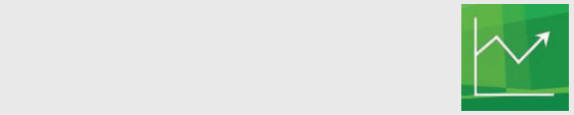
EN 2022

05

Special report

Cybersecurity of EU institutions, bodies and agencies

Level of preparedness overall not commensurate with the threats



CURIA RATIONUM

EUROPEAN
COURT
OF AUDITORS

Contents

Executive summary

I The EU Cybersecurity Act defines cybersecurity as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats". Due to the sensitive information they process, EU institutions, bodies and agencies (EUIBAs) are attractive targets for potential attackers, particularly groups capable of executing highly sophisticated stealth attacks for cyber espionage and other purposes. EUIBAs are strongly interconnected, despite their institutional independence and administrative autonomy. Therefore, weaknesses in individual EUIBAs could expose others to security threats.

II Given that the number of cyberattacks on EUIBAs is increasing sharply, the objective of this audit was to determine whether the EUIBAs, as a whole, have established adequate arrangements to protect themselves against cyber threats. We conclude that the EUIBA community has not achieved a level of cyber preparedness commensurate with the threats.

III We found that key cybersecurity good practices were not always implemented, including some essential controls, and a number of EUIBAs are clearly underspending on cybersecurity. Sound cybersecurity governance is also not yet in place in some EUIBAs: IT security strategies are in many cases lacking or are not endorsed by senior management, security policies are not always formalised, and risk assessments do not cover the entire IT environment. Not all EUIBAs have their cybersecurity regularly subject to independent assurance.

IV Cybersecurity training is not always systematic. Just over half of EUIBAs offer ongoing cybersecurity training for IT staff and IT security specialists. Few EUIBAs provide mandatory cybersecurity training for managers responsible for IT systems containing sensitive information. Phishing exercises are an important tool for training staff and raising awareness, but not all EUIBAs use them systematically.

V While EUIBAs have established structures for cooperation and information exchange on cybersecurity, we noted that potential synergies are not fully exploited. EUIBAs do not systematically share with each other information on cybersecurity-related projects, security assessments and service contracts. Furthermore, basic communication tools such as encrypted email or videoconference solutions are not fully interoperable. This can lead to less secure exchanges of information, duplication of efforts and increased costs.

VI The Computer Emergency Response Team of the EUIBAs (CERT-EU) and the European Union Agency for Cybersecurity (ENISA) are the two main entities tasked with supporting EUIBAs on cybersecurity. However, due to resource constraints or priority being given to other areas, they have not been able to provide EUIBAs with all the support they need, particularly in relation to capacity building for less mature EUIBAs. Although CERT-EU is highly valued by the EUIBAs, its effectiveness is compromised by an increasing workload, unstable funding and staffing, and insufficient cooperation from some EUIBAs, which do not always share timely information on vulnerabilities and on significant cybersecurity incidents that have impacted them or may impact others.

VII Based on these conclusions, we recommend that:

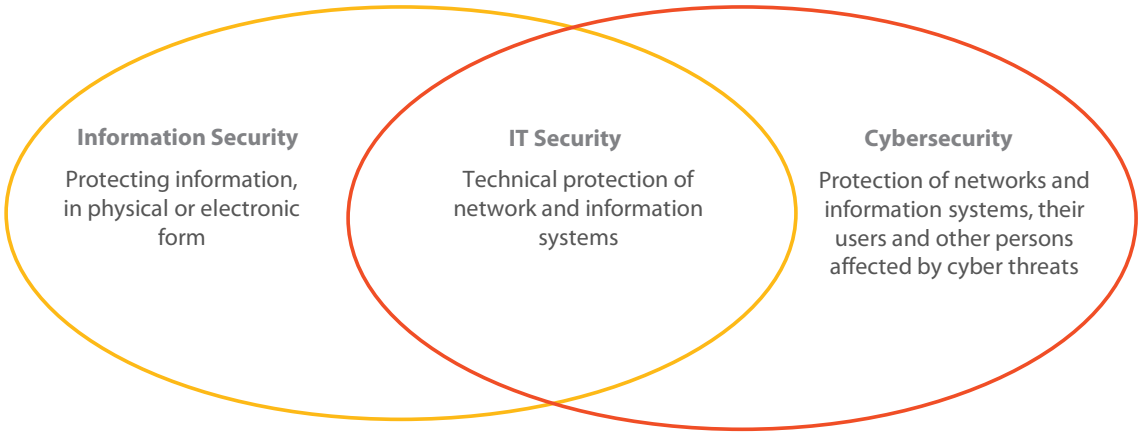
- the Commission improve the cyber preparedness of EUIBAs through a legislative proposal introducing common binding rules on cybersecurity for all EUIBAs and increased resources for CERT-EU;
- the Commission, in the context of the Interinstitutional Committee for the Digital Transformation, promotes further synergies among EUIBAs in selected areas;
- CERT-EU and ENISA increase their focus on EUIBAs that are less mature in cybersecurity;

Introduction

What is cybersecurity?

01 The EU Cybersecurity Act[1] defines cybersecurity as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats". Cybersecurity relies on information security, which is about preserving confidentiality, integrity and availability of information[2], whether in physical or electronic form. In addition, the protection of network and information systems where such information is stored is known as information technology (IT) security (See ***Figure 1***).

Figure 1 – Cybersecurity is linked to information security and IT security



Source: ECA.

02 As a discipline, cybersecurity involves identifying preventing, detecting, responding to and recovering from cyber incidents. Incidents may range, for example, from accidental disclosures of information to attacks aiming to compromise critical infrastructure, and to theft of identities and personal data[3].

03 A cybersecurity framework comprises many elements, including requirements and technical controls for the security of network and information systems, as well as appropriate governance arrangements and cyber awareness programmes for staff.

---

1 Regulation (EU) 2019/881.

2 ISO/IEC 27000:2018.

3 ECA review 02/2019: Challenges to effective EU cybersecurity policy (Briefing Paper).

Cybersecurity in EU institutions, bodies and agencies

04 Due to the sensitive information they process, EU institutions, bodies and agencies (EUIBAs) are attractive targets for potential attackers, particularly groups capable of executing highly sophisticated, stealth attacks ("advanced persistent threats") for cyber espionage and other purposes[4]. Successful cyber-attacks against EUIBAs can have significant political implications, harm the overall reputation of the EU and undermine the trust in its institutions.

05 The COVID-19 pandemic has forced EUIBAs, like many other organisations worldwide, to abruptly accelerate the digital transformation and embrace remote working. This has considerably increased the number of potential access points for attackers (the "attack surface"), expanding each organisation's perimeter to internet-connected homes and mobile devices, where new vulnerabilities can be exploited. Remote access services are one of the most common routes by which groups targeting EUIBAs with advanced persistent threats obtain initial access to their networks[5].

06 The number of cyber incidents is on the rise, and a particularly concerning trend is the dramatic increase in significant incidents affecting EUIBAs[6], making 2021 a record-setting year. Significant incidents are incidents that are neither repetitive nor basic. They typically involve the use of new methods and technologies and can take weeks if not months to investigate and recover from. Significant incidents increased more than tenfold between 2018 and 2021[7]. At least 22 individual EUIBAs have been hit by significant incidents in the past two years alone. One recent example was the cyberattack on the European Medicines Agency, where sensitive data was leaked and manipulated in a way designed to undermine trust in vaccines[8].

07 EUIBAs are a very heterogeneous group, comprising institutions, agencies and a number of different bodies. The seven EU institutions are established by the Treaties. EU decentralised agencies and other bodies, on the other hand, are set up by acts of secondary legislation and are each separate legal entities. There are different legal types of agencies: six Commission executive agencies and 37 EU decentralised

---

4 CERT-EU, Threat Landscape Report, June 2021.

5 Ibid.

6 Ibid.

7 Ibid.

8 Cyberattack on EMA – update 6, 25.1.2021.

agencies[9]. EUIBA also include EU offices, a diplomatic corps (the European External Action Service), joint undertakings and other bodies. EUIBAs are each responsible for defining their own cybersecurity requirements and implementing their own security measures.

08 To reinforce the cybersecurity of EUIBAs, in 2012 the Commission established the Computer Emergency Response Team of the EUIBAs (CERT-EU) as a permanent task force. CERT-EU acts as the cybersecurity information exchange and incident response coordination hub for the EUIBAs, and cooperates with other computer security incident response teams (CSIRTs) in Member States and specialised IT security companies. The organisation and operation of CERT-EU are currently governed by a 2018 interinstitutional arrangement[10] (IIA) between the EUIBAs it serves, also known as its "constituents". There are currently 87 constituents.

09 Another key player supporting EUIBAs is the European Union Agency for Cybersecurity (ENISA), which is dedicated to achieving a high common level of cybersecurity across the EU. Established in 2004, ENISA's mission is to enhance the trustworthiness of information and communications technology (ICT) products, processes and services with cybersecurity certification schemes, to cooperate with EUIBAs and Member States, and to help them prepare against cyber threats. ENISA assists EUIBAs in capacity building and operational cooperation.

10 Despite their institutional independence, EUIBAs are strongly interconnected. They exchange information on a daily basis and share a number of common systems and networks. Weaknesses in individual EUIBAs could expose others to security threats, as many cyberattacks take more than one step to reach their objective or final target[11]. A successful attack against a weaker EUIBA may be used as a stepping stone to target others. EUIBAs are also interconnected with public and private organisations in Member States and, by not being sufficiently cyber prepared, may likewise expose them to cyber threats.

11 Currently, there is no legal framework for information security and cybersecurity in EUIBAs. They are not subject to the broadest EU legislation on cybersecurity, the

---

[9] ECA special report 22/2020: Future of EU agencies – Potential for more flexibility and cooperation, paragraph 01.

[10] OJ C 12, 13.1.2018, p. 1.

[11] ENISA, Threat Landscape 2020, Sectoral/thematic threat analysis.

2016 NIS directive[12], nor to its proposed revision, the NIS2 directive[13]. There is also no comprehensive information on the amount spent by EUIBAs on cybersecurity.

12 In July 2020, the Commission published a communication on the EU Security Union Strategy[14] for the 2020-2025 period. Its key actions include "common rules on information security and on cybersecurity for all EUIBAs". This new framework is intended to underpin strong and efficient operational cooperation centring around the role of CERT-EU. In the EU Cybersecurity Strategy for the Digital Decade[15], published in December 2020, the Commission undertook to propose a regulation on common cybersecurity rules for all EUIBAs. It also proposed the establishment of a new legal basis for CERT-EU to reinforce its mandate and funding.

[12] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

[13] Proposal for a Directive on measures for a high common level of cybersecurity across the Union.

[14] COM(2020) 605 final.

[15] JOIN(2020) 18 final.

Audit scope and approach

13 Given that the number of cyberattacks is increasing sharply and that weaknesses in one EUIBA can expose others to security threats, the objective of this audit was to determine whether the EUIBAs have established adequate arrangements, as a whole, to protect themselves against cyber threats. To answer this main audit question, we addressed three sub-questions:

(1) Are key cybersecurity practices adopted across EUIBAs?

(2) Is there efficient cooperation between the EUIBAs on cybersecurity?

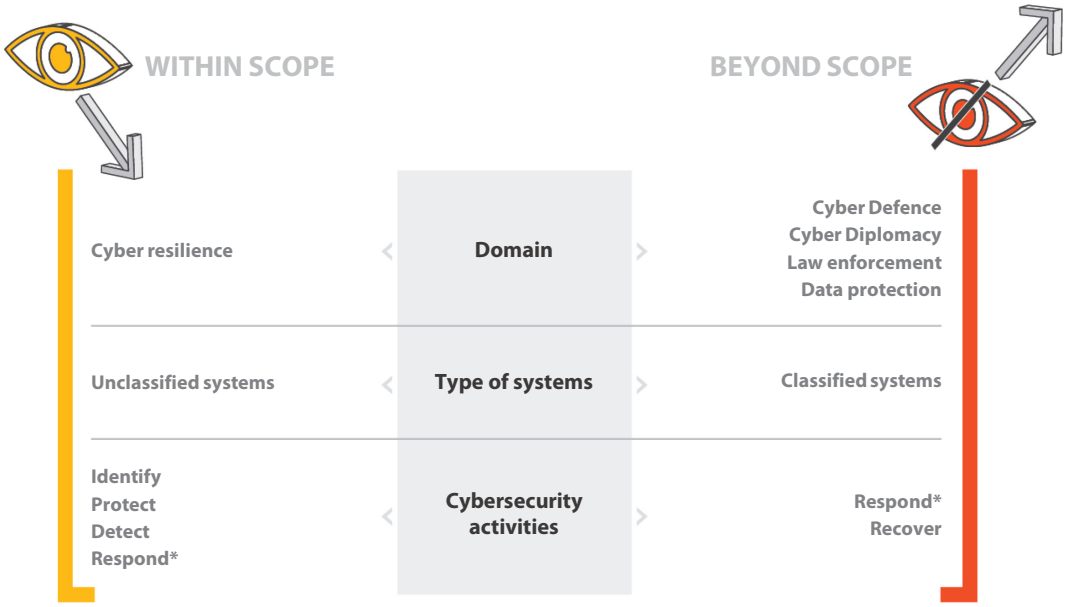
(3) Do ENISA and CERT-EU provide adequate support to EUIBAs in the field of cybersecurity?

