EUROPEAN
COMMISSION

Brussels, 22.3.2022
SWD(2022) 68 final

**COMMISSION STAFF WORKING DOCUMENT**

**SUMMARY OF THE IMPACT ANALYSIS**

***Accompanying the document***

**Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union**

{COM(2022) 122 final} - {SWD(2022) 67 final}

## 1. Introduction

In 2020, the number of significant incidents affecting Union institutions, bodies and agencies, authored by advanced persistent threat (APT) actors, surged. This is also reflected in the number of forensics images CERT-EU analysed in 2020, which more than tripled in comparison to 2019, while the number of significant incidents rose more than tenfold since 2018.

However, the cybersecurity capabilities and IT security spending in the Union institutions, bodies and agencies are in some cases strikingly unequal, resulting in a broad spectrum of cybersecurity maturity levels between the Union institutions, bodies and agencies. Additionally, the threat landscape analysis and IT security incident statistics show that cyber exposure for Union institutions, bodies and agencies will only intensify.

## 2. Objectives

The shortcomings identified, ultimately lead to an insufficient level of cyber resilience across the Union institutions, bodies and agencies, fragmented IT security resourcing and unbalanced IT security postures.

The aim of a legislative act would be to provide measures for a high common level of cybersecurity at the Union institutions, bodies and agencies. This would foster and assure that the cybersecurity maturity will keep pace with the accelerating digitalisation of Union institutions, bodies and agencies.

## 3. An Interinstitutional Cybersecurity Board and a cybersecurity framework

The proposal of an Interinstitutional Cybersecurity Board and a cybersecurity framework will introduce measures for a high common level of cybersecurity at the Union institutions, bodies and agencies enabling alignment around a framework that addresses the cybersecurity threats of all the Union institutions, bodies and agencies and will establish monitoring and reporting to an Interinstitutional Cybersecurity Board.

The proposal modernises CERT-EU's mission and tasks considering the changed and increased digitisation of the Union institutions, bodies and agencies in recent years and the evolving cybersecurity threat landscape.

There are no direct impact or budgetary consequences for the Member States or EU citizens.

The legal ground for the Regulation is Article 298 of the Treaty on the Functioning of the European Union which foresees that in carrying out their missions, the institutions, bodies, offices and agencies of the Union shall have the support of an open, efficient and independent European administration.

This proposal builds on the EU Security Union Strategy (COM(2020) 605 final) and the EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final).

## 4. Conclusion

An Interinstitutional Cybersecurity Board and a cybersecurity framework achieves most of the intended objectives in a relatively effective, efficient and coherent manner with other Union policies with the broadest stakeholders support. This solution that has been selected is the most viable option given the prevailing legal boundaries under which we act, also, a 'one-size fits all' approach would not respond to the heterogeneous maturity of the Union

institutions, bodies and agencies today and disparities in technological risk and complexity that they face.

EUROPEAN
COMMISSION

Brussels, 22.3.2022
SWD(2022) 67 final

# COMMISSION STAFF WORKING DOCUMENT

# IMPACT ANALYSIS

***Accompanying the document***

**Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union**

{COM(2022) 122 final} - {SWD(2022) 68 final}

**Table of Contents**

# 1. INTRODUCTION

## 1.1. Political context and legal framework

This proposal is provisioning for measures for a high common level of cybersecurity at the Union institutions, bodies and agencies[1]. It is in line with the Commission's priorities to make Europe fit for the digital age and to build a future-ready economy that works for the people. Cybersecurity is a priority in the Commission's response to the COVID-19 crisis.

This proposal builds on the EU Security Union Strategy (COM(2020) 605 final) and the EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final).

The proposal modernises CERT-EU's mission and tasks, taking account of the changed and increased digitisation of the Union institutions, bodies and agencies in recent years and the evolving cybersecurity threat landscape. Both developments have been further amplified since the onset of the COVID-19 crisis, while the number of cyber incidents continues to rise, with increasingly sophisticated attacks coming from a wide range of sources.

