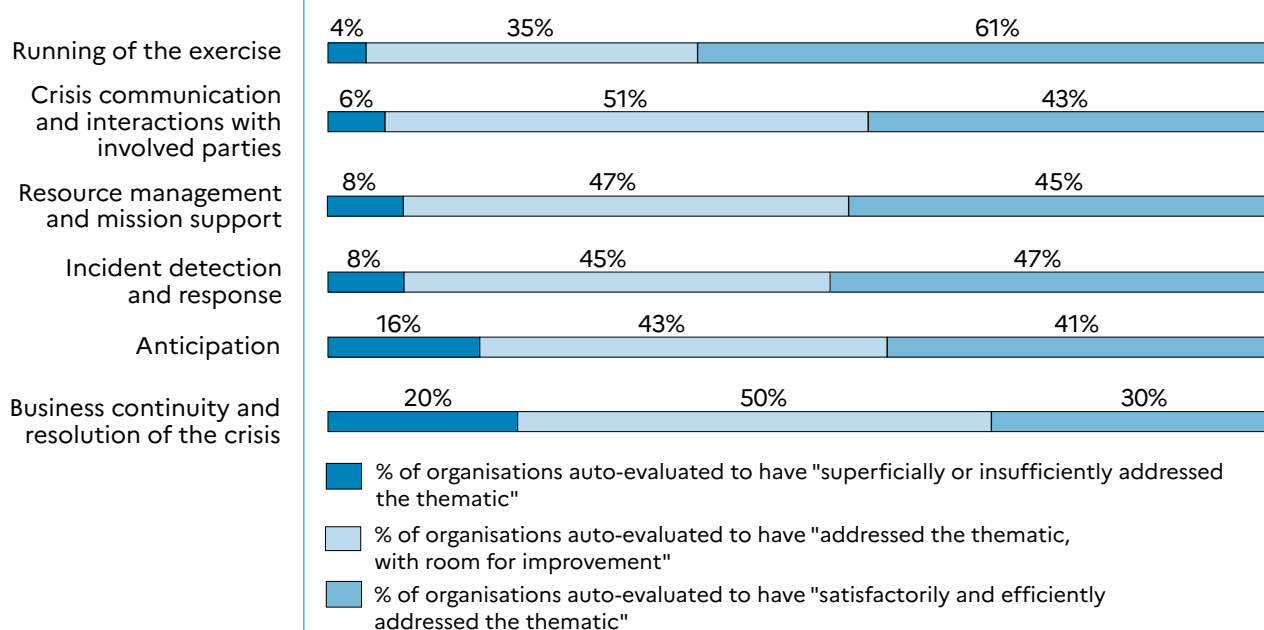
This section presents a **summary, per preparedness level and theme**, of the **main highlights, areas for improvement, and observations** reported by participants in their responses to the survey and during mutual feedback.

*Noter: only the most recurrent and representative comments and observations are addressed herein. This approach makes it possible to detect solid, significant trends, all the while reducing any potential biases resulting from the diverse nature of participating organisations.*

The players, observers, and moderators present in each crisis unit were called upon to address six different structuring themes intended to represent the primary aspects of cyber-crisis management and the means with which to prepare for it:

- > running of the exercise;
- > crisis communication and interactions with involved parties;
- > resource management and support missions;
- > incident detection and response;
- > anticipation;
- > business continuity and resolution of the crisis.

## Level of effectiveness in addressing the thematic, per participating organisation



These results brought to light a discrepancy in the maturity levels of different organisations within the French ecosystem. While a culture of crisis management exercises is now firmly established – as evidenced by the majority of organisations on the topic of the “running of the exercise” – several key aspects of cyber crisis management remain underdeveloped.

Technical elements (such as incident detection and response) generally appear to be better integrated and structured, which suggests a certain level of operational appropriation. However, on topics such as crisis communication, anticipation, and business continuity, there remains significant room for improvement.

These discrepancies highlight the necessity of reinforcing strategic preparation and organisational resilience – aspects of crisis management which are often overlooked in favour of immediate incident and crisis response.