14 The timing of the audit is aligned with the EU Security Union Strategy. By assessing the EUIBAs' current cybersecurity arrangements, we aim to identify areas for improvement, which the Commission can consider when drafting its legislative proposal for common binding cybersecurity rules for all EUIBAs.

15 The audit covered developments and initiatives in the area of cybersecurity from January 2018 (when the CERT-EU interinstitutional arrangement was established) until October 2021.

16 We limited our audit scope to cyber resilience and unclassified systems. We focused on preparedness aspects (activities corresponding to "identify, protect, detect"). "Respond" and "recover" were beyond our scope. However, we examined some organisational elements of incident response. In addition, data protection, law enforcement, cyber defence and cyber diplomacy aspects are beyond our scope (see ***Figure 2***).

Figure 2 – Audit scope



Source: ECA.

17 Our audit findings are based on extensive analysis of available documentation, complemented by interviews. We carried out a self-assessment survey involving 65 EUIBAs to collect information on their cybersecurity arrangements and their views on interinstitutional cooperation. We surveyed all EUIBAs that are covered by the ECA's audit rights and manage their own IT infrastructure, as well as our own institution. These included institutions, decentralised agencies, joint undertakings and bodies. We also surveyed civilian missions, which are temporary autonomous entities funded by the EU budget and independent from an IT perspective. ***Annex I*** provides a full list of the EUIBAs surveyed. The European Ombudsman and the European Data Protection Supervisor were not included in the scope of this audit.

18 The survey had a 100 % response rate and served as a starting point for further analysis. In addition, we selected a sample of seven EUIBAs that is representative of the heterogeneity of EUIBAs and followed up on their responses with interviews and requests for documentation. The selection criteria we considered included legal basis, size (in terms of staff and budget) and sector. The sample of EUIBAs consisted of the European Commission, the European Parliament, the EU Agency for Cybersecurity (ENISA), the European Banking Authority (EBA), the European Maritime Security Agency (EMSA), the EU Advisory Mission in Ukraine (EUAM Ukraine), and the Innovative Medicines Initiative Joint Undertaking (IMI JU).

19 We also held video meetings with CERT-EU, the Agency Network's ICT Advisory Committee (ICTAC), the Interinstitutional Committee for Digital Transformation (ICDT) and other relevant stakeholders.

Observations

EUIBAs have very different levels of cybersecurity maturity and do not always comply with good practice

20 This section examines the EUIBAs' individual arrangements and cybersecurity frameworks. We assessed whether they approach cybersecurity consistently and adequately, in terms of IT security governance, risk management, allocation of resources, awareness training, controls and independent assurance.

IT security governance in EUIBAs is often not well developed and risk assessments are not comprehensive

There are gaps in IT security governance in many EUIBAs

21 Good governance plays an essential role in an effective framework for the security of information and IT systems, as it defines the organisation's objectives and provides direction through prioritisation and decision-making. According to the Information Systems Audit and Control Association (ISACA)[16], an IT security governance framework should generally include several elements:

- a comprehensive security strategy intrinsically linked with business objectives;
- governing security policies that address each aspect of the strategy, controls and regulation;
- a complete set of standards for each policy describing the operational steps necessary to comply with policy;
- institutionalised monitoring processes to ensure compliance and provide feedback on effectiveness;
- an effective organisational structure with no conflicts of interest.

22 We found shortcomings in IT security governance in many EUIBAs. Only 58 % of EUIBAs (38 out of 65) have an IT security strategy or at least an IT security plan approved at board/senior management level. A breakdown by EUIBA type reveals that civilian missions and decentralised agencies (which together account for 71 % of the

[16] ISACA, Certified Information System Auditor review manual, 2019.

EUIBA surveyed) have the lowest percentages (see ***Table 1***). Not having an IT security strategy or IT security plan approved at senior management level entails the risk of top management not being aware of, or not sufficiently prioritising, IT security issues.

Table 1 – Percentage of EUIBAs with an IT security strategy or plan approved by senior management

Breakdown by number of staff

< 100 staff (22 EUIBAs)	100 to 249 staff (17 EUIBAs)	250 to 1 000 staff (16 EUIBAs)	>1 000 staff (10 EUIBAs)
45 %	53 %	69 %	80 %

Breakdown by EUIBA type

Decentralised agencies (35 EUIBAs)	Civilian missions (11 EUIBAs)	Bodies (4 EUIBAs)	Institutions (6 EUIBAs)	Joint undertakings (9 EUIBAs)
45 %	56 %	75 %	83 %	89 %

Source: ECA survey.

23 We examined the IT security strategies/plans provided by the seven sampled EUIBAs (see paragraph ***18***). We found the EUIBAs' strategies to be reasonably well connected to their business objectives. For example, the Commission's IT security strategy covers the IT security dimension of the European Commission Digital Strategy[17] and is designed to support its roadmap and objectives. However, only three EUIBAs in our sample had included in their IT security strategies/plans concrete goals and a timeframe for their achievement.

24 Security policies set the rules and procedures that individuals using or managing information and IT resources must follow. They help mitigate cybersecurity risks and inform what to do in case of incidents. We found that 78 % of EUIBAs have a formal information security policy, while only 60 % have formal IT security policies (see ***Figure 1*** for the definitions of information and IT security). We also found that four out of the seven EUIBAs in our sample have security policies in line with their IT security strategies. However, in three of these four, IT security policies are only partially complemented by up-to-date detailed security standards describing the operational steps necessary to implement the policies. The lack of formal security standards increases the risk of IT security issues not being dealt with appropriately and consistently across the same EUIBA. Furthermore, it makes it harder to measure the

[17] Communication to the Commission, European Commission digital Strategy: A digitally transformed, user-focused and data-driven Commission, C(2018) 7118 final, 21.11.2018.

organisation's compliance with its IT security policy. Of the seven EUIBAs sampled, only the Commission has structured procedures for monitoring compliance with its IT security policies and standards, albeit used only by a limited number of Directorate-General (DG) (see ***Box 1***).

Box 1

IT security compliance at the Commission

In line with the Commission's devolved IT governance, the head of each DG is the service owner responsible and accountable for its systems meeting IT security standards. The Directorate-General for Informatics (DG DIGIT) and the Directorate-General for Human Resources and Security (DG HR) monitor and facilitate the implementation of compliance management practices. DG DIGIT has set up a tool (known as "GRC") which allows DGs to measure and report on their compliance with IT security policy controls.

The 580 controls are divided into three groups: general controls (mostly on governance); DG specific controls; and system-specific controls. The tool is operational, but only five DGs are using it so far. DG DIGIT therefore has no overview of compliance across the Commission as a whole. However, the Commission's Information Technology and Cybersecurity Board (ITCB), may request DG DIGIT to investigate compliance with a specific standard (e.g. multi-factor authentication in 2021) and can issue non-binding opinions and recommendations or, for critical risks, also formal requirements.

25 Another important element in good cybersecurity governance is the appointment of a Chief Information Security Officer (CISO). Although not explicitly required by the ISO 27000 family of standards[18], having a CISO or equivalent role has become a widespread practice across organisations and is part of the ISACA guidelines. Typically, the CISO has overall responsibility for the organisation's information and IT security programmes. To avoid any conflict of interest, the CISO should have a certain degree of independence from the IT function/department[19].

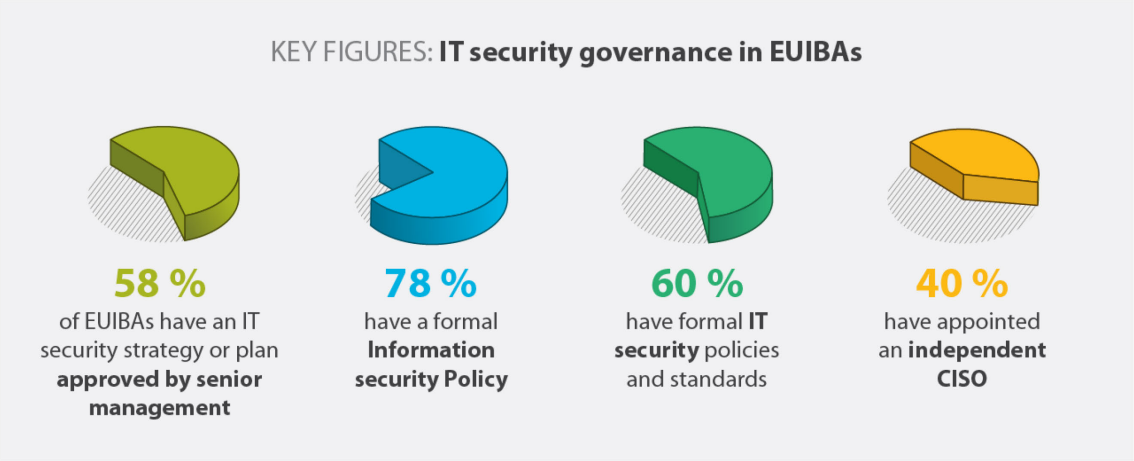
26 According to our survey, 60 % of EUIBAs have not designated an independent CISO or equivalent role. Even when CISOs (or equivalent) are appointed, their roles differ greatly in nature – and their functions are understood differently – between EUIBAs. Especially in small and medium-sized EUIBAs, CISOs tend to be associated with more operational roles, not functionally independent from the IT department.

---

[18] ISO/IEC standard 27000:2018, chapter 5.

[19] COBIT 5 for Information Security, section 4.2.

This may limit the CISOs' autonomy to implement their security priorities. ENISA is currently working on a EU Cybersecurity Skills Framework that, among others, aims to create a common understanding of roles, competencies and skills.



EUIBAs' IT security risk assessments mostly do not cover their entire IT environment

27 All the international standards for IT security underline the importance of establishing a suitable method for assessing and handling security risks affecting IT systems and the data they contain. Risk assessments should be performed periodically to address changes in an organisation's information security requirements and risks it faces[20]. The assessments should be followed by a risk mitigation plan (or an IT security plan).

28 Most EUIBAs surveyed (58 out of 65) indicated that they follow a framework or methodology to perform risk assessments on their IT systems. However, there is no common methodology across all EUIBAs. At least 26 EUIBAs make partial or full use of those developed by the Commission, in particular 31 % of EUIBAs used the 2018 IT security risk management methodology (ITSRM2). The others follow methodologies based on well-known industry standards (such as ISO27001, ISO27005, the National Institute of Standards and Technology cybersecurity framework (NIST-CSF) or Center for Internet Security (CIS) controls) or use other internal methodologies.

29 Among the seven EUIBAs sampled, only two perform comprehensive risk assessments covering their entire IT environment (i.e. all their IT systems). Most perform individual risk assessments only for their most important IT systems. We identified several examples of risk assessments carried out before deploying new

[20] See for example ISO/IEC 27000:2018, section 4.5.

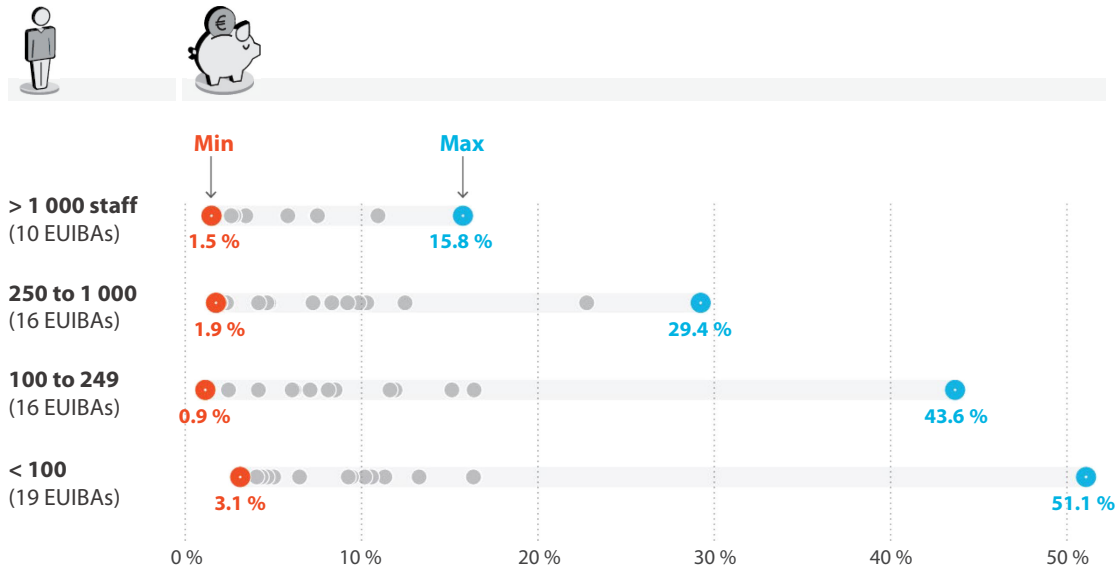
systems. However, we did not find evidence of follow-up risk assessments linked, for example, to subsequent changes to their systems/infrastructure.

