CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Need for Speed — Challenges in Security Accreditation

Jan Wünsche, Sungbaek Cho & Philippe Zotz[1]
NATO CCDCOE

[1] As of mid-2021, Philippe Zotz assumed a role as cyber defence expert at the Luxembourg Armed Forces.

Tallinn 2021

CCDCOE

The CCDCOE is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 29 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, governmental, academic and industrial backgrounds.

The CCDCOE is home to the *Tallinn Manual*, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise, Locked Shields. Every spring, the Centre hosts the International Conference on Cyber Conflict, CyCon, in Tallinn, a unique event bringing together key experts and decision-makers of the global cyber defence community. The Centre is also responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by the following NATO nations and partners of the Alliance: Austria, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

Cover

The cover shows a word cloud where the size of each word represents the frequency of use of the word in the free text answers to the questionnaire that was part of the study reported in this paper.

Acknowledgements

The authors would like to sincerely thank all the respondents to the questionnaire, without whose support and collaboration this project would not have been possible. A huge thank you also goes to Dr Jonas Hallberg and Johan Bengtsson of the Swedish Defence Research Institute (FOI), Dr Frank Micevski Scharf of the NATO Office of Security and our CCDCOE colleague Major Erwin Orye for support and inspiration, Dr Lauri Lindström and Henrik Beckvard for reviewing our drafts and providing invaluable comments, and to Commander Michael Widmann for allowing us to pursue this project and supporting us throughout.

Table of Contents

Executive Summary

Security accreditation is an important part of the measures taken by states and international organisations to ensure adequate cybersecurity in national security systems. This paper reports the findings from a survey of CCDCOE member nations, NATO and EU organisations to investigate possible shortcomings of current security accreditation practices for national security systems. The survey was conducted from the perspective of the security accreditation authorities (SAAs). Another aim of the survey was to identify projects and initiatives to address such issues. A description of the projects and initiatives identified is given in Annex B.

An analysis of the responses shows that nations and international organisations experience similar challenges with their security accreditation processes even though there are differences in the organisation and performance of accreditation activities.

The issues raised were varied, with the most commonly noted one being that the process is too time-consuming. The times reported for accrediting a national security system vary from just under one month to 18 months. These times are clearly too long in many cases, especially if they apply to re-accreditation in an agile development environment. Costs and resource requirements and a lack of staff are also seen as challenges.

The causes of the issues reported by SAAs can be said to fall into five broad categories: funding, competence, changing technology, clients and requirements. Both a lack of funding and competent personnel affects the SAA's ability to manage the workload. Job market competition with private industry is raised as a particular concern. The rapidly changing technology puts additional strain on the SAAs in keeping knowledge and requirements current and also increases the rate of new and changed systems in need of accreditation. The clients are the operational authorities or business owners who wish to have their systems accredited. A lack of awareness and focus on security from the clients will impede the security accreditation process. Finally, complex and sometimes unclear or poorly understood requirements also hamper the ability to efficiently achieve compliance.

Based on the analysis, we make some policy recommendations that will address some of the challenges. The first is to define security requirements more clearly. One option is to define specific requirements for different types of systems rather than just applying generic security principles. The next is to require that vendors clearly specify the systems they deliver in a standardised manner. Third, we recommend that nations and organisations work to secure a sufficient number of competent accreditors and look into the possibility of outsourcing part of the workload. The fourth recommendation is to define the role of the client in the security accreditation process to make expectations from the SAA clear. The fifth is to establish an efficient and effective accreditation continuity strategy to manage the challenges of maintaining the security of systems that are updated more frequently than before. The sixth is to use automated validation and verification tools to make re-accreditation more efficient. Finally, we recommend that nations and organisations increase their efforts to share information on security measures and vulnerabilities. Such exchanges are becoming more important as information technologies change rapidly and it will be more difficult for a single nation to tackle all security issues within an appropriate time frame.

1. Introduction

Many nations and international organisations such as NATO and the EU require the formal approval of systems that process classified information. The process of arriving at such an approval, the *security accreditation* process, is the subject of this study. What is understood by security accreditation in NATO is detailed in the relevant policies [1] and directives [2] [3]. For this study, and in line with NATO's view, we define security accreditation as a formal process to determine that an adequate level of protection has been achieved, and is being maintained, for a specific Communication and Information System (CIS) for a particular use. This is distinct from the evaluation and approval of individual hardware or software products or the certification of security products such as the approval of crypto devices, although such certification may be part of the accreditation process.[2] We also restrict ourselves to the security accreditation of national security systems, i.e. mainly CIS processing classified information, but in some cases including systems that are otherwise significant for national security and therefore covered by the same regulations. These are mainly CIS that is owned and operated by the military or other government organisations but may, depending on national legislation, also be classified systems operated by private enterprises. A more detailed description of the process in NATO and how it relates to certification can be found in [4].