## 1.2. Consistency with existing policy provisions in the policy area

This proposal is aimed at increasing the resilience of the Union institutions, bodies and agencies against threats, while aligning with existing legislation:

- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. It also aligns with the proposal for a Directive (EU) XXXX/XXXX on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 [proposal NIS 2].
- Regulation (EU) 2019/881 on the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification (Cybersecurity Act).
- Proposal for a Regulation (EU) XXXX/XXXX on information security in the institutions, bodies, offices and agencies of the Union.
- Commission Recommendation of 23 June 2021 on building a Joint Cyber Unit.
- Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.

## 1.3. Stakeholder consultation

Substantial stakeholder consultation has been carried out including through repeated discussion of drafts in an interservice steering group, in the cybersecurity subgroup of the Interinstitutional Committee on Digital transformation of the Union institutions, bodies and agencies.

A written consultation of the Directors-General responsible for IT security of the Union institutions, bodies and agencies took place between 10/12/2021 and 10/01/2022.

[1] 'Union institutions, bodies and agencies' means the Union institutions, bodies, offices and agencies set up by, or on the basis of, the Treaty on European Union, the Treaty on the functioning of European Union or the Treaty establishing the European Atomic Energy Community.

On 25 June 2021, representatives of Member States in the Council and European Parliament and relevant stakeholders from the Union institutions, bodies and agencies participated in a workshop organised by the Commission to discuss the content of the future proposal for Regulation. Consultation of Union institutions and a Commission interservice consultation in February 2022, paved the way for adoption of the proposal by the European Commission in the first quarter of 2022.

## 2. PROBLEM DEFINITION AND EVOLUTION

The Union institutions, bodies and agencies' cyber threat landscape continues to evolve. Diverse threat actors carry out a large variety of malicious operations in the digital space, ranging from large-scale intrusions to narrowly targeted campaigns which lead to significant incidents.

The prominent motives are diverse but change little, amongst others:

- stealing valuable non-public information,
- making money,
- promoting a cause and
- manipulating public opinion.

Incidents undermine the digital infrastructure of the Union institutions, bodies and agencies and use the victims as a beachhead to compromise other targets, including public administrations in the Member States due to the intensive information flows between the Union institutions, bodies and agencies and the Member States. Meanwhile the tactics, techniques and procedures (TTPs) employed by threat actors keep evolving. The pace at which threat actors conduct their activity is higher than ever, while their campaigns are increasingly sophisticated and automated, targeting continuously expanding attack surfaces and quickly exploiting vulnerabilities. To mitigate these risks, a deep understanding of the most recent and prominent TTPs is necessary.

CERT-EU conducted an assessment of the principal cyber threats to which Union institutions, bodies and agencies are currently exposed or are likely to be exposed to in the foreseeable future[2].

Three categories of observations were used in the analysis:

1. Attempts to breach Union institutions, bodies and agencies' IT infrastructure (when successful, they are treated as incidents, in the other cases they are still recorded as detected attempts).
2. Threats detected in the proximity of Union institutions, bodies and agencies (e.g. in their related sectors, their stakeholder communities, or in the European Union).
3. Major threat trends observed globally.

Furthermore, the analysis considered major ongoing shifts affecting the way Union institutions, bodies and agencies manage and use their IT infrastructure and services. This includes:

[2] https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf

- Increased teleworking.
- Migration to the cloud.
- Increased outsourcing of IT services.

CERT-EU concludes that Union institutions, bodies and agencies are highly attractive targets. According to CERT-EU's observations, there are three main motives for attackers to go after the Union institutions, bodies and agencies:

1. Targeting sensitive information on specific matters: The primary objective of the adversary is to steal sensitive information from a specific Union institution, body and agency depending on its sector of activity (e.g. diplomacy, health, energy, transportation, finance, etc.).
2. Targeting the community of Union institutions, bodies and agencies: the Union institutions, bodies and agencies form a group of stakeholders in which substantial information flows take place under well established, mutual trust. The threat actor's goal is to compromise a member of the community whose cybersecurity maturity is lower than others for further exploitation
3. Targeting EU communities of interest: All Union institutions, bodies and agencies have close working relationships with an ecosystem of public and private organisations based in EU member states. APT groups can breach, abuse and blend in the flows within this ecosystem. Adversaries may compromise a Union institutions, bodies and agencies to facilitate attacks against various public or private organisations across the EU.