EUIBAs do not approach cybersecurity consistently and essential controls are not always in place

The allocation of resources to cybersecurity varies widely among EUIBAs

30 In our survey, we asked EUIBAs to provide their total IT expenditure in 2020 and an estimate of the amount spent on cybersecurity. Our data shows significant variations in the percentage of IT expenditure individual EUIBAs allocate to cybersecurity. This is true even among EUIBAs of similar size, in terms of staff numbers. As shown in ***Figure 3***, differences tends to be particularly high among EUIBAs with fewer staff.

Figure 3 – Cybersecurity expenditure as percentage of total IT expenditure (EUIBAs grouped by number of staff)



Note: Four EUIBAs have not provided figures on cybersecurity expenditure.

Source: ECA survey.

31 An optimal level of cybersecurity spending is difficult to assess in absolute terms. It depends on many factors, such as the organisation's attack surface, the sensitivity of the data it handles, its risk profile and appetite, and sectoral legal/regulatory requirements. However, our data highlights that the differences are substantial and the reasons for this are not always obvious. Some EUIBAs spend considerably less on cybersecurity than their peers of similar size, which may indicate an underspending if they are exposed to similar threats and risks.

32 Most EUIBAs are small to medium in terms of both staffing and IT expenditure, with two thirds of EUIBAs having fewer than 350 staff. The smallest EUIBA has only 15 staff. Managing cybersecurity is more challenging and resource-intensive for smaller EUIBAs. In most cases, they cannot benefit from economies of scale and they do not have sufficient internal expertise. Based on our survey and interviews, the biggest institutions, such as the Commission and the European Parliament, have teams of experts that manage cybersecurity full time. However, at the smallest EUIBAs, where staff and resources are particularly limited, there are no experts at all, and cybersecurity is managed part time by staff with an IT background. Since EUIBAs are strongly interconnected, this poses an increased risk (see also paragraph ***10***).

33 In our survey, we asked EUIBAs what the major challenges were in implementing effective cybersecurity policies in their organisations (see ***Figure 4***). The biggest challenge is that cybersecurity experts are a scarce resource and many EUIBAs struggle to attract them, due to competition both from the private sector and from other EUIBAs. Recurrent issues include lengthy recruitment procedures, uncompetitive contractual conditions and lack of attractive career prospects. The shortage of specialist staff poses a significant risk to the effective handling of cybersecurity.

Figure 4 – Challenges in implementing effective cybersecurity policies in EUIBAs (more than one factor could be selected)

Source: ECA survey.

Most EUIBAs offer some form of cybersecurity awareness training, but it is not systematic or well targeted

34 Taking advantage of vulnerabilities in systems and devices is not the only way for potential attackers to cause harm. They can also induce users to reveal sensitive information or download malicious software, for example through phishing or social engineering. Staff are part of the first line of defence for every organisation. Therefore,

cyber awareness and training programmes are a key element in an effective cybersecurity framework.

35 The vast majority of the EUIBAs surveyed (95 %) provide some form of general cyber-awareness training for all staff, but three do not. However, only 41 % of EUIBAs organise specific training or awareness sessions for managers and only 29 % provide mandatory cybersecurity training for managers responsible for IT systems containing sensitive information. Management awareness and commitment is crucial for effective cybersecurity governance. From the eleven EUIBAs that mentioned the absence of management support as a challenge to effective cybersecurity, only three provided some awareness training for their management. Ongoing cybersecurity training for IT staff and for IT security specialists is offered by 58 % and 51 % of EUIBAs respectively.

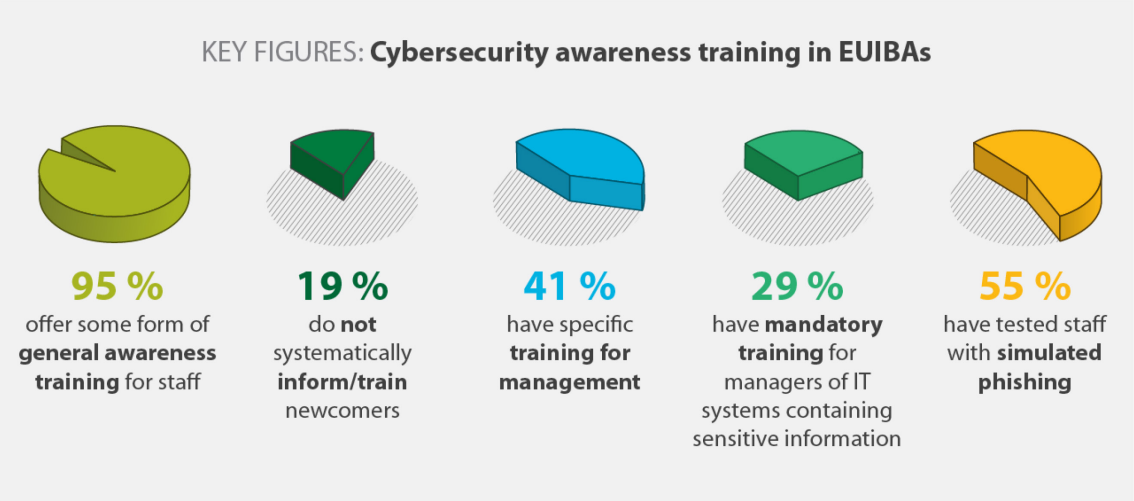
36 Not all EUIBAs have mechanisms to monitor staff attendance of cybersecurity training and the subsequent change in their awareness and behaviour. Especially in smaller organisations, cyber awareness sessions may be provided in the context of informal staff meetings. The main way organisations measure staff awareness is to periodically test them on their behaviours, including through maturity surveys or phishing exercises. In the past five years, 55 % of EUIBAs have organised one or more simulated phishing campaigns (or similar exercises). As phishing is one of the key threats facing staff in public administrations[21], these exercises are an important tool to train staff and raise awareness. We found the Commission's cyber awareness actions to be a good practice and available to other interested EUIBAs (see ***Box 2***).

Box 2

Cyber awareness training at the Commission

The Commission has a dedicated "Cyber Aware" team in DG DIGIT that leads the corporate cybersecurity awareness-raising programme. The programme is managed and run jointly with DG HR, the Secretariat-General, the Directorate-General for Communications Networks, Content and Technology (DG CNECT) and CERT-EU. The training is of a high quality and in many cases has an interinstitutional reach. Training sessions are advertised via the Learning Bulletin, which reaches around 65 000 EU staff. Through the "Cyber Aware" platform, the Commission has organised 15 phishing exercises in the past five years and recently performed the first Commission-wide exercise.

[21] ENISA, Thread Landscape 2020, Sectoral/Thematic threat analysis.



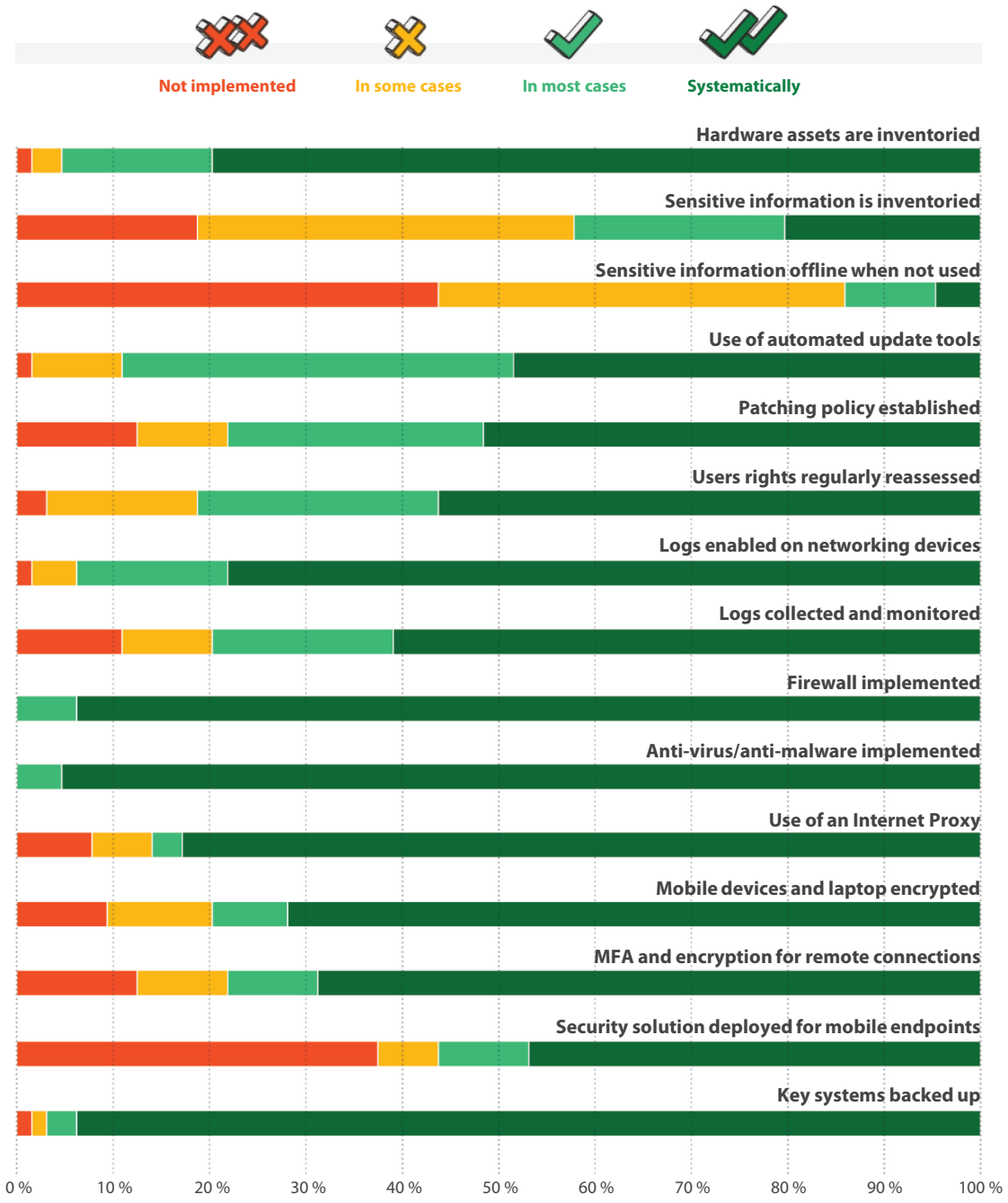
Essential controls are not always implemented, or are not formalised into standards

37 We asked EUIBAs to self-assess their implementation of a selection of essential controls[22]. We selected a set of best practices that even smaller organisation could reasonably implement[23]. The results are summarised in ***Figure 5***. Most EUIBAs surveyed have adopted the selected essential controls. However, for some areas, controls appear to be deficient or limited in at least 20 % of EUIBAs.

[22] Set of controls derived from the CIS Controls 7.1, a framework of best practices curated by the Centre for Internet Security.

[23] Implementation group 1 (IG1) of the CIS Controls.

Figure 5 – Implementation of essential controls in EUIBAs (self-assessment results)



Source: ECA survey.

38 For the seven EUIBAs sampled, we requested supporting documents and corresponding standards/policies for each control that they declared as having been implemented. We obtained these documents for 62 % of controls. As clarified during the interviews, in several cases technical controls were in place but were not formalised into - up to date - standards or policies, which increases the risk of IT

security issues not being dealt with consistently across the same EUIBA (see also paragraph ***24***).

Several EUIBAs do not have their cybersecurity arrangements subject to regular independent assurance

39 According to the ISACA[24], internal audit is one of the three essential lines of defence in an organisation, the other two being management and risk management. Internal audits contribute to improving information and IT security governance. We examined how frequently EUIBAs gather independent assurance on their IT security framework, through internal or external audits and through proactive testing of their cyber defences.