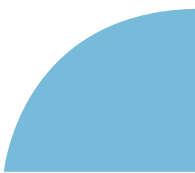
Note that each of these thematic areas was overall better addressed by organisations which had previously performed cyber-crisis management exercises, in comparison to organisations for which this was a first-time experience. This observation highlights the importance of training to reinforce cyber-crisis management and coordination capabilities.


## 3.1 Proficiency and experience in the conduct of crisis exercises

In general, participating organisations displayed a solid understanding of the challenges associated with cyber crises. REMPLAR25 acted as a lever to further raise awareness, and provided an initial methodological framework which less mature organisations could use to familiarise themselves with the essential reflexes to implement when faced with a crisis. Organisations which possessed a moderate level of maturity observed the implementation of specific action plans, which involved efficient prioritisation and ensured a structured response, adapted to the rhythm of the exercise which, according to some, was rather fast-paced.

In the case of organisations with lower levels of maturity (L1), the absence of crisis documentation often made it difficult for teams to draw on formal repositories and procedures. Furthermore, failure to comply with the distribution of roles within crisis units sometimes caused confusion when it came to decision-making and prioritisation. Difficulties in using the logbook were also observed, which suggests a lack of familiarity with this tracking tool. Lastly, wherever it was in place, the crisis-management procedure was sometimes insufficiently mastered. This made coordination and the elaboration of a collective response during the exercise more challenging.

The most aware of organisations (L3), on the other hand, displayed excellent reflexes, both operational and organisational, in crisis management. Crisis documentation was clear and used effectively, the distribution of roles was respected, and procedures were rigorously implemented – indicating a real mastery of crisis-management mechanisms and close coordination within crisis units. A degraded mode of operation was often enforced to test the reflexes and responsiveness of crisis units in situations where the usual digital tools are not available, which made it possible to assess the adaptability of teams and their ability to ensure operational continuity.





## 3.2 A display of significant responsiveness at the operational level, with the implementation of crisis-specific reflexes

Whatever their level of preparedness (L1, L2, or L3), participating organisations displayed a good mastery of the initial information system security measures which should be implemented in the event of a cyber crisis. They swiftly identified which containment and securisation measures to prioritise, indicating their effective appropriation of essential techniques from the early stages of crisis management.

Less mature organisations (L1) noted that they lacked an up-to-date map of their information system, which further complexified the identification of the compromise perimeter and the prioritisation of response measures in a situation of crisis.

Several organisations observed greater consideration of the role played by helpers in incident response during cyber crises. This change suggests that organisations have developed a greater understanding of which actors to mobilise in the face of such crises.

Note that the exercise was only an operational and strategic drill; it was not intended to address the tactical aspect of crisis management. This limitation may have impacted the operational simulation and reduced the pedagogical scope of these sequences by limiting the ability of teams to analyse, prioritise, and implement relevant technical measures.

### 3.3 Poorly planned crisis communication, often subject to improvisation in crisis situations

Organisations with limited maturity (L1) observed that existing communication mediums – including those intended for the media – were ill-suited to cyber-crisis management, preventing responsive and contextualised communication.

Organisations with an intermediate level of maturity (L2) expressed that they had trouble anticipating the successive stages of crisis communication. During the exercise, this could engender a lack of visibility of their medium-term strategy, in spite of their ability to rapidly formalise communication strategies – both internal and external – adapted to the specific challenges associated with cyber crises. This responsiveness guaranteed the cohesiveness of messages broadcast and the efficient management of interactions with other involved parties.

The most advanced of organisations (L3) were particularly well prepared in terms of crisis communication, with the elaboration of ready-to-use models and language elements.

Through the use of the simulated media pressure platform, participating organisations were able to tangibly establish their communication strategy.

The issue was addressed by all organisations involved in the exercise. However, they must work to further develop their communication plan prior to the emergence of a crisis, so that it may be adapted when such a time comes. The question of the potential use of alternative channels and practices in cases where the usual tools have been rendered unavailable merits further consideration.