In 2020, the number of significant incidents affecting Union institutions, bodies and agencies, authored by advanced persistent threat (APT) actors, surged. This is also reflected in the number of forensics images CERT-EU analysed in 2020, which more than tripled in comparison to 2019, while the number of significant incidents rose more than tenfold since 2018.

The use of videoconferencing and other collaboration tools has surged in 2020 due to increased teleworking, and so have the incidents affecting Union institutions, bodies and agencies. Besides the classic flaws (e.g. misconfigurations, vulnerabilities, admin errors), the move to a digital infrastructure and software that is hosted and managed by a third party entails specific risks. Cloud environments are exposed to a number of new threats. Additionally, supply chain attacks, as demonstrated by the recent SolarWinds Orion campaign, one of the most sophisticated cyberattacks in history, can have devastating effects and their scope may never be fully grasped.

Complementary to the CERT-EU threat analysis, the Commission has carried out an evaluation of the IT security functioning of 20 Union institutions, bodies and agencies[3]. Different angles were taken in the analysis to provide a complementary insight into the strategic, tactical and operational levels of the cybersecurity implementation in the Union institutions, bodies and agencies. It gives insight in how formal the IT security practice is established, how effective the organisations build their IT security management capabilities

3 https://media.cert.europa.eu/static/Maturity_EUIBA/IT%20Security%20Maturity%20Analysis%20of%20the%20EU%20institutions,%20bodies%20and%20agencies.pdf

as well as how the Union institutions, bodies and agencies perform on a selected list of benchmarking technical security controls observed from an independent and external point of view.[4]

The evaluations are based on questionnaires to which these institutions, bodies and agencies responded, publicly available data and data provided directly by the Union institutions, bodies and agencies themselves and hence cannot be interpreted as an in-depth audit with evidence collection and an extended assessment with tailored stakeholder workshops and feedback sessions. It provides though sufficient insights in the current situation to make some key conclusions:

- IT security maturity, IT infrastructure size and IT security levels of capability vary substantially from organisation to organisation, confirming the heterogeneousness of the sampled population.
- Detection and response capabilities are better developed than IT security governance capabilities. Risk-based management is not an integral part of the IT security governance process.
- IT security frameworks (strategy, policy and rules base) are not covering all the main IT security domains, processes, roles and responsibilities, in particular business continuity management, compliance and audit, continuous improvement.
- Some prominent technical controls are less applied by the Union institutions, bodies and agencies.

### 2.1. Analysis and diagnosis

The conclusions that can be drawn from these reports are that information sharing on cyber threats, vulnerabilities and incidents is ad hoc, there is a no common cybersecurity framework or oversight and there is a fragmented approach of on baseline security requirements and implementation. Moreover, the cybersecurity capabilities and IT security spending in the Union institutions, bodies and agencies are in some cases still strikingly unequal, resulting in a broad spectrum of cybersecurity maturity levels between the Union institutions, bodies and agencies.