40 The Commission's Internal Audit Service (IAS) is responsible, among other things, for performing IT audits of the Commission, and of decentralised agencies, joint undertakings and the EEAS. The service's mandate covers 46 (70 %) of the 65 EUIBAs we surveyed and the IAS has performed audits related to IT security on 6 different EUIBAs in the past five years. In addition, DG HR is competent to perform IT security inspections covering technical information security aspects[25]. Of the remaining EUIBAs, seven reported having their own internal audit function covering IT aspects, but for twelve EUIBAs, the replies to our survey were not sufficient to determine whether they have such internal audit capacity.

41 External IT security audits carried out by independent entities are another way to gather independent assurance. Despite the rapidly changing cyber landscape, between the start of 2015 and the first quarter of 2021, 34 % of EUIBAs had not been subject to any internal or external IT security audit. A breakdown of the latter figure by EUIBA type reveals that 75 % of EU bodies, 66 % of joint undertakings and 45 % of civilian missions have not undergone an internal or external IT security audit since 2015.

42 Aside from internal and external audits, another way for organisations to obtain assurance on their IT security framework is by proactively testing their cyber defences to identify vulnerabilities. Penetration tests (also known as ethical hacking), consisting of authorised simulated cyberattacks on individual computer systems, are one method of doing this. In response to our survey, 69 % of EUIBAs stated they had performed at

---

[24] ISACA, Auditing Cyber Security: Evaluating Risk and Auditing Controls, 2017.

[25] Decision 46/2017 on the security of communication and information systems in the European Commission.

least one penetration test in the last five years. In 45 % of the cases, CERT-EU was the entity performing the penetration tests.

43 "Red team" exercises are another way to test cyber defences through simulated attacks, using techniques recently used in real-world attacks. They are more complex and comprehensive than penetration tests in that they involve multiple systems and potential avenues of attack. EUIBAs perform them less often: 46 % of EUIBAs reported at least one red team exercise in the past five years. CERT-EU performed 75 % of these exercises. Red team exercises require a substantial amount of work to prepare and perform and CERT-EU currently has the capacity to perform no more than five to six exercises per year.

44 Excluding two recently established EUIBAs, 16 (25 %) of the EUIBAs surveyed had not performed penetration tests or red team exercises in the past five years. Overall, seven EUIBAs (10 %) have not been subject to any form of independent assurance on their IT security arrangements: one joint undertaking, one decentralised agency and five civilian missions.

KEY FIGURES: **Independent assurance on IT security in EUIBAs in the past 5 years**

66 %
of EUIBAs were **subject** to at least **one internal or external audit** related to IT security

69 %
performed at least **a penetration test**

46 %
performed at least **a Red Team exercise**

10 %
were **not subject** to any form of **independent audit or testing** of IT security

EUIBAs have established mechanisms for cooperation but there are shortcomings

45 This section looks at the actors and committees established to promote cooperation among EUIBAs in the area of cybersecurity, as well as interinstitutional governance and coordinating arrangements. More specifically, we examined two interinstitutional actors, ENISA and CERT-EU, and two interinstitutional committees, the Interinstitutional Committee for Digital Transformation (ICDT), in particular its cybersecurity subgroup (CSSG), and the Information and Communication Technologies Advisory Committee (ICTAC). We also assessed the extent to which these have delivered synergies to increase EUIBAs' cybersecurity preparedness.

There is a formalised structure for EUIBAs to coordinate their activities, albeit with some governance issues

46 The ICDT and ICTAC are the two main committees promoting cooperation on IT among EUIBAs. Comprising the IT managers of the EU institutions and bodies, the ICDT is a forum for fostering information exchange and cooperation. It has a cybersecurity subgroup (ICDT CSSG) that reports to the ICDT and can recommend taking decisions on specific issues. ICTAC, on the other hand, is a subgroup of the EU Agencies Network (EUAN), an informal network set up by the heads of the EU agencies that focuses on cooperation among agencies and joint undertakings. Both the ICDT and ICTAC have clearly defined, complementary roles: ICTAC covers decentralised agencies and joint undertakings, while the ICDT covers institutions and bodies. By nature, ICDT and ICTAC are rather informal advisory groups and forums for exchanging information and best practice. More information on these interinstitutional committees is presented in ***Annex II***.

Representation of EUIBAs in relevant forums is not always adequate

47 Although the structures for representation are clear, not all EUIBAs consider their actual representation sufficient. When asked in our survey to provide an opinion on the statement "My needs are sufficiently considered in the relevant interinstitutional forums and my EUIBA has adequate representation in the decision-making boards", 42 % of EUIBAs disagreed. Some of the smallest ones considered that they did not have sufficient resources to actively participate in interinstitutional forums.

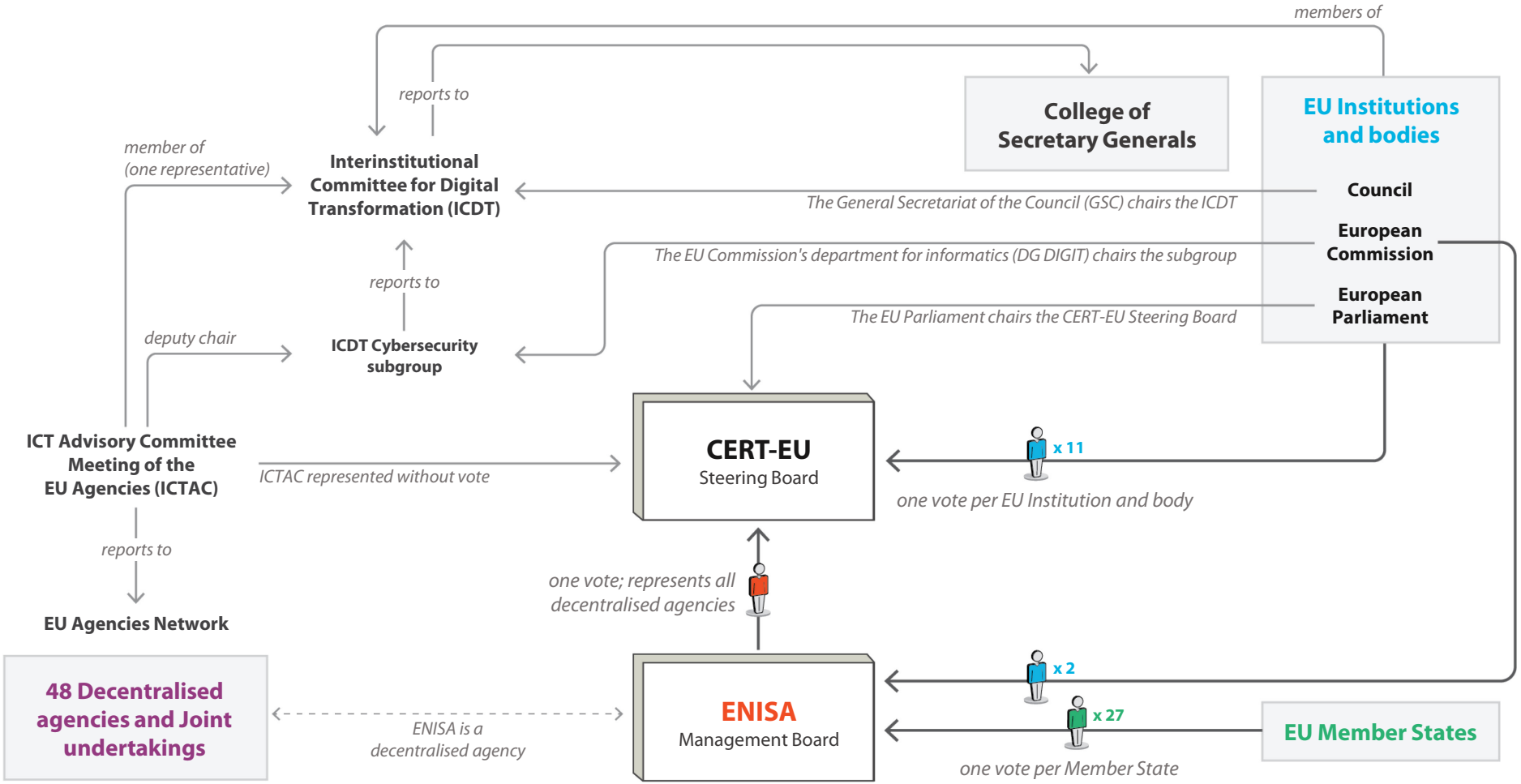
48 CERT-EU's steering board, its main decision-making body, is also not representative of its constituents as a whole. CERT-EU provides services to 87 EUIBAs and 3 non-EUIBAs. However, its steering board only includes representatives of the 11 signatories to the interinstitutional arrangement (the seven EU institutions plus the EEAS, the Economic and Social Committee, the Committee of the Regions and the European Investment Bank), and a representative of ENISA, each of them having one vote[26].

49 More than half of CERT-EU's constituents are EU decentralised agencies and joint undertakings, which together have approximately 12 000 staff. Formally, their interests are represented on CERT-EU's steering board by ENISA. However, ENISA's mandate to represent EU agencies and joint undertakings is weak, as it was not directly appointed or elected by them. In practice, the views of decentralised agencies

[26] Article 7 of the interinstitutional arrangement (IIA) signed on 20.12.2017.

and joint undertakings are voiced in steering board meetings by an ICTAC representative, who is permitted to attend to assist ENISA in its role of representing the agencies. Despite voicing the views and interests of 48 EUIBAs, the ICTAC representative currently has no formal seat or vote on the steering board. In April 2021, the ICTAC sent the chair of the CERT-EU steering board a formal request for voting rights on the board. At the time of writing, this request has not yet been granted. An overview of the representation of EUIBAs on decision-making boards and committees is provided in ***Figure 6***.

Figure 6 – Overview of cybersecurity governance and representation in decision-making boards and committees



Source: ECA.

50 The EUIBAs' interinstitutional cybersecurity governance is fragmented and no single entity currently has a comprehensive overview of EUIBAs' cybersecurity maturity, or the authority to take a lead role or to enforce common binding rules. Both ENISA and CERT-EU can only "support" and "assist" EUIBAs. The relevant committees have no decision-making power and can only make recommendations to the EUIBAs. Furthermore, for a fifth of the EUIBAs surveyed it is also not clear where to turn for a specific service, tool or solution.

Memoranda of understanding among key actors exist but so far they have not produced concrete results

51 A memorandum of understanding (MoU) between ENISA, CERT-EU, Europol's European Cybercrime Centre (EC3) and the European Defence Agency (EDA) was signed in May 2018. It focused on five areas of cooperation: information exchange; education and training; cyber exercises; technical cooperation; and strategic and administrative matters. Although this MoU could help avoid duplications by having a common work programme, we have not seen evidence that it has produced concrete deliverables and joint actions.

52 The Cybersecurity Act (CSA), which entered into force in June 2019, envisaged the signing of a new and specific cooperation arrangement between CERT-EU and ENISA. It is noteworthy that it took more than a year and a half to finally sign the MoU, in February 2021. This MoU attempts to establish structured cooperation between CERT-EU and ENISA. It defines their areas of cooperation (capacity building, operational cooperation, and knowledge and information) and sets out a rough division of roles between them: CERT-EU will take the lead in assisting EUIBAs, with ENISA contributing to the effort. The MoU does not define the practical arrangements, as they are specified in an annual cooperation plan. The first annual cooperation plan for 2021 was adopted by ENISA's management board in July 2021 and the CERT-EU steering board in September 2021. It is therefore too early for our audit to assess whether this plan has produced any tangible result.

53 As both the MoUs mentioned in paragraphs ***51*** and ***52*** have common aims and areas of cooperation such as training, exercises, or exchange of information, there is a risk of overlaps and redundancies.

Potential synergies through cooperation are not yet fully exploited

Positive steps have been taken to achieve synergies

54 The ICTAC and ICDT CSSG committees' work programmes identify relevant topics where efficiency gains can be achieved through collaboration. Practical examples of initiatives that have allowed EUIBAs to benefit from synergies include:

- interinstitutional framework contracts;
- a common disaster recovery centre hosted since 2019 by the European Union Intellectual Property Office (EUIPO) for the decentralised agencies, allowing for a cost saving of at least 20 % compared to market prices (nine agencies have adopted this disaster recovery solution);
- agreements between six joint undertakings located in the same building to share common infrastructure and a common IT security framework (since 2014).

55 Another important example is the "GovSec", a system that helps EUIBAs perform risk assessments in view of adopting cloud solutions. According to our survey, 75 % of EUIBAs already use some public cloud platforms, and several of those that do not are planning to migrate to the cloud. Since 2019, the Commission has pursued a "cloud-first" approach, envisaging a secure hybrid multi-cloud service offering[27]. The Commission also acts as a cloud broker for all EUIBAs, in the context of the "Cloud II" framework contract. Managing security and data protection risks on cloud platforms requires new skills and a different approach compared to traditional "on premise" IT infrastructure. Effective information security risk management in the cloud is a common challenge for EUIBAs, and GovSec is an example of a solution that may respond to the needs of several, if not all, EUIBAs.