## 3.4 Logistical support, human resources, and legal and financial means remain too poorly organised to sustain crisis management over time

Poor understanding of support functions was observed on several occasions within the crisis units established by less mature organisations (L1), which hindered the efficient application of core competencies at such times when they were necessary. Insufficient planning was also observed in the distribution of roles and missions, at times resulting in imprecise coordination and in the loss of operational efficiency in crisis management. The observations made surrounding this issue suggest that financial matters – often mentioned but not fully integrated in crisis management – remain only superficially addressed. Psychosocial risks are generally well-identified and understood, but insufficiently taken into account in operational frameworks.

Organisations with intermediate or advanced levels of maturity (L2, L3) stood out with their proficient management of transverse impacts, possessing a clear overview of the issue at hand and the ability to anticipate the spillover effects of a cyber crisis on their various functions and activities. They nonetheless noted the absence of a clearly-defined strategy for legal matters, expressing a need for clearer guidance with regards to legal obligations and the steps to follow, beyond the filing of a complaint, in the event of a cyberattack. Lastly, several organisations reported shortcomings in the distribution of roles which, at times, resulted in grey areas in the division responsibilities and the coordination of actions.

Organisations also observed a significant rise in awareness of the necessity to integrate representatives of transverse subjects within crisis units (legal, HR, communication), in order to ensure a more global and cohesive approach to cyber-crisis management. However, these matters remain insufficiently addressed.

## 3.5 Work initiated within organisations to instruct anticipation in cyber-crisis management

Organisations with limited or intermediated levels of maturity showed that they possessed a good capacity for anticipation, founded on common sense but not formalised in existing procedures. This intuitive approach gave them a head start in the scenario and allowed them to respond coherently to the first signs of crisis. Nevertheless, these organisations also reported that they struggled to fully grasp the stakes and objectives of anticipation in cyber-crisis management. Indeed, anticipation is often misconstrued as immediate response instead of being understood to involve the implementation of measures to gain perspective and anticipate upcoming actions – including “business” actions in a degraded mode of operation. Some of these organisations handled the crisis in a responsive manner, with little to no anticipation from their players during the exercise, and displayed a dependence on triggered events rather than proactively approaching the scenario.

Organisations with an intermediate level of maturity (L2) however exhibited greater anticipation of IT impacts, owing to the mobilisation of IT/ISS teams which possessed in-depth knowledge of their technical environment and of their information system’s critical interdependencies.

The most mature of organisations stood out with the realisation of anticipation scenarios during the exercise, displaying an advanced mastery of operational projection and planification. They furthermore reflected on the establishment of a unit specifically dedicated to anticipation, with the intention of enhancing monitoring efforts, prospective analysis, and interdepartmental coordination prior to the emergence of a crisis. They faced some difficulty attempting to expand anticipation scenarios as the crisis progressed, and they struggled to adapt their initial hypotheses and update their action plans as new situational elements arose.

The notion of structured anticipation remains poorly understood and is often not mobilised to its full extent during crisis management.



## 3.6 Existing but rarely tested and updated business continuity mechanisms

Organisations with an intermediate level of maturity (L2), unlike their less mature counterparts (L1), stood out with the use of operational documentation – which included business continuity plans (BCP) and reflex sheets – to help them manage each phase of the crisis. They also exhibited proficiency in the implementation of degraded modes of operation, which allowed their business teams to maintain and adapt the processes of their essential functions to the situation. The question of crisis resolution was however still insufficiently addressed, as the prioritisation of critical applications and activities remains a complex process in strained environments. The operational usefulness of existing business continuity plans – which had not been previously tried and tested or were simply unadapted to the realities of a crisis – was furthermore limited, as they were often unfamiliar to the operational teams at work. Lastly, persistent challenges when ensuring the continuity of transverse functions (human resources, financial, legal, etc.) were observed, revealing the uneven coordination of “support” roles.