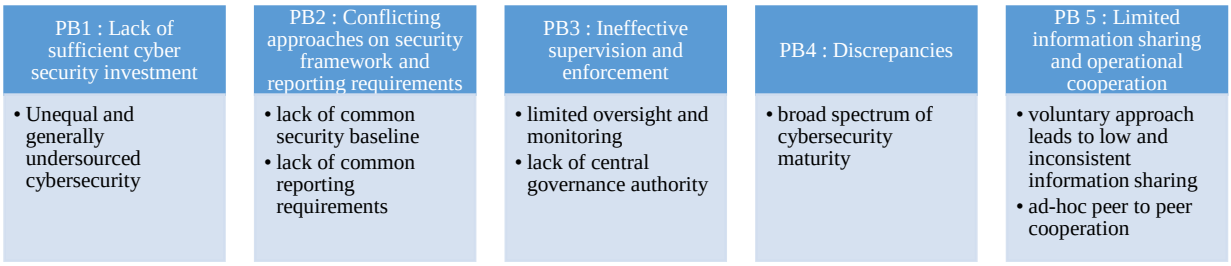
At the same time, digitisation and exposure to cyber risks across sectors will continue to increase. As a result, Union institutions, bodies and agencies are very unlikely to take all the measures necessary to achieve a high level of cyber resilience on a voluntary basis. This is especially true for those entities currently having low IT expenditure and support staff, but also for Union institutions, bodies and agencies that have better developed cybersecurity capabilities but whose level of cyber resilience remains low due to issues described in the IT Security Maturity Assessment. Additionally, the threat landscape analysis and IT security incident statistics show that Cybersecurity exposure for Union institutions, bodies and agencies will only intensify.

The aim of a legislative act would be to lay down measures for a high common level of cybersecurity at the Union institutions, bodies and agencies. This would foster and assure that

[4] A further analysis of the cybersecurity maturity of the Union institutions, bodies and agencies is forthcoming as a Special Report by the European Court of Auditors.

the IT Security Maturity Assessment will keep pace with the accelerating digitalisation of Union institutions, bodies and agencies.

The shortcomings that are synthesised around the five problem statements below, ultimately lead to an insufficient level of cyber resilience across the Union institutions, bodies and agencies, fragmented IT security resourcing and unbalanced IT security postures.




## 3. WHY SHOULD THE EU ACT?

As set out in the Communication 'Shaping Europe's digital future', it is crucial for Europe to reap all the benefits of the digital age and to strengthen its industry and innovation capacity, within safe and ethical boundaries. The European strategy for data sets out four pillars – data protection, fundamental rights, safety and cybersecurity – as essential prerequisites for a society empowered by the use of data.

The EU Security Union Strategy (COM(2020) 605 final) covers the period 2020-2025 and focuses on building capabilities and capacities to secure a future-proof security environment with the goal to offer a security dividend to protect everyone in the Union.

EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final) sets out how the EU will shield its people, businesses and institutions from cyber threats, and how it will advance international cooperation and lead in securing a global and open Internet.

The regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks arising from it.

The Union institutions, bodies and agencies shall take a front-runner position in increasing their cybersecurity resilience against threats, while aligning with existing Directives and Legislation.

### 3.1. Legal ground

The legal ground for the Regulation is Article 298 of the Treaty on the Functioning of the European Union which foresees that in carrying out their missions, the institutions, bodies, and agencies of the Union shall have the support of an open, efficient and independent European administration. In compliance with the Staff Regulations and the Conditions of Employment adopted on the basis of Article 336, the European Parliament and the Council, acting by means of regulations in accordance with the ordinary legislative procedure, shall establish provisions to that end.

Article 298 TFEU is the only legal basis that can serve.

Technology has provided new ways for Union institutions, bodies and agencies to work, interact with citizens and improve overall operations. A modern European administration manages to maintain its openness and efficiency through the use of technology. As technology continues to evolve, the cyber threat landscape evolves along with it. Union institutions, bodies and agencies have become highly attractive targets of sophisticated cyberattacks. Having appropriate and necessary cybersecurity practices in place ensures that Union institutions, bodies and agencies can accomplish their missions, knowing that their people, data and networks are secure.

The levels of IT security maturity vary substantially from administration to administration, confirming the heterogeneousness of the current Union IT security. This Regulation ensures that all Union institutions, bodies and agencies will implement a common baseline of security measures and cooperate among each other with as its goal the open and efficient functioning of the European administration.