Collaboration and practice sharing among EUIBAs is still not optimal

56 The existence of interinstitutional committees does not automatically lead to synergies, and EUIBAs do not always share best practices, expertise, methodologies and lessons learned. In addition, it is up to each EUIBA to decide on its level of engagement in the ICDT CSSG's work. Members of the ICDT CSSG, despite attending meetings, can only contribute to the extent that their regular duties in the EUIBAs allow, and this has already slowed progress in implementing the actions agreed by some task forces.

---

[27] European Commission, The European Commission Cloud Strategy, 2019.

57 We found specific areas where there are no arrangements for EUIBAs to share experience and initiatives. For example, under the "Network Defence Capability" (NDC) framework contract, EUIBAs can request a study to consolidate cybersecurity requirements and find out solutions. However, there is no repository of such studies performed or requested by other EUIBAs, and EUIBAs can therefore request the same study multiple times. In addition, EUIBAs do not systematically disclose to one another that they have contractual relationships with specific suppliers or use a specific software solution. This knowledge gap can lead to additional costs and missed synergies.

58 Neither do EUIBAs systematically share information with one another on cybersecurity projects they are undertaking, even if they could have an interinstitutional impact. The ICDT CSSG's mandate includes a provision for EUIBAs to share information on new projects potentially affecting the cybersecurity of other EUIBAs and/or the protection of information originating from them. However, the ICDT CSSG is not kept informed of such projects.

59 When a new agency is created, it has to build its IT infrastructure and IT security framework from scratch. There is no "service catalogue", toolbox or clear guidelines/requirements for new agencies. The result is substantial heterogeneity in IT environments across EUIBAs, where every organisation is potentially free to procure its own software, hardware, infrastructure and services independently. The same happens with the IT security framework, in the absence of common requirements and standards. This situation leads to potential duplication of efforts and inefficient use of EU money, but also to increased complexity for CERT-EU in terms of the support it needs to provide.

There are practical shortcomings in the exchange of sensitive information

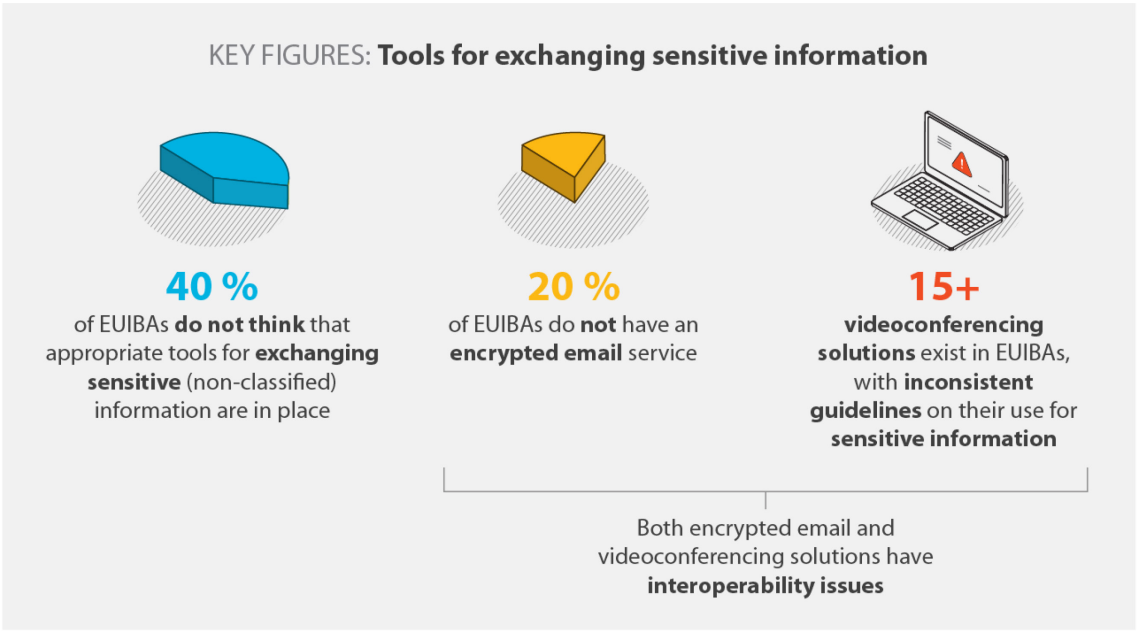
60 Some EUIBAs still do not have appropriate solutions for exchanging sensitive non-classified information. Those that do have generally adopted their own different products and systems, meaning interoperability is an issue. Common secure platforms exist only for specific purposes, an example being the platforms CERT-EU offers to all constituents for exchanging sensitive information on incidents, threats and vulnerabilities.

61 For example, more than 20 % of EUIBAs do not have an encrypted email service. Those that do often face interoperability issues and certificates are not mutually recognised. The ICTAC and ICDT have been discussing options for a scalable and

interoperable solution for years, and in 2018 there was a pilot project. However, this issue has not yet been resolved.

62 Another issue is the absence of common markings for sensitive non-classified information. Markings are categorisations that tell information holders the specific protection requirements for that information. They differ between EUIBAs, thus complicating the exchange and proper handling of information.

63 In 2020, the COVID-19 pandemic forced EUIBAs to adopt communication and videoconferencing tools on a large scale to ensure business continuity. We identified at least 15 different videoconferencing software solutions in use among EUIBAs. Even when different EUIBAs use the same solution/platform, interoperability is still often lacking even when all parties use the same software solution. In addition, guidelines on what information (in terms of sensitivity) could be shared or discussed on a given platform differed between EUIBAs. Such issues lead to economic and operational inefficiencies and may create potential security problems.



ENISA and CERT-EU have not yet provided EUIBAs with all the support they need

64 For this section, we examined the two main entities tasked with supporting EUIBAs on cybersecurity: ENISA and CERT-EU. We assess whether the support provided by both these entities has reached EUIBAs and is addressing their needs, highlighting the reasons behind the shortcomings identified.

ENISA is a key player in the EU cybersecurity landscape, but its support has so far reached very few EUIBAs

65 In June 2019, the Cybersecurity Act (CSA)[28], which replaced ENISA's previous legal basis[29], came into force and gave the agency a stronger mandate. More specifically, it provides that ENISA should actively support both Member States and EUIBAs in improving cybersecurity through capacity building, enhancing operational cooperation and establishing synergies. In the area of capacity building, ENISA now has a mandate to assist EUIBAs "in their efforts to improve the prevention, detection and analysis of cyber threats and incidents in particular through appropriate support for the CERT-EU"[30]. ENISA should also assist EU institutions in developing and reviewing EU cybersecurity strategies, promoting their dissemination and tracking progress in their implementation.

66 Although the CSA clearly states that ENISA should support EUIBAs in improving their cybersecurity, ENISA has not yet completed any action plans in relation to its objective of assisting EUIBAs' capacity building (see ***Box 3*** for details).

[28] ENISA's tasks are listed in in Chapter II (Articles 5-12) of Regulation (EU) 2019/881.

[29] Regulation (EU) No 526/2013 of the European Parliament and Council; for ENISA's tasks under this regulation, see Article 3.

[30] Article 6 of Regulation (EU) 2019/881.

Box 3

Insufficient alignment between ENISA's objective and outputs in relation to EUIBAs

Some of ENISA's three-year priorities listed in the 2018-2020 multiannual work programme under objective 3.2 "Assist EU institutions' capacity building" are:

- "Offer proactive advice to the Union institutions on the reinforcement of their network and information security (NIS) (Identify priorities for EU agencies and bodies with the most NIS capacity-building needs by establishing regular interactions with them (e.g. annual workshops) and focus on these priorities)";
- "Seek to assist with and facilitate EU institutions in relation to approaches on NIS (Make partnerships with CERT-EU and institutions with strong NIS capabilities with a view to supporting its actions under this objective.)"

In ENISA's 2018, 2019 and 2020 work programmes, there are only two operational objectives (outputs) under objective 3.2:

- "Participation in the Steering Board of CERT-EU and representation of the EU agencies using the CERT-EU service".
- "Cooperation with relevant EU bodies on initiatives covering NIS dimension related to their missions (including EASA, CERT-EU, EDA, EC3)".

The operational objectives do not include any activity related to proactive advice. In addition, the objective of identifying priorities for agencies with the greatest needs was not translated into operational outputs, as it was replaced by the objective of liaising with agencies to represent their needs on the CERT-EU steering board.

67 ENISA's main decision-making body is its management board, composed of one member appointed by each of the 27 Member States and two members appointed by the Commission[31] (see ***Figure 6***). Each member has one vote and decisions are taken by majority vote[32]. As a result, actions concerning Member States can have higher priority over those for EUIBAs. For example, in ENISA's 2018 work programme, the management board decided, due to lack of sufficient resources, to prioritise certain activities and remove three, one of which was "support for the assessment of existing policies/procedures/practices on NIS within EU institutions". This activity was meant to

[31] Article 14 of the CSA.

[32] Article 18 of the CSA.

allow ENISA to build an overview of EUIBAs' practices and indicative cybersecurity maturity, as a basis for future targeted actions.

68 Therefore, ENISA's ambition of providing proactive assistance to EUIBAs, as expressed in its strategic objectives, has not materialised into operational objectives or concrete actions. Support in the areas of capacity building and operational cooperation has so far been limited, upon request, to some specific EUIBAs.

69 The CSA also stipulates that, in order to assist EUIBAs with capacity building, ENISA should provide appropriate support to CERT-EU. At the time of the audit, such support had been limited to a few specific actions. For example, in 2019 ENISA carried out a peer review of CERT-EU, in the context of its membership of the EU CSIRTs network (established by the NIS Directive).

70 According to our survey responses, ENISA publishes high-quality reports and guidelines on cybersecurity, some of which are used by EUIBAs. However, there are no specific guidelines targeting EUIBAs and their own environment and needs. EUIBAs, especially those less advanced in cybersecurity, need practical guidance not only on "what" to do, but also "how" to do it. To date, ENISA and CERT-EU have provided such support to a limited, unsystematic extent.

71 ENISA has held a number of training courses on cybersecurity, which were mainly aimed at Member State authorities but also attended by a limited number of participants from EUIBAs. It provided only two self-learning courses specifically aimed at EUIBAs. ENISA also offers online training material on its website which EUIBAs can access, but to date these have been mainly courses for CSIRT technical experts and, as such, not helpful for most EUIBAs.

72 Apart from training, ENISA can support EUIBAs through cybersecurity exercises. In October 2020 ENISA, in cooperation with CERT-EU, helped to run a cybersecurity exercise for ICTAC, which is the only exercise ENISA has organised specifically for participants from EUIBAs. Apart from that, ENISA has helped organise a number of exercises at the request of some EUIBAs (e.g. EU-LISA, EMSA, the European Parliament and Europol), mainly for their stakeholders in Member State authorities, with some EUIBA staff also participating.