More mature organisations (L3) likewise stood out with their clear business continuity documentation (BCP, reflex sheets), familiar to and regularly tested by their teams to ensure swift and efficient mobilisation during crises. These organisations also formalised a crisis-resolution action plan, defining a path to recovery and a return to normal. Lastly, in the aftermath of the crisis, they implemented a strategy for the reconstruction of their information system. This endeavour conveyed a proactive and resilient approach, involving the complete integration of post-crisis efforts in their cyber-crisis management framework.

Note that the format of the exercise provided few opportunities to practice realistic crisis resolution, given that, due to time constraints, the simulated conditions for recovery did not accurately reflect the temporal complexity of genuine post-crisis restoration.

Business continuity mechanisms are historical crisis-management mechanisms of which organisations generally have a solid understanding. They must, however, be further operationalised in order to be used as general crisis-management tools not just by IT/ISS teams, but by all teams.

# **4. SEVERAL COURSES OF ACTION TO IMPROVE THE RESILIENCE OF ORGANISATIONS OVER THE NEXT FEW YEARS**

---



The summary provided below addresses the thematic of crisis management which have been identified as acquired by the majority of participating organisations, as well as the growth trajectories identified or reported during the feedback collection process.

## 4.1 Well-integrated thematic which must be sustained over time

### → **Internal communication**

Internal communication was one of the highlights of the exercise. Crisis units clearly and cohesively relayed instructions. They also maintained a steady flow of information, keeping personnel informed as the crisis progressed.

### → **External communication, including communication with vendors and the authorities**

External communication is, by and large, now well integrated. Clear and cohesive language elements were communicated, filtering out « noise », with an external communication strategy specifically adapted to the context of crisis. Communication with the authorities and external stakeholders was also taken into account.



## 4.2 Partly integrated thematics which will require further consolidation

—→ **Taking into account the extended organisation and limiting the propagation of the attack**

Technical reflexes were overall successfully applied: doubt removal, initiation of immediate action on the ground, use of the relevant information system mapping. However, essential measures to limit the risk of propagation were less systematically implemented: interruption of incoming and outgoing flows to isolate or take into account shadow IT. These observations revealed the limited consideration of participating organisations' upstream and downstream interdependencies.

—→ **Human factors and personnel management**

Human factors are now better integrated in cyber-crisis management, with the implementation of adapted measures: placement on leave, exceptional teleworking, mobilisation of surge support. However, these measures remain overly responsive and not anticipatory, particularly when it comes to the monitoring and management of human resources.

—→ **Management of impacts on the entity's operations**

This thematic was marked by good operational responsiveness, but also by an often superficial approach to prioritisation and recovery. Business impacts were generally well identified and managed, but rarely hierarchised. This had an adverse effect on the organisation's ability to efficiently prioritise recovery efforts. Control and verification processes were not always considered prior to the restoration of impacted information systems, which conveyed a certain hastiness in the recovery process.

—→ **Degraded modes of operation considered – Cyber BCP**

This thematic was particularly well addressed, with both effective continuity reflexes and shortcomings in the conduct of substantive analyses. Suitable continuity measures were generally implemented, with appropriate responses such as the verification of backup integrity to avoid a subsequent crisis. However, projections of the duration of unavailability and of the impact of degraded modes remained insufficiently developed. This indicates that there remain too few "cyber" business continuity mechanisms which take specificities, including potentially long durations, into account.

—→ **Management of crisis resolution and of the "aftermath"**

Organisations enforced the necessity to file complaints, reflecting a good understanding of immediate post-incident procedures. Crisis resolution documents such as recovery or hardening action plans, however, were not formalised. This hindered recovery and the capitalisation of lessons learned.



## 4.3 Thematics with significant room for improvement which should be further developed by organisations

### —> **Legal affairs and insurance-related matters**

The legal and insurance-related mechanisms used to cover the side effects engendered by a crisis remain rarely tested and anticipated. These mechanisms – cyber-insurance especially – are, however, essential to facilitate crisis resolution and prevent subsequent crises.

### —> **Management of economic impacts**

Surface treatment of this thematic indicated a limited command of the economic aspects of crisis management. Some mechanisms have yet to be fully engrained in crisis management: emergency purchase procedures, compensation, elaboration of a post-crisis financial statement, and assessment of formalised impacts leading to tangible budgetary management or arbitration measures.