### 3.2. Subsidiarity

Cybersecurity across the Union institutions, bodies and agencies cannot be effective if approached in a disparate manner through vertical silos. The IT infrastructure of Union institutions, bodies and agencies is often interconnected both directly and indirectly causing cybersecurity incidents in one administration to have a spill over effect on other administrations. The Regulation partly addressed this shortcoming, by setting a common baseline and ensuring the cooperation among Union institutions, bodies and agencies.

### 3.3. Proportionality

The rules proposed in this Regulation do not go beyond what is necessary to meet the specific objectives satisfactorily. The envisaged common baseline and cooperation requirements will enhance the level of protection of the Union institutions, bodies and agencies and is proportionate to the increasingly high risks faced by the Union institutions, bodies and agencies. The costs for ensuring a common baseline and cooperation amongst Union institutions, bodies and agencies would be small as compared to the potential damages caused by cybersecurity incidents that can spill over from one impacted administration to the other.

### 3.4. Choice of instrument

The choice of a Regulation, which is directly applicable, is considered the appropriate legal instrument to define and streamline the obligations imposed on Union institutions, bodies and agencies and to allow for targeted improvements.

## 4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

The following Specific Policy Objectives (SPO), describe the overarching goals of a possible EU intervention, reaching those goals would substantially improve the situation on the key problems identified:

- SPO1: Increasing the level of cyber resilience of the Union institutions, bodies and agencies is the main objective, by putting in place rules that ensure taking adequate

cybersecurity measures and building mature cybersecurity capabilities through adequate IT security expenditure.

- SPO2: Ensure that all Union institutions, bodies and agencies follow the same obligations based on the concept of risk management when it comes to security measures and report all incidents based on a uniform set of criteria and procedures. This is including but not limited to:
  - the de facto baseline security standard
  - the security and incident reporting requirements
  - the provisions for uniform reporting
- SPO3: Ensure that competent authorities monitor compliance with the regulation.
- SPO4: Ensure a comparable level of resources is allocated across Union institutions, bodies and agencies that would allow them to fulfil the core tasks laid out by the regulation, reducing inconsistencies in the cybersecurity resilience and maturity levels between Union institutions, bodies and agencies.
- SPO5: Ensure that essential information is exchanged between Union institutions, bodies and agencies by introducing clear obligations for competent authorities to share information and cooperate when it comes to cyber threats and incidents, including best practices and resources.

## 5. INFORMAL IMPACT ASSESSMENT AND HOW TO SOLVE THE PROBLEM

An internal impact assessment in the form of a Threat Landscape Analysis and an IT Security Maturity Assessment of the Union institutions, bodies and agencies were performed. Their findings point to an urgent need for improvements in the areas of IT security governance, risk management and the implementation of IT security controls. An overview can be found in the section 'problem definition and evolution'.

The Commission considered a number of policy options for common security rules for Union institutions, bodies and agencies:

- **Policy option 0 – maintaining the status quo**

  In this option the scope, requirements and obligations are maintained as they currently exist. Existing work of the Union institutions, bodies and agencies' technical teams and CERT-EU is continued without coordinated alignment on investments done by Union institutions, bodies and agencies and without the establishment of common measures on IT security. Rules on cybersecurity would continue to be set independently by the Union institutions, bodies and agencies internal IT security frameworks and provisions, as well as by existing or future regulatory initiatives[5]. However, there is no common approach to

[5]
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. The objective of the Directive is to strengthen the protection of critical infrastructures in the energy and transport sectors.

ensure cybersecurity throughout the Union institutions, bodies and agencies. The lack of overarching supervision and enforcement of security framework implementation leads to suboptimal and less effective security spending. This could have a negative impact or even enlarge the unequal security postures of the different Union institutions, bodies and agencies.

With CERT-EU providing services according to its budget, it is very likely that it would continue to be under resourced to fulfil its mandate and support the increasing demands of the Union institutions, bodies and agencies. Furthermore, the option is potentially ineffective in evening up the disparities in IT security spending between Union institutions, bodies and agencies, due to the voluntary nature and uncoordinated nature of the efforts.