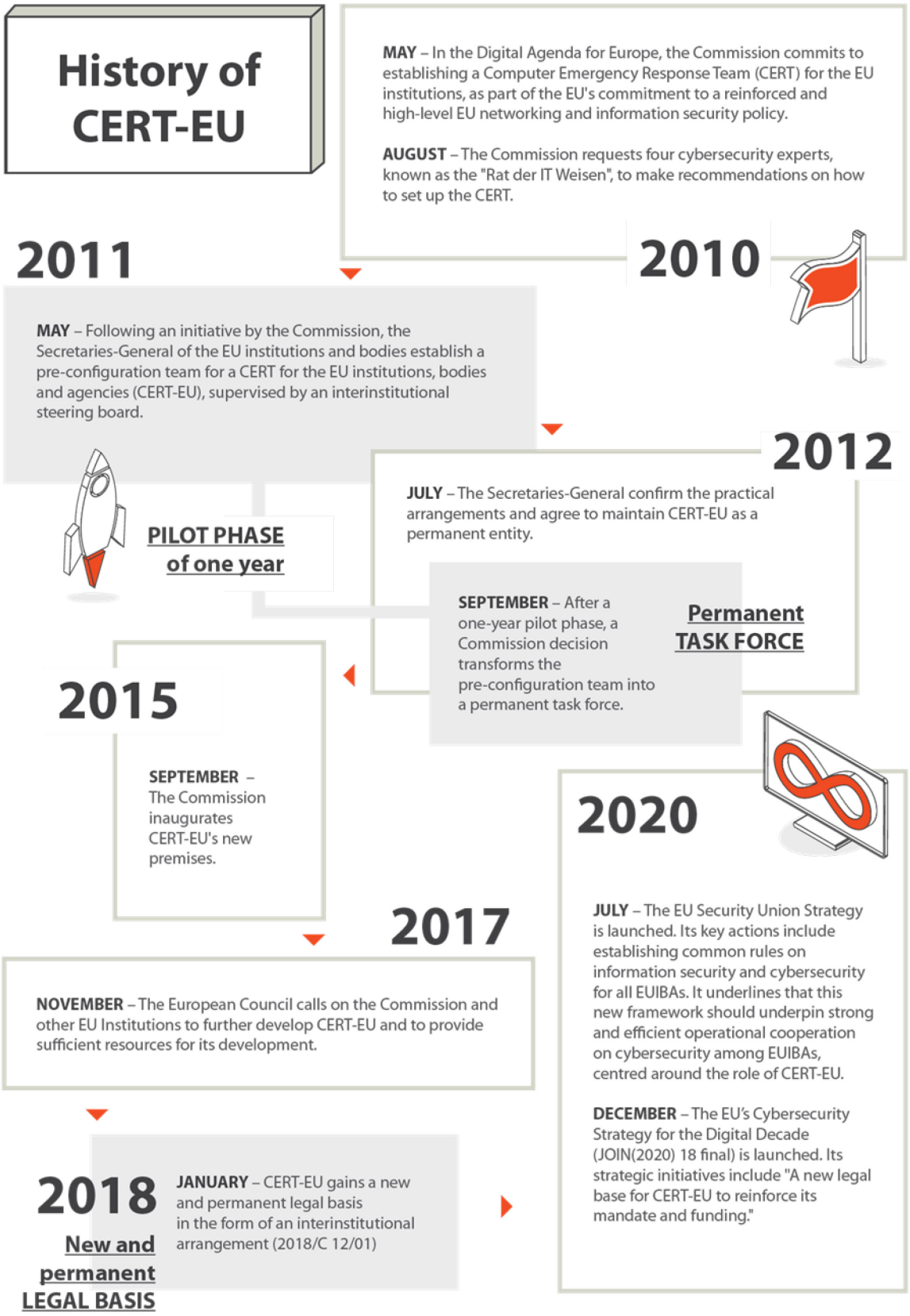
73 The CSA also introduced a new role for ENISA in assisting EUIBAs with their vulnerability disclosure policies, on a voluntary basis. However, ENISA has still no overview of individual EUIBAs' vulnerability disclosure policies and does not assist them in establishing and implementing these.

CERT-EU is highly valued by its constituents but its means are not commensurate with current cybersecurity challenges

74 Following a series of initiatives (see ***Figure 7***), in September 2012, a Commission decision[33] established the Computer Emergency Response Team (CERT-EU) as a permanent task force for the EUIBAs (see paragraph ***08***).

[33] European Commission press release: Cyber security strengthened at EU institutions following successful pilot scheme.

Figure 7 – History of CERT-EU



Source: ECA.

75 Although independent in its operations, CERT-EU remains a task force, with no legal personality. It is administratively posted in the European Commission (DG DIGIT), from which it receives logistical and administrative support. CERT-EU's aim is to make EUIBAs' ICT infrastructure more secure by enhancing their capacity to deal with cyber threats and vulnerabilities and to prevent, detect and respond to cyber attacks. CERT-EU has around 40 staff organised in teams of specialists focusing for example on cyber threat intelligence, digital forensic and incident response.

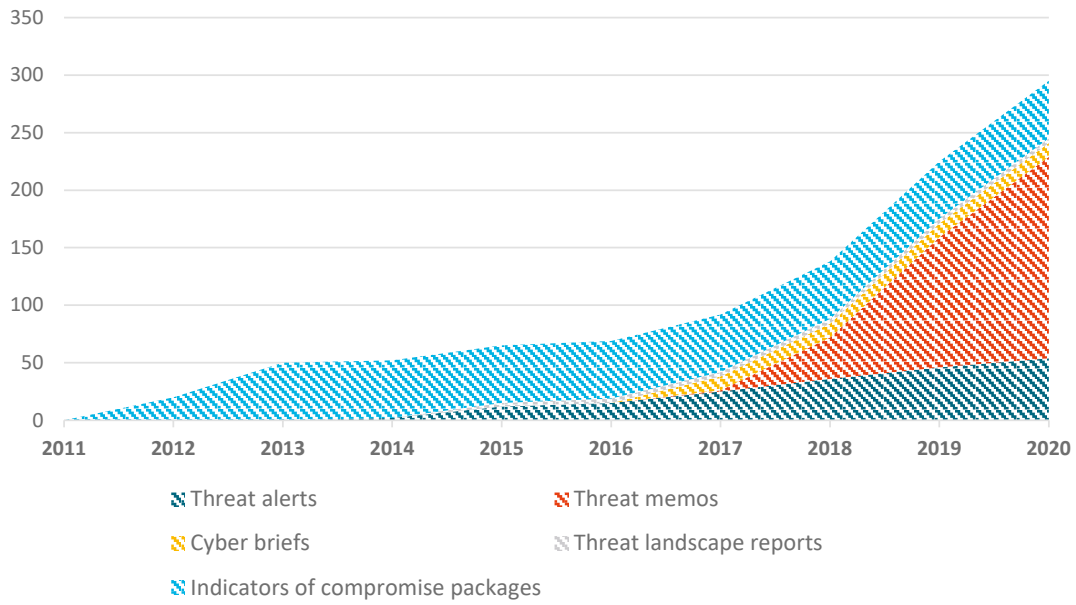
CERT-EU is an appreciated partner, with an increasing workload

76 CERT-EU requests feedback and suggestions from its constituents through quarterly workshops and annual bilateral meetings and satisfaction surveys. According to the satisfaction surveys and our own survey, constituents are largely satisfied with the services provided by CERT-EU. The evolution of CERT-EU's service catalogue attests to its effort to adapt to the needs of EUIBAs.

77 While large EUIBAs with significant in-house capacity tend to use CERT-EU mainly as an information-sharing hub and source of threat intelligence, smaller EUIBAs rely on CERT-EU for a wider array of services, such as monitoring logs, penetration tests, red team exercises and support for incident response. CERT-EU's services are particularly valuable for smaller EUIBAs, due to their limited internal expertise and lack of economies of scale (see paragraphs ***31*** and ***33***).

78 CERT-EU has strengthened its capabilities and procedures in recent years, against the backdrop of a dramatic increase in threats and incidents. The number of CERT-EU information products, in particular threat alerts and memos, has been growing constantly (***Figure 8***). In 2020, CERT-EU issued 171 threat memos and 53 threat alerts (considerably more than the 80 memos and 40 alerts it originally expected to issue).

Figure 8 – Increase in threat intelligence products



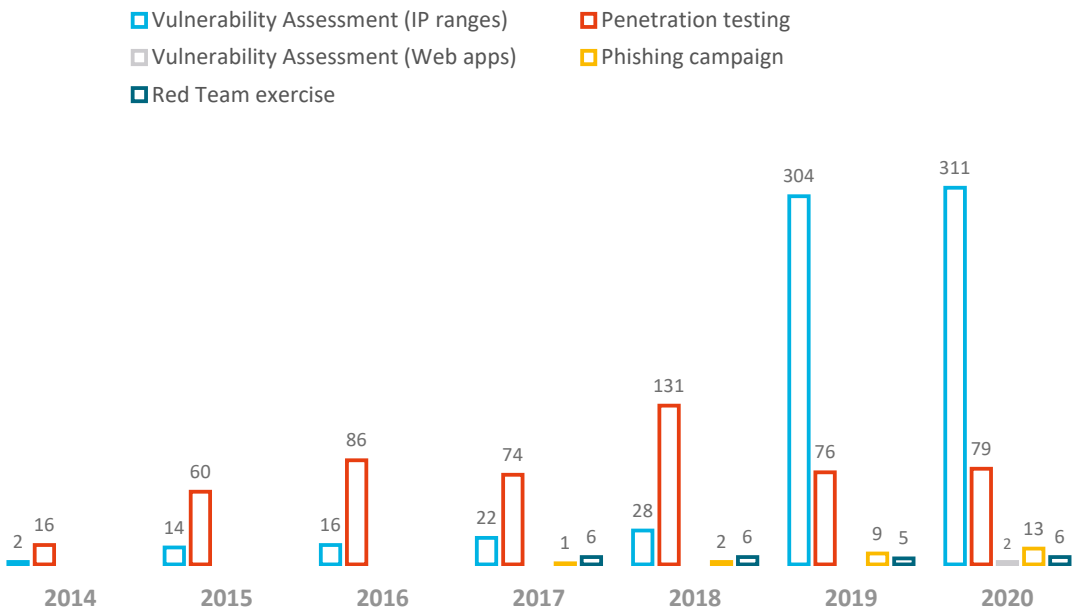
Source: ECA, based on CERT-EU data.

79 CERT-EU also supports EUIBAs in handling cyber incidents. While 52 % of EUIBAs have an internal response team or at least an incident coordinator, the other 48 % rely on CERT-EU and/or other external providers in the event of an incident. However, even large EUIBAs with in-house response capacity may request support from CERT-EU in dealing with complex incidents.

80 The total number of incidents handled by CERT-EU rose from 561 in 2019 to 884 in 2020. Significant incidents, in particular, have increased from just 1 in 2018, to 13 in 2020. In 2021, the number of significant incidents reached 17, up from 13 in 2020, which itself was a record-setting year. These significant incidents are generally caused by highly sophisticated threats. They may affect multiple EUIBAs, involve contact with authorities, and usually take weeks to months of work for the parties affected and for CERT-EU to investigate and eradicate.

81 CERT-EU is also the main provider of proactive assessments and tests of EUIBAs' cyber defences. A summary of CERT-EU's activity in this area is presented in ***Figure 9*** below. In addition, as from 2020, CERT-EU also performs external network scans.

Figure 9 – Tests and assessments performed by CERT-EU



Source: ECA, based on CERT-EU's data.

Constituents do not share relevant information with CERT-EU in a timely manner

82 The IIA[34] states that constituents should notify CERT-EU of significant cybersecurity incidents. However, in practice, this has not always happened. The IIA does not provide a mechanism to enforce mandatory and timely reporting of "significant" incidents by CERT-EU constituents. The generic definition of "significant incidents" in the IIA leaves it up to the discretion of the EUIBAs whether to report an incident. According to CERT-EU's management, some constituents have not shared information on significant incidents in a timely manner, hindering CERT-EU's role as a cybersecurity information exchange and incident response coordination hub for all EUIBAs. For example, one constituent facing a very sophisticated threat did not inform CERT-EU or seek its support. This prevented CERT-EU from gathering cyber threat intelligence that would have been useful when supporting other constituents facing the same threat. At least six EUIBAs were impacted by this attack.

83 Constituents have also not actively shared timely information with CERT-EU on cybersecurity threats and vulnerabilities affecting them, despite the IIA[35] requiring them to do so. CERT-EU's Digital Forensics and Incident Response team has not received notifications of vulnerabilities or deficiencies in controls discovered outside

[34] Article 3.3 of the interinstitutional arrangement (IIA) signed on 20.12.2017.

[35] Article 3.2 of the interinstitutional arrangement (IIA).

the context of incidents it is actively investigating. Constituents do not proactively share relevant findings from internal or external security audits.

84 In addition, the IIA does not make it compulsory for EUIBAs to report significant changes in their IT environment to CERT-EU, and as a result constituents have not informed CERT-EU systematically of relevant changes. For example, EUIBAs do not always inform CERT-EU of any changes in their IP ranges (i.e. their infrastructure's list of internet addresses). CERT-EU needs updated IP ranges in order to, for example, perform scans when major vulnerabilities are discovered. Failure by EUIBAs to inform CERT-EU of such changes affects its ability to support them. Failure to notify CERT-EU also impacts its ability to monitor systems and leads to more work to correct inaccurate data in the monitoring tools. According to its management, CERT-EU sometimes discovers previously unknown IT infrastructure when dealing with an incident. Moreover, beyond specific cases, CERT-EU currently has no comprehensive overview of the IT systems and networks of the EUIBA community.

85 In the absence of any enforcement mechanism in the IIA, notifications from EUIBAs to CERT-EU –an essential element in creating a EUIBA community of cyber preparedness centred around CERT-EU – will remain unsystematic.