Note that the over-representation of IT/ISS communities in this exercise may account for this limited consideration of economic matters.

### —> **Orientation of investigations by crisis units**

Crisis units provided few clear directions to support technical investigations and efficiently steer research. This responsive – rather than proactive – approach restricted the depth of analyses and hindered the structuration of investigations.

### —> **Anticipation of impacts brought about by the crisis, and of the decisions to be taken regarding the entity's operations**

Participating organisations were particularly sensitive to technical vulnerabilities such as those resulting from defects in security solutions (e.g. the exercise scenario), but these have not yet sparked reflection on operational, legal, financial, and reputational impacts. Business anticipation scenarios remain underdeveloped, and few preventive measures prior to the potential exfiltration and publication of data were implemented. This conveys a low level of maturity with regards to anticipation.

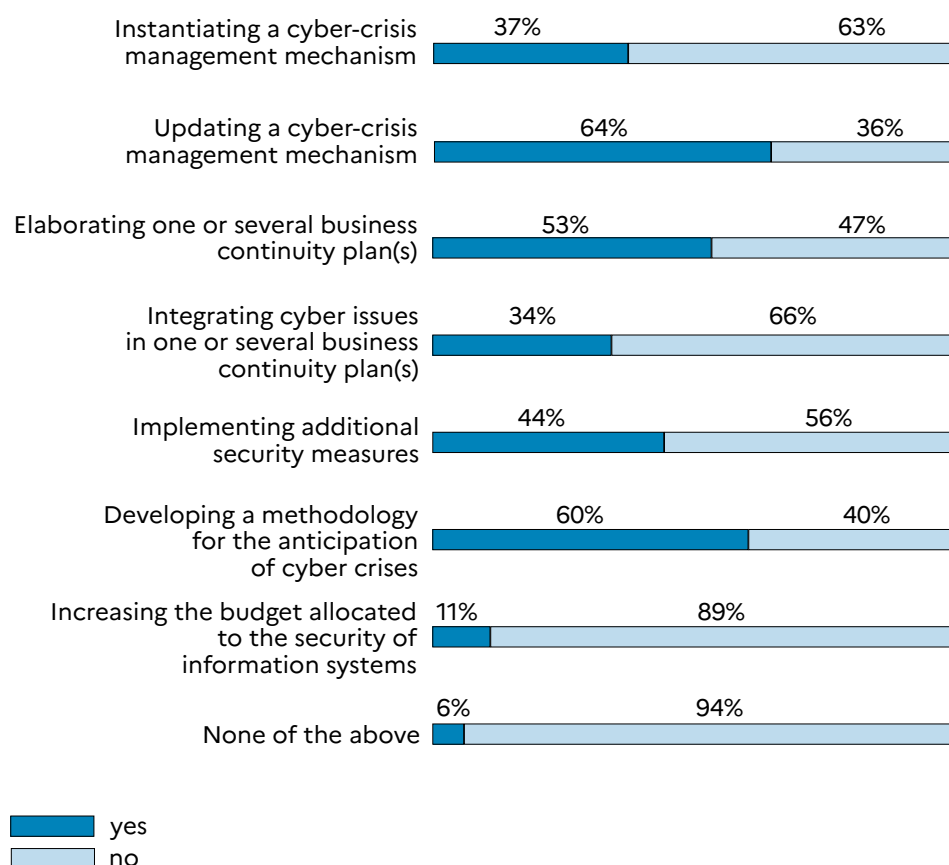
### Areas of improvement identified by participants in their post-exercise action plan

A few weeks after the exercise, autonomous participants were invited to share the major areas of improvement they had subsequently incorporated into their action plans. The main takeaway from this feedback is that participants now have a better grasp of the importance of addressing the subject head-on; for around 95% of them in fact, REMP25 was an opportunity to implement new measures in crisis management and/or information system security.