The lack of enforced and structured information sharing negatively impacts the risk exposure of the Union institutions, bodies and agencies as a whole.

Although targeting a status quo should have a minimal impact on the IT security spending budget, it is likely that it is not possible to maintain the current risk exposure with the current security investment levels, due to the increasing number of threats and attacks in combination with suboptimal security spending.

There is no direct impact or budgetary consequences for the Member States or EU citizens.

- **Policy option 1 – non-legislative measures to align the Union institutions, bodies and agencies**

Introducing guidelines and recommendations on cybersecurity for Union institutions, bodies and agencies addressing the cybersecurity threats of all the Union institutions, bodies and agencies to be implemented on a voluntary basis, will provide a common starting point for increasing IT security maturity. This will provide guidance to Union institutions, bodies and agencies on how and where to improve their IT security posture. Those efforts would be complementary to the Union institutions', bodies' and agencies' internal IT security frameworks and provisions, as well as by existing or future regulatory initiatives[6]. However, there is no common approach to ensure cybersecurity throughout the Union institutions, bodies and agencies.

Although this option is a step in the right direction, it would not resolve the problems of the past that improvements are small and very slow. This option will not respond to the fast increase of the risk and threats that European Union institutions, bodies and agencies are facing.

With CERT-EU providing services according to its budget, it is very likely that it would continue to be under resourced to fulfil its mandate and support the increasing demands of the Union institutions, bodies and agencies. Furthermore, the option is potentially ineffective in evening up the disparities in IT security spending between Union

- COM (EU) (2020) 37 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission Work Programme 2020, Brussels, 29.1.2020.
- Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 of 24 September 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1.

6 See footnote 5.

institutions, bodies and agencies, due to the voluntary nature and uncoordinated nature of the efforts.

Equally as in options 0, the IT security spending is prone to be suboptimal and insufficient to face the increased level of incidents and threats.

There is no direct impact or budgetary consequences for the Member States or EU citizens and could be implemented under the legal provisions of the institutions.

- **Policy option 2 – Interinstitutional Cybersecurity Board and a cybersecurity framework**

This option introduces measures for a high common level of cybersecurity at the Union institutions, bodies and agencies enabling alignment around a framework that addresses the cybersecurity threats of all the Union institutions, bodies and agencies and establishing monitoring and reporting to an Interinstitutional Cybersecurity Board.

The reinforced role of CERT-EU with adequate resourcing and broader service offerings, will be able to support the Union institutions, bodies and agencies in achieving improved security levels. It would foster the CERT-EU's trust-relation to Union institutions, bodies and agencies and improve the overall information sharing.

An Interinstitutional Cybersecurity Board would implement the regulation through guidance documents and recommendations aimed at improving the Union institutions, bodies and agencies' security posture.

Despite the fact that this option would give rise to costs of both one-off and recurring nature, these costs of preventive measures are estimated to be surpassed by the savings due to efficiencies, and fewer incidents, especially major. In particular, when considering the operational and reputational costs of recovering of major incidents. Moreover, the establishment of a baseline provides for the minimum level of action to achieve an uplift in the overall security posture of Union institutions, bodies and agencies.

This option will neither result in fully binding common rules, nor will it provide common methodologies. In this sense Option 2 delivers somewhat suboptimal solutions to some of the key problems identified. But it is the only viable option within the existing budgetary and legal boundaries, given the legal autonomy of the Union institutions, bodies and agencies. Also, a 'one-size fits all' approach would not respond to the heterogeneous maturity of the Union institutions, bodies and agencies today and disparities in technological risk and complexity that they face.

This option has no direct impact or budgetary consequences for the Member States or EU citizens.