CERT-EU's resourcing is unstable and not commensurate with the current threat level

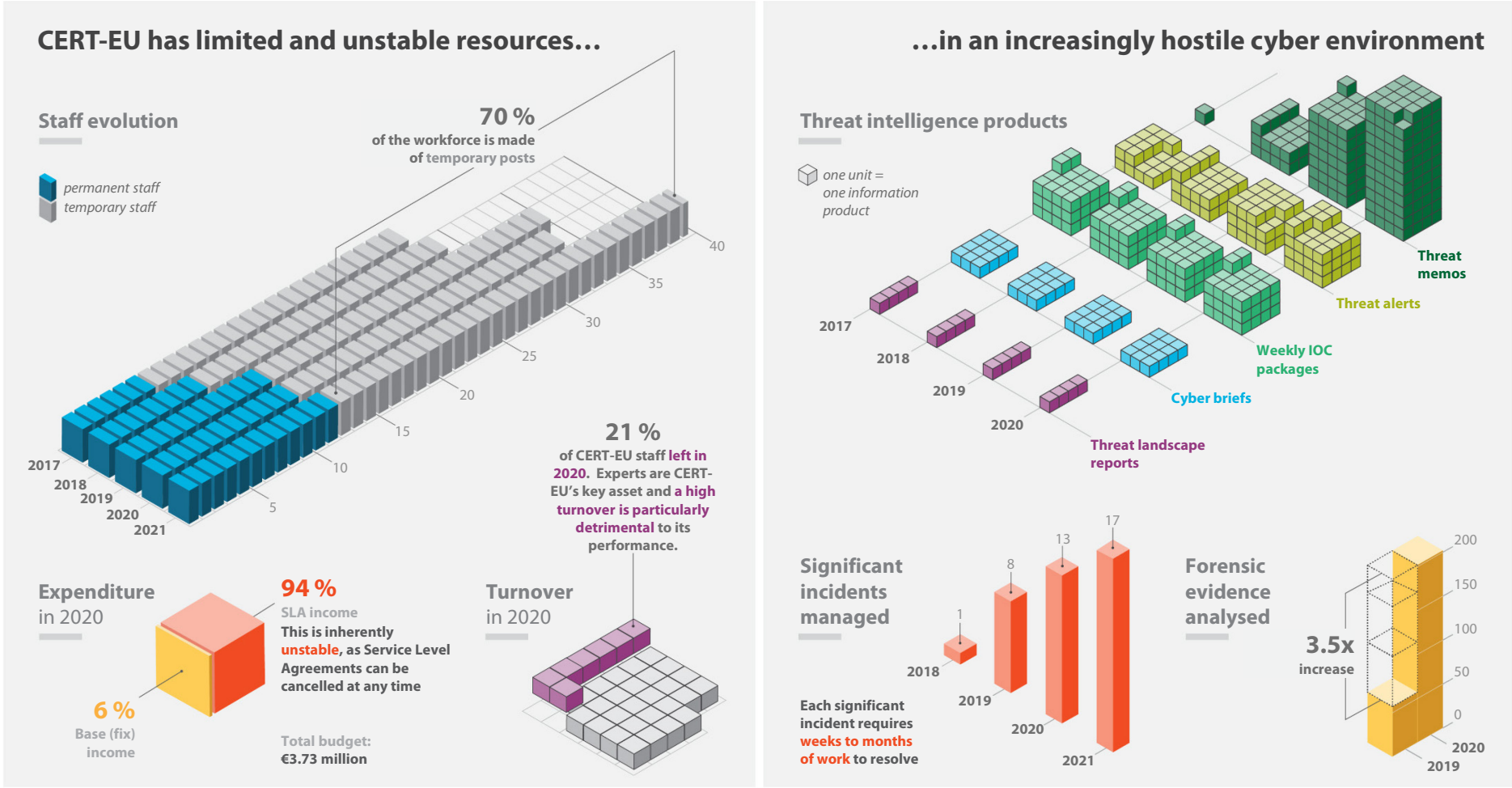
86 The IIA[36] states that "CERT-EU should be provided with sustainable funding and staffing, while ensuring value for money and an adequate core of permanent staff". CERT-EU's most important asset is its highly trained and specialised staff. ***Figure 10*** shows the change in staffing levels at CERT-EU from its inception in 2011 to the present day.

87 More than two thirds of CERT-EU staff members have temporary contracts. Their salary is not very competitive on the market for cybersecurity experts, and according to CERT-EU's management, it has become increasingly difficult to hire and retain them. When salaries are not attractive enough for senior candidates, CERT-EU must resort to hiring junior staff and invest time in training them. In addition, contracts have a maximum duration of six years, meaning CERT-EU has no option but to let contract staff go at the peak of their expertise. Staff turnover was particularly high in 2020: 21 % of staff left CERT-EU and not all replacements could be recruited. As regards previous years, 9 % of staff left in 2019 and 13 % in 2018.

---

[36] Recital 7 of the interinstitutional arrangement (IIA).

Figure 10 – CERT-EU's resources and challenges



Source: ECA, based on data from CERT-EU.

88 CERT-EU's management has underlined that, at present, CERT-EU's Digital Forensic and Incident Response Team is frequently overstretched, and its other teams cannot keep up with demand. As a result, CERT-EU has been forced to scale back activities. For example, CERT-EU does not currently carry out maturity assessments of its constituents, due to lack of resources. CERT-EU's "warnings on suspicious activity" service entered into production later than expected, again due to resource shortage. Furthermore, several constituents we interviewed commented on the long time they had to wait to access CERT-EU's services.

89 Resource constraints have so far forced CERT-EU to focus in particular on protecting conventional "on premise" IT infrastructure against major threats from (typically nation-state-supported) groups posing advanced persistent threats. But according to its management, the EUIBAs' expanded IT perimeter (now including the cloud, mobile devices and teleworking tools) needs enhanced monitoring and protection, and lower-level threats (such as cybercrime and ransomware) also require more attention.

90 The IIA does not provide for CERT-EU to have operational capability twenty-four hours a day, seven days a week. CERT-EU does not currently have the resources or the appropriate HR framework to operate beyond working hours on a permanent and structured basis, even though cybersecurity attacks do not adhere to these hours. For the EUIBAs themselves, only 35 of the 65 EUIBAs surveyed have an IT officer reachable outside working hours.

91 To finance CERT-EU's operations, the steering board in 2012 approved a service level agreement (SLA) model. All constituents receive core services for free and can pay to acquire extended services, by signing an SLA. CERT-EU's 2020 budget was €3 745 000 of which 6 % was funded from the EU Budget and 94 % from SLAs. However, constituents are very heterogeneous: some have mature IT security requirements while others have modest IT budgets and a very low level of cybersecurity maturity. Because of this, SLA discussions result in a combination of high security requirements for some EUIBAs and a relative lack of willingness or ability to contribute on the part of others.

92 Moreover, SLAs need to be renewed individually every year. As well as being an administrative burden, this creates cash flow problems, as CERT-EU does not have funds coming in at the same time from all SLAs. In addition, agencies can terminate SLAs at any moment. This risks starting a vicious circle where, due to lost revenue, CERT-EU has to scale back its services and cannot keep up with demand, in turn

prompting other EUIBAs to terminate their SLAs and move to private providers. In view of these considerations, the current funding model is not ideal for ensuring a stable and optimal level of service.

93 Faced with a rapidly evolving cybersecurity threat landscape (see paragraph ***06*** and ***80***), the CERT-EU steering board, at its meeting on 19 February 2020, endorsed a strategic proposal for CERT-EU to broaden its cybersecurity services and develop "full operational capabilities". The proposal was accompanied by an analysis of CERT-EU's staffing and funding needs. This analysis concluded that CERT-EU would require 14 additional permanent administrator posts, added incrementally over the 2021-2023 period. CERT-EU would then operate at full capacity from 2023 onwards. According to this proposal, in terms of funding, CERT-EU would need to increase its budget by €7.6 million over the 2021-2023 period, to reach €11.3 million by 2024.

94 However, despite endorsing the strategic proposal on the provision of the additional resources for CERT-EU, EUIBAs have not yet reached an agreement on practical modalities, firstly for the interim period of 2021-2023, and secondly for the long term after the future cybersecurity regulation enters into force (see paragraph ***12***).

Conclusions and recommendations

95 We conclude that the EU institutions, bodies and agencies (EUIBA) community has not achieved a level of cyber preparedness commensurate with the threats. Our work shows that EUIBAs have different levels of cybersecurity maturity, and since they are often interconnected with one another and with public and private organisations in Member States, one EUIBA's cybersecurity weaknesses can expose several other organisations to cyber threats.

96 We found that key cybersecurity good practices were not always implemented, including some essential controls. Sound cybersecurity governance is essential for the security of information and IT systems, but is not yet in place in some EUIBAs: IT security strategies and plans are in many cases lacking or are not endorsed by senior management, security policies are not always formalised, and risk assessments do not cover the entire IT environment. Cybersecurity spending is uneven with some EUIBAs clearly underspending compared to peers of similar size (see paragraphs ***21***-***33*** and ***37***-***38***).

97 Cyber awareness and training programmes are a key element in an effective cybersecurity framework. However, only 29 % of EUIBAs provide mandatory cybersecurity training for managers responsible for IT systems containing sensitive information, and the training offered is often informal. In the past five years, 55 % of EUIBAs have organised one or more simulated phishing campaigns (or similar exercises). These exercises are an important tool for training staff and raising awareness, but EUIBAs do not use them systematically (see paragraphs ***34***-***36***). In addition, not all EUIBAs have their cybersecurity regularly subject to independent assurance (see paragraphs ***39***-***44***).

98 CERT-EU is highly valued by the EUIBAs serves, but its capacity is overstretched. Its workload, in terms of threat intelligence and incident handling, has been growing rapidly since 2018. Significant cybersecurity incidents have increased more than tenfold. At the same time, EUIBAs do not always share timely information on significant incidents, vulnerabilities and important changes in their IT infrastructure. This hinders CERT-EU’s effectiveness, preventing it from alerting other EUIBAs potentially impacted and may result in significant incidents remaining undetected. In addition, CERT-EU’s resources are unstable and not presently commensurate with the current threat level or EUIBAs’ needs. A strategic proposal on the provision of the additional resources needed by CERT-EU was endorsed by its steering board in 2020, but constituents have not yet reached an agreement on the practical modalities for the

provision of such resources. As a result, CERT-EU staff cannot keep up with demand and are forced to scale back activities (see paragraphs *74*-*93*).

Recommendation 1 – Improve the cybersecurity preparedness of all EUIBAs through common binding rules and increased resources for CERT-EU

The Commission should include the following principles in its forthcoming proposal for a regulation on measures for a high common level of cybersecurity in all EUIBAs:

(a) Senior management should carry the responsibility for cybersecurity governance by endorsing cybersecurity strategies and key security policies and appointing an independent Chief Information Security Officer (or equivalent role).

(b) EUIBAs should have an IT security risk management framework covering the entirety of their IT infrastructure and carry out regular risk assessments.

(c) EUIBAs should provide systematic awareness training for all staff, including management.

(d) EUIBAs should ensure regular audits and tests of their cyber defences. The audits should also include the adequacy of the resources dedicated to cybersecurity.

(e) EUIBAs should report, without delay, to CERT-EU on significant cybersecurity incidents and relevant changes and vulnerabilities regarding their IT infrastructure;

(f) EUIBAs should increase and earmark in their budgets resources allocated to CERT-EU in line with the needs identified in the strategic proposal endorsed by its steering board;

(g) The regulation should include provisions for appointing an entity, representative of all EUIBAs, that has the appropriate mandate and means to monitor all EUIBAs compliance with the common cybersecurity rules and to issue guidance, recommendations and calls for actions.

Target implementation date: Q1 2023

99 EUIBAs have established mechanisms for cooperation in the area of cybersecurity, but we noted that potential synergies are not fully exploited. There is a formalised structure for information exchange, with actors and committees having complementary roles. However, participation in interinstitutional forums by smaller

EUIBAs is hindered by limited resources, and the representation of decentralised agencies and joint undertakings on the CERT-EU steering board is not optimal. We also found that EUIBAs do not systematically share among each other information on cybersecurity related projects, security assessments and other service contracts. This can lead to duplication of efforts and increased costs. We noted operational difficulties in the exchange of sensitive non-classified information, via encrypted email or in videoconference, due to lack of interoperability of IT solutions, inconsistent guidelines on their allowed use and the lack of common information markings and handling rules (see paragraphs ***45***-***63***).

Recommendation 2 – Advocate for further synergies among EUIBAs in selected areas

The Commission, in the context of the Interinstitutional Committee for the Digital Transformation, should promote the following actions among EUIBAs:

(a) adopt solutions for the interoperability of secure communication channels from encrypted email to videoconferencing, and advocate common markings and common handling rules for sensitive non-classified information;

(b) share systematically information on cybersecurity-related projects with a potential interinstitutional impact, security assessments carried out on software, and contracts in force with external suppliers and;

(c) define specifications for common procurement and framework contracts for cybersecurity services in which all EUIBAs can participate to foster economies of scale.

Target implementation date: Q4 2023

100 The European Union Agency for Cybersecurity (ENISA) and CERT-EU are the two main entities tasked with supporting EUIBAs on cybersecurity. However, due to resource constraints and priority being given to other areas, they have not been able to provide EUIBAs with all the support they need, particularly in relation to capacity building for EUIBAs that are less mature in cybersecurity (see paragraphs ***64***-***93***).