The security accreditation processes are usually strictly regulated and systems need to meet certain criteria in areas such as encryption, emission security, user authentication and separation from other systems to be accredited. The processes are often resource-intensive and take a significant amount of time to complete. As more and more information processing moves to the digital realm and the needs change ever more rapidly, there is a drive to be able to accredit and deploy national security systems quickly and efficiently while maintaining the necessary security. This paper reports the findings from a survey of CCDCOE member nations, NATO and EU organisations to investigate possible shortcomings of current security accreditation practices for national security systems.

In NATO, security accreditation is the subject of a number of policy and guidance documents setting out the requirements for accrediting systems to be used within NATO, and setting the minimum standards for member nations and partners when processing NATO classified information. The most important of these are the enclosure on CIS Security in the NATO Security Policy [1], the Primary Directive on CIS Security [2] and the Management Directive on CIS Security [3].

Similar to the NATO procedures, in the EU the Council Security Regulations [5] play a similar role and set out rules similar to those in NATO. These rules are also to be respected by member states when accrediting systems processing EU classified information.

Nations each have their own schemes for accreditation sometimes modelled on the NATO or EU schemes, but usually with differences due to historical or national legal reasons. Some respondents to the survey highlighted a risk-based approach when describing their security accreditation process, while others focused more on compliance with security requirements fixed in regulations. Other differences concern the division of tasks and duties between those involved in the process; for example, the accreditor and business owner roles in accepting residual risk. Despite the differences, it is fair to say that the schemes seem to be broadly similar both in aim and execution.

There are typically two main players involved. The first is *the client* – the operational authorities or business owners that wish to have their systems that process classified information authorised for use.

---

[2] In the US the NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems* [14], now superseded, referred to the process as the Security Certification and Accreditation process, using the term accreditation for the official management decision and certification for the assessment of the security controls in support of the accreditation.

The second, and the one we targeted in the survey, is *the SAA*, the body tasked to make a security assessment and produce an accreditation recommendation or decision. How tasks within the accreditation process are divided between these bodies varies from nation to nation, but the client will typically be tasked to produce, collect and present evidence showing the security measures taken, and the accreditation body will examine this evidence and may also perform a further evaluation of the security controls. The main object of this process is to establish an adequate level of assurance that the controls will be effective.

While it is possible to have one authority making all the accreditation decisions in a nation, it is not uncommon to split the responsibility into a civilian and a military part or to delegate the authority for the military to a body within the defence ministry or the armed forces. Another option is to allow agencies to accredit their own systems, leaving the central authority responsible for regulation and oversight. Even in that case, accreditation tasks will typically be performed by a security authority (the SAA) separate from the part of the organisation responsible for procuring or developing the system (the client) to maintain a degree of independence in the accreditation decision.

Most respondents mentioned some level of international cooperation regarding security accreditation. Nations and international organisations such as NATO and the EU enter into security agreements setting out rules for sharing and handling of classified information. These agreements will usually not cover the approval of CIS for handling classified information in any detail. The agreements will usually prescribe that a recipient should protect the classified information according to one of three principles:

1. To a standard no less than given to the recipients own classified information of the corresponding classification level; [6]
2. To a standard equivalent to what is required by the originator; [7] or
3. To some agreed common standard. [8]

In the last case, the standard may be an existing common standard, as in the case of the multinational agreement between EU member states [9], or it may be agreed upon in subsequent technical arrangements.

The only common more detailed prescription is that electronic transmission of classified information should be encrypted using cryptographic systems approved by specific authorities. Technical arrangements, either in general or for specific projects, may specify more detailed requirements concerning security accreditation of CIS for classified information exchanged between states or international organisations.

The security agreements will in general mean that the states will have to trust the security accreditation performed by the states receiving their classified information. There may be clauses allowing for inspections or audits although, in general, a great deal of trust is placed in the other party.

In the survey, many respondents noted accreditation of systems operated together with other nations and interconnection between systems from different states or international organisations as the area of international cooperation. When such systems are set up, it is customary for the participating nations to provide statements of compliance, indicating the adherence of their part of the system to any agreed common security requirements, and that the system has been approved by the competent authorities. These statements will be endorsed by a joint security accreditation board establishing the security accreditation of the system as a whole.

It is often said that the laborious and time-consuming nature of security accreditation processes mandated by these rules and agreements cause delays in fielding CIS needed for operations. The use of agile processes and the incremental deployment of functionality, which is quickly becoming the norm even for military CIS, exacerbates these challenges. Every change to a system will potentially affect its security properties, and measures need to be taken to ensure that security is not weakened. If updates with new functionality are expected to be rolled out perhaps as often as every other week, it is clear that a security accreditation process that may take months is not practical. At the same time, current

practices are not guaranteed to find all vulnerabilities, and even more effective security reviews are sometimes called for. The subject of security accreditation causing delays in fielding CIS and what to do about it has long been discussed but there is little publicly available research into the problem. Some research that we have found is described briefly here.