- **Policy option 3 – Far-reaching central authority and extensive common binding cybersecurity rules**

Introducing common cybersecurity legislation for Union institutions, bodies and agencies combined with an independent centralised cybersecurity body for supervision of Union institutions, bodies and agencies would be by far the fastest, most effective and efficient option to align and improve the IT security posture of the Union institutions, bodies and agencies. In addition, to a common cybersecurity legislation for Union institutions, bodies and agencies, a new authority would be established to supervise the implementation of the regulatory provisions empowered to take sanctioning decisions.

As with option 2, the role of CERT-EU would be transformed and receive more resourcing and a broader service offering would be available to the Union institutions, bodies and agencies. Strengthening CERT-EU's trust-relation with the Union institutions, bodies and agencies would improve the overall information sharing and joint situational oversight of the Union institutions, bodies and agencies security posture.

As the central authority would have the means to steer the Union institutions, bodies and agencies actively with mandatory common security rules, provided that adequate resources are available, it would pave the way to a faster overall maturity improvement and a common security baseline.

Despite the fact that this option would give rise to slightly higher costs than option 2, both one-off and recurring nature, the return on IT security investment would by far surpass that of option 2. Indeed, the savings due to economies of scale, efficiencies, the common framework and security baseline, effective information sharing and resourcing alignment between the Union institutions, bodies and agencies, would put them in a position to keep pace with the ever-increasing threat landscape.

This option would have no direct impact or budgetary consequences for the Member States or EU citizens. This policy option, however, would go beyond the boundaries of the legal base Article 298 TFEU and could infringe the autonomy of the Union institutions, and is hence not retained.

| **Problems (PB)** | **Specific policy objectives (SPO)** | **Policy options** | | | |
|---|---|---|---|---|---|
| | | **Policy option 0 – *maintaining the status quo*** | **Policy option 1 – *non-legislative measures to align the Union institutions, bodies and agencies*** | **Policy option 2 – *Interinstitutional Cybersecurity Board and a cybersecurity framework*** | **Policy option 3 – *Far-reaching central authority and extensive common binding cybersecurity rules*** |
| **PB.1:** Lack of sufficient cybersecurity investment by Union institutions, bodies and agencies | **SPO1**: Improve the IT security maturity level of the Union institutions, bodies and agencies to an adequate level. | Maintaining the scope, requirements and obligations. Continue existing work of the Union institutions, bodies and agencies technical teams and CERT-EU without coordinated alignment on investments of Union institutions, bodies and agencies. | Maintaining the scope, requirements and obligation, while providing specific guidance via the existing CERT-EU operational setup. | Bring additional CERT-EU services under the scope of their mandate.<br>Require Union institutions, bodies and agencies to take the necessary provisions to ensure they have the technical, financial and human resources in place to implement adequate cybersecurity in their organisations and in particular for the shared funding of CERT-EU services and the Interinstitutional Cybersecurity Board. | Bring additional CERT-EU services under the scope of their mandate and provide CERT-EU with a broader and more robust legal base provisioning for own budget and resourcing.<br>Require and enforce Union institutions, bodies and agencies to take the necessary provisions to ensure they have the technical, financial and human resources in place to implement adequate cybersecurity in their organisations and in particular for the shared funding of CERT-EU services and the governance body. |
| **PB.2:** Conflicting approaches on security framework and reporting requirements | **SPO2:** Ensure that all Union institutions, bodies and agencies must follow the same obligations based on the concept of risk management when it comes to security measures and must report all incidents based on a uniform set of criteria and procedures. | Maintaining the scope, requirements and obligations. Continue existing work of the Union institutions, bodies and agencies technical teams and CERT-EU without coordinated alignment on common security frameworks and common reporting of Union institutions, bodies and agencies. | Guidelines on security and incident reporting requirements | Align IT security and incident reporting requirements and measures as part of strong guidelines proposed by CERT-EU and issued by the Interinstitutional Cybersecurity Board. | Introduce and inforce uniform and explicit security and incident reporting requirements, potentially directly applicable to the relevant Union institutions, bodies and agencies.<br>Introduce more explicit reporting obligations concerning incidents reporting.- |