Recommendation 3 – Increase CERT-EU's and ENISA's focus on less mature EUIBAs

CERT-EU and ENISA should:

(a) identify priority areas where EUIBAs need most support, for example through maturity assessments;

(b) implement capacity-building actions, in line with their MoU.

Target implementation date: Q4 2022

This Report was adopted by Chamber III, headed by Mrs Bettina Jakobsen, Member of the Court of Auditors, in Luxembourg on 22 February 2022.

For the Court of Auditors

Klaus-Heiner Lehne
President

Annexes

Annex I – List of EUIBAs surveyed

Name of EUIBA	Type
European Parliament (EP)	Institution (art. 13(1) TEU)
Council of the European Union & European Council (GSC)	Institution (art. 13(1) TEU)
European Commission (EC)	Institution (art. 13(1) TEU)
Court of Justice of the European Union (CJEU)	Institution (art. 13(1) TEU)
European Central Bank (ECB)	Institution (art. 13(1) TEU)
European Court of Auditors (ECA)	Institution (art. 13(1) TEU)
European External Action Service (EEAS)	Body (art. 27(3) TEU)
European Economic and Social Committee (EESC) & European Committee of the Regions (CoR)[37]	Bodies (art 13(4) TEU)
European Investment Bank (EIB)	Body (art. 308 TFEU)
European Labour Authority (ELA)	Decentralised agency
European Union Agency for the Cooperation of Energy Regulators (ACER)	Decentralised agency
Office of the Body of the European Regulators for Electronic Communications (BEREC Office)	Decentralised agency
Community Plant Variety Office (CPVO)	Decentralised agency
European Agency for Safety and Health at Work (EU-OSHA)	Decentralised agency
European Border and Coast Guard Agency (Frontex/EBCGA)	Decentralised agency
European Union Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)	Decentralised agency
European Union Agency for Asylum (EUAA)	Decentralised agency
European Union Aviation Safety Agency (EASA)	Decentralised agency
European Banking Authority (EBA)	Decentralised agency
European Centre for Disease Prevention and Control (ECDC)	Decentralised agency
European Centre for the Development of Vocational Training (Cedefop)	Decentralised agency
European Chemicals Agency (ECHA)	Decentralised agency
European Environment Agency (EEA)	Decentralised agency
European Fisheries Control Agency (EFCA)	Decentralised agency

[37] EESC and CoR are counted as one EUIBA.

Name of EUIBA	Type
European Food Safety Authority (EFSA)	Decentralised agency
European Foundation for the Improvement of Living and Working Conditions (Eurofound)	Decentralised agency
European Union Agency for the Space Programme [to replace: European GNSS Agency - GSA] (EUSPA)	Decentralised agency
European Institute for Gender Equality (EIGE)	Decentralised agency
European Insurance and Occupational Pensions Authority (EIOPA)	Decentralised agency
European Maritime Safety Agency (EMSA)	Decentralised agency
European Medicines Agency (EMA)	Decentralised agency
European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)	Decentralised agency
European Union Agency for Cybersecurity (ENISA)	Decentralised agency
European Union Agency for Law Enforcement Training (CEPOL)	Decentralised agency
European Police Office (Europol)	Decentralised agency
European Union Agency for Railways (ERA)	Decentralised agency
The European Securities and Markets Authority (ESMA)	Decentralised agency
European Training Foundation (ETF)	Decentralised agency
European Union Agency for Fundamental Rights (FRA)	Decentralised agency
European Union Intellectual Property Office [known as OHIM until 23 March 2016] (EUIPO)	Decentralised agency
Single Resolution Board (SRB)	Decentralised agency
European Union Agency for Criminal Justice Cooperation (Eurojust)	Decentralised agency
Translation Centre for the Bodies of the European Union (CdT)	Decentralised agency
European Public Prosecutor's Office (EPPO)	Decentralised agency
European Institute of Innovation and Technology (EIT)	Body created under R&I
Single European Sky Air Traffic Management Research Joint Undertaking (SESAR)	Joint Undertaking under TFEU
Electronic Components and Systems for European Leadership Joint Undertaking (ECSEL)	Joint Undertaking under TFEU
Fuel Cells and Hydrogen 2 Joint Undertaking (FCH2)	Joint Undertaking under TFEU
Innovative Medicines Initiative 2 Joint Undertaking (IMI2)	Joint Undertaking under TFEU
Clean Sky 2 Joint Undertaking (Cleansky 2)	Joint Undertaking under TFEU
Bio-Based Industries Joint Undertaking JTI Joint Undertaking (BBI)	Joint Undertaking under TFEU
Shift2Rail Joint Technology Initiative JU (S2R)	Joint Undertaking under TFEU
European High Performance Computing Joint Undertaking (EuroHPC)	Joint Undertaking under TFEU
European Joint Undertaking for ITER - Fusion for Energy (F4E)	Joint Undertaking under TFEU

Name of EUIBA	Type
European Union Advisory Mission in Ukraine (EUAM Ukraine)	Civilian Mission (CSDP)
EU Border Advisory Mission Libya (EUBAM Libya)	Civilian Mission (CSDP)
EU Capacity Building Mission in Niger (EUCAP Sahel Niger)	Civilian Mission (CSDP)
EU Monitoring Mission in Georgia (EUMM Georgia)	Civilian Mission (CSDP)
EU Coordinating Office for Palestinian Police Support (EUPOL COPPS)	Civilian Mission (CSDP)
EU Advisory Mission Central African Republic (EUAM Central-African Republic)	Civilian Mission (CSDP)
EU Advisory Mission Iraq (EUAM Iraq)	Civilian Mission (CSDP)
EU Border Assistance Mission at the Rafah Crossing Point (EUBAM Rafah)	Civilian Mission (CSDP)
EU Capacity Building Mission in Mali (EUCAP Sahel Mali)	Civilian Mission (CSDP)
EU Capacity Building Mission in Somalia (EUCAP Somalia)	Civilian Mission (CSDP)
EU Rule of Law Mission in Kosovo (EULEX Kosovo)	Civilian Mission (CSDP)

Annex II – Additional information on the key interinstitutional committees

Interinstitutional Committee for the Digital Transformation (ICDT)

The ICDT is a forum to exchange information and foster cooperation in IT. It was established in May 2020, replacing the former Comité Interinstitutionnel de l'Informatique (CII). The ICDT is composed by the managers of IT departments in EUIBAs. The ICDT has a cybersecurity subgroup (ICDT CSSG) whose role is to promote cooperation between EUIBAs on cybersecurity, and serve as a forum for exchanging information.

The ICDT's decision-making power is limited to issues that do not affect "the way institutions deliver on their mission" and do not "impinge on governance within each institution". For decisions going beyond its remit, the ICDT may make recommendations to the college of secretaries-general of the EU institutions and bodies.

According to the ICDT's mandate, its members are representatives of each EU institution and body, and one representative designated by the EU agencies (ICTAC). The General Secretariat of the Council is currently chairing the ICDT.

ICDT cybersecurity subgroup (ICDT CSSG)

The ICDT CSSG, in its current configuration, was established in September 2020, replacing the former CII's standing security subgroup. Compared to its predecessor, the ICDT CSSG has a more structured, ambitious and results-oriented approach. Its activities are carried out by task forces (TF) that meet regularly and focus on key common issues:

- TF1 "Common standards, benchmarking and maturity"
- TF2 "Sharing platform methods and tool and contracts"
- TF3 "Cloud security"
- TF4 "Cyberskills talent development"
- TF5 "CyberAwareness"
- TF6 "Security of videoconferences"

According to the CSSG's mandate, its secretariat is responsible for regularly monitoring and reporting on the progress of the task forces' activities. It delivers regular reports to

the chair and deputy chair of the ICDT's cybersecurity subgroup, regularly collecting input from task-force coordinators. At the end of each year, the CSSG must also present a summary activity report.

The Commission is currently chairing the ICDT CSSG, with an ICTAC representative as deputy chair. Although the CSSG has no decision-making power, it can recommend decisions on relevant issues to the ICDT.

Agencies Network

The EU Agencies Network (EUAN) is an informal network set up by Heads of EU Agencies in 2012. EUAN currently comprises 48 decentralised EU agencies and Joint Undertakings. Its aim is to provide a platform for exchange and cooperation for the Network members on areas of common interest. The ICT Advisory Committee (ICTAC) is the subgroup of the EUAN in charge of promoting cooperation in the area of ICT, including in cybersecurity.

Information and Communications Technologies Advisory Committee (ICTAC)

The ICTAC promotes cooperation among the agencies and joint undertakings in the field of ICT. It aims to find viable and economical solutions to common problems, to exchange information and to adopt common positions, where appropriate. According to the ICTAC's terms of reference, general meetings bringing together all its members take place twice per year. There are also regular monthly meetings between ICTAC's representatives on CSSG Task Forces, ICTAC's representative on the CSSG and ICTAC's "Troika". The Troika consists of ICTAC's current, previous and future Chairpersons (each Chairperson serves for a period of one year). The Troika's role is to support the current Chairperson on all matters related to his/her role, including his/her substitution, if circumstances so require.

Acronyms and abbreviations

APT: Advanced Persistent Threat

CERT-EU: Computer Emergency Response Team of the EUIBAs

CIS: Communication and Information Systems

CISO: Chief Information Security Officer

CSA: Cybersecurity Act

CSIRT: Computer Security Incident Response Team

DG DIGIT: Directorate-General for Informatics

DG HR: Directorate General for Human Resources and Security

ENISA: European Union Agency for Cybersecurity

EUAN: European Union Agencies Network

EUIBAs: European Union Institutions, Bodies and Agencies

EU-LISA: European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

FTE: Full Time Equivalent

ICDT: Interinstitutional Committee for Digital Transformation

ICDT CSSG: Interinstitutional Committee for Digital Transformation Cyber Security Sub-Group

ICT: Information and Communications Technology

ICTAC: Information and Communications Technology Advisory Committee

IIA: Interinstitutional Agreement

ISACA: Information Systems Audit and Control Association

ITCB: Information Technology and Cybersecurity Board

MoU: Memorandum of Understanding

NIS: Network and Information Security

SLA: Service Level Agreement

Glossary

Advanced Persistent Threat: Attack in which an unauthorised user accesses a system or network in order to steal sensitive data, and remains there for an extended period of time.

Computer Emergency Response Team of the EUIBAs: Information exchange and incident response coordination hub whose clients ("constituents") are the EU institutions, bodies and agencies.

Cyber espionage: The act or practice of obtaining secrets and information from the internet, networks or individual computers without the permission and knowledge of the holder of the information.

Cyberspace: the global online environment in which people, software and services communicate through networks of computers and other connected devices.

Cybersecurity: Measures to protect IT networks and infrastructure, and the information they contain, from outside threat.

Penetration testing: Method for assessing the security of an IT system by attempting to breach its security safeguards with the tools and techniques typically used by adversaries.

Phishing: Sending emails purporting to originate from a trusted source to trick recipients into opening malicious links or sharing personal data.

Red teaming: Realistic simulation of cyber-attacks employing the element of surprise and techniques recently observed in the real world, focusing on specific objectives through multiple lines of attack.

Social engineering: In information security, psychological manipulation to trick people into doing something or sharing confidential information.

Replies of the Commission

https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=60922

Replies of the CERT-EU and ENISA

https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=60922

Timeline

https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=60922

COPYRIGHT

PDF	ISBN 978-92-847-7608-5	1977-5679	doi:10.2865/615675	QJ-AB-22-003-EN-N
HTML	ISBN 978-92-847-7588-0	1977-5679	doi:10.2865/294640	QJ-AB-22-003-EN-Q

The number of cyberattacks on EU institutions, bodies and agencies (EUIBAs) is increasing sharply. As EUIBAs are strongly interconnected, weaknesses in one can expose others to security threats. We examined whether the EUIBAs have adequate arrangements to protect themselves against cyber threats. We found that, overall, EUIBAs' level of preparedness is not commensurate with the threats, and that they have very different levels of cybersecurity maturity. We recommend that the Commission improve EUIBAs' preparedness by proposing the introduction of binding cybersecurity rules and an increase in resources for the Computer Emergency Response Team (CERT-EU). The Commission should also promote further synergies among EUIBAs, and CERT-EU and the European Union Agency for Cybersecurity should focus their support on less mature EUIBAs.

ECA special report pursuant to Article 287(4), second subparagraph, TFEU.

EUROPEAN COURT OF AUDITORS

Publications Office of the European Union

EUROPEAN COURT OF AUDITORS
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Enquiries: eca.europa.eu/en/Pages/ContactForm.aspx
Website: eca.europa.eu
Twitter: @EUAuditors