About 80% of respondents reportedly instantiated or updated their cyber-crisis management mechanisms, and over 60% expressed a desire to elaborate a business continuity plan or to integrate cyber issues in an existing BCP. Close to half of the participants plan to implement additional security measures.

Beyond these organisational, methodological, or documentation-related measures, the question of ISS budget allocation remains a difficult subject for a majority of organisations.

### MEASURES IDENTIFIED IN PARTICIPANT FEEDBACK



## Going one step further

An exercise kit made available to all to facilitate the organisation of a crisis exercise.

In an effort to facilitate participation in REMPLAR25 for all organisations, ANSSI provides the necessary documents and materials on its [website](#).

**The “REMPAR25” kit is made up of the following components:**

- Exercise implementation and adaptation webinars
- A scenario detailing the chain of compromise and the associated chronograms;
  - A primary chronogram, with several sectorial variants;
  - Chronograms intended for territorial and sectorial CSIRTs;
  - Chronograms intended for prefectures (Departmental Operational Centres – DOC)
- Attachments associated with chronogram stimuli
- Tool box: crisis directory, logbook, observation checklist;
- Briefing documents for moderators and observers;
- Simulation file;
- Documents pertaining to the organisation and conduct of feedback collection;

ANSSI encourages organisations to capitalise on this feedback and to utilise the ready-to-use kit to implement it. Crisis exercises are effective tools to develop a greater, shared understanding of the issues at hand amongst pluridisciplinary teams. The best way to manage a cyber crisis is to prepare for it.

# APPENDIX

## LIST OF PARTNERSHIPS

REGION	PARTNER
Auvergne-Rhône-Alpes	Campus Région du numérique
Bourgogne-Franche-Comté	Préfecture de la région Bourgogne-Franche-Comté Direction régionale de l'économie, de l'emploi, du travail et des solidarités (DREETS)
Bretagne	Agence régionale de santé Bretagne / e-Santé Bretagne Breizh Cyber Bretagne Cyber Alliance CLUSIR Bretagne Cyber place École des hautes études en santé publique European Digital Innovation Hub Bretagne GACYB Bretagne Le Pool Pôle d'excellence Cyber Préfecture d'Ille-et-Vilaine
Centre-Val de Loire	CybeRéponse Ministère de l'économie, des finances et de la Souveraineté industrielle Service de l'information stratégique et sécurité économiques Service départemental d'incendie et de secours du Loiret
Corse	Agence de développement économique de la Corse CAPA Paesi d'Aiacciu (Communauté d'agglomération du Pays Ajaccien) CLUSIR Corsica Collectivité de Corse CSIRT CyberCorsica Préfecture de Corse
Grand Est	Grand Reims Numica
Hauts-de-France	Campus Cyber Hauts-de-France Lille Métropole CLUSIR Nord de France
Île-de-France	Campus Cyber Club de la continuité d'activité CESIN CLUSIF Métropole du Grand Paris
La Réunion	Cyber Réunion
Normandie	Agence de développement pour la Normandie
Nouvelle-Aquitaine	Campus régional de cybersécurité et de confiance numérique de Nouvelle-Aquitaine
Occitanie	Cyber'Occ
Pays de la Loire	Nantes Digital Week Nantes Métropole
Polynésie française	Haut-commissariat de la République en Polynésie française
Provence-Alpes-Côte d'Azur (site de Marseille)	Campus Cyber Région Sud / Euromed CCI Aix-Marseille-Provence Métropole Aix-Marseille-Provence
Provence-Alpes-Côte d'Azur (site de Sophia Antipolis)	Campus Cyber Région Sud / Sophia Antipolis CCI Nice Côte d'Azur CLUSIR Sud – PACA Communauté d'agglomération Sophia Antipolis Entreprise Europe Network Sictiam Telecom Valley Urgence Cyber région Sud Région de gendarmerie de Provence-Alpes-Côte d'Azur
National	Campus Cyber Club de la continuité d'activité

Version 1.0 – February 2026

Open Licence (Etalab — v2.0)

**FRENCH CYBERSECURITY AGENCY**

ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP

[www.cyber.gouv.fr](http://www.cyber.gouv.fr)