| **Problems (PB)** | **Specific policy objectives (SPO)** | **Policy options** | | | |
|---|---|---|---|---|---|
| | | **Policy option 0 – *maintaining the status quo*** | **Policy option 1 – *non-legislative measures to align the Union institutions, bodies and agencies*** | **Policy option 2 – *Interinstitutional Cybersecurity Board and a cybersecurity framework*** | **Policy option 3 – *Far-reaching central authority and extensive common binding cybersecurity rules*** |
| **PB.3.** Ineffective supervision & enforcement | **SPO3:** Ensure that competent authorities enforce the rules laid down by the legal instrument more effectively through aligned supervisory and enforcement measures | Maintaining the scope, requirements and obligations. No supervision nor enforcement of security framework implementation. | Guideline on supervision and enforcement | Establish an Interinstitutional Cybersecurity Board to implement the regulation through guidance documents and recommendations that is advised by CERT-EU.<br>Establish a voluntary peer-review system. | Establish principles, as well as a more granular list of minimum requirements, for supervisory measures and enforcement.<br>Establish general conditions for application of administrative fines and a minim level thereof.<br>Establish a peer-review system, including on the implementation of supervisory measures and enforcement.<br>Introducing liability rules for natural persons responsible for or acting as a representative of the legal person. |
| **PB.4**. Discrepancies in Union institutions, bodies and agencies. | **SPO4:** Ensure a comparable level of resources across Union institutions, bodies and agencies allocated to competent authorities that would allow them to fulfil the core tasks laid out by the regulation. | Maintaining the scope, requirements and obligations. Ad-hoc funding and incident based improvement and security enforcement. | Incentivise Union institutions, bodies and agencies via the common working groups and other advisory governance bodies, and through peer pressure to adequately fund their cybersecurity.<br>Increase the cybersecurity awareness reach out to Union institutions, bodies and agencies | Require Union institutions, bodies and agencies to take the necessary measures to ensure they have the technical, financial and human resources in place to implement adequate cybersecurity in their organisations and in particular for the shared funding of CERT-EU services and the Interinstitutional Cybersecurity Board. | Set up a peer-review mechanism to assess, among others, the capabilities of the Union institutions, bodies and agencies. |

| **Problems (PB)** | **Specific policy objectives (SPO)** | **Policy options** | | | |
|---|---|---|---|---|---|
| | | **Policy option 0 – *maintaining the status quo*** | **Policy option 1 – *non-legislative measures to align the Union institutions, bodies and agencies*** | **Policy option 2 – *Interinstitutional Cybersecurity Board and a cybersecurity framework*** | **Policy option 3 – *Far-reaching central authority and extensive common binding cybersecurity rules*** |
| **PB.5:** Limited information sharing and operational cooperation. | **SPO5:** Ensure that essential information is exchanged between Union institutions, bodies and agencies by introducing clear obligations for competent authorities to share information and cooperate when it comes to cyber threats and incidents | Continue working in the setup and legal base currently provisioned for the CERT-EU operations. | Develop additional Standard Operational procedures to improve cooperation and alignment between Union institutions, bodies and agencies. | Mandate and incentivise cybersecurity information sharing with CERT-EU and the Interinstitutional Cybersecurity Board. | Set up specific mandatory mutual assistance and cooperation mechanisms when cross-border elements are involved.<br>Incentivise voluntary information sharing with CERT-EU and the governance authority.<br>Adding the role of cybersecurity observatory to monitor and perform audits of cybersecurity maturity and IT security postures.<br>Introducing annual/biennial/regular reports on the state of cybersecurity in the governance authority. |

## 6. CONCLUSION

**Option 2** achieves most of the intended objectives in a manner that is relatively effective, efficient and coherent with other Union policies with the broadest stakeholders support.

Although this option does not deliver full solutions to the key problems identified in comparison with Option 3, it is the only viable option, given the prevailing legal boundaries under which we act.