In a project proposal, Richards [10] looks at the process of determining that a software system's risk is acceptable and concludes that the use of human evaluators is a limiting factor of these processes within the US DoD, also observing that vague or poorly written certification requirements lead to inconsistencies. The project suggested was to explore how this could be alleviated through automated evaluation of software assurance evidence.

Buszta [11] describes the challenges in certification and accreditation under the US Federal Information Security Management Act (FISMA), breaking them down to matters relating to funding, governance and interpretation.

Wrona, Scharf and Jarosz [4] explore the possibility of automation, not only of the actual testing but also of collecting evidence and checking compliance through the use of smart contracts. The approach is promising, particularly when it comes to the efficient and formal management of the vast amounts of verification work and record-keeping needed during the security accreditation process.

Agile development practices such as Scrum[3] and DevOps[4] are frequently employed to speed up the development cycle and to facilitate frequent updates and enhancement of software systems. While the overall development speed may be enhanced by using such methods, providing security compliance evidence to, for example, maintain security accreditation status will influence the process and may make it difficult to maintain agility. The US Navy has launched an initiative dubbed 'Compile to Combat in 24 hours', intended to make use of agile processes and make the security accreditation times match [12]. Moyón et al. [13] provide a systematic survey of the literature on integrating security standard requirements into agile processes and summarise the key findings. They conclude that current contributions do not yet provide practical strategies on how to overcome these challenges and that there is a lack of experience reports describing challenges and success stories.

This paper seeks to investigate the challenges SAAs face in getting CIS security accredited efficiently and effectively, and to make recommendations on how to begin to overcome some of those challenges. We also set out to collect information about current projects and initiatives aiming to address those issues.

[3] *Scrum* is an agile process for incrementally building software in a complex environment. It is designed for small teams and breaks work into goals that can be achieved in short iterations called *sprints*, typically two weeks long. [15]

[4] *DevOps* is a set of practices combining software development and IT operations. It aims to shorten the development life cycle and to provide continuous integration and deployment. [16]

2. Research Approach

We hypothesised that the time to reach a security accreditation decision after a system has been developed or integrated is often longer than desirable for both the clients and the SAAs. We also expected nations and international organisations to be actively looking for solutions to this challenge, possibly engaging in projects exploring new ways of doing the accreditation.

To verify the hypothesis and to find what other challenges nations have identified in their security accreditation processes we conducted a survey. A questionnaire was sent out through the representatives in the CCDCOE steering committee to all of the Centre's member nations and to the nations currently in the process of joining the Centre, for distribution to their respective SAAs. The questionnaire was also sent to the NATO Office of Security and the SAAs of three EU institutions. Some 18 responses were obtained, representing NATO, two EU institutions and authorities in 13 nations: Belgium, Canada, Denmark, Estonia, Finland, Germany, Hungary, Japan, Republic of Korea, Poland, Slovenia, Sweden and Switzerland.

The questionnaire was divided into two parts. Part A investigated the processes used for security accreditation and what shortfalls and problems the SAAs found with them. It also asked in general if the nation or organisation had any projects or initiatives addressing those challenges (see Annex A). There are substantial differences between the respondents' regulatory frameworks, division of responsibilities, processes, procedures and terminology, and so one has to be aware that the responses are not always directly comparable and must be interpreted within the correct context.

The fact that the questions were posed mainly to the SAAs rather than to the clients of the process will undoubtedly have influenced the types of issues raised and how they are prioritised. Even though the SAAs are not directly affected by delays in the process, it was our assumption they would be well-positioned to observe those effects and to be able to balance them against the security implications of alternative approaches. Responses concerning problems identified at the client-side of the process also have to be interpreted in this context.

Many aspects of the security accreditation of national security systems are confidential. Revealing details about current processes, the organisations that perform them or potential weaknesses may give an adversary an edge in analysing and attacking the systems that are the subject of the security accreditation. This translates, understandably, into a certain caution in sharing details about the processes in a survey like this. We know that for this reason some nations have chosen not to respond at all and it is evident that some have chosen not to answer all the questions. This may skew the results since some weaknesses in current practices may have been consciously withheld. From our experience, however, we believe that the general types of issues have, at least to a large extent, been covered in the responses and that what is missing is mainly the details of specific practices. Nevertheless, we believe that there is great value in performing a survey where the findings can be distributed openly within the community. Going further, the findings and recommendations of this study could be verified by more in-depth research also using classified information.

Part B) of the questionnaire asked for details on any projects or initiatives to investigate or develop approaches to security accreditation to address some of the identified issues with the current practice (see Annex B). Considering the sensitive nature of some of these projects, respondent engagement was understandably lower for this part. This should not, however, be taken as an indication that the respondents are not working to find solutions to some of the challenges.

3. Findings

In this chapter, the findings regarding issues in security accreditation drawn from some of the responses to Part A of the questionnaire are summarised. Respondents were asked to pick the three most important concerns in security accreditation and describe them and the reasons they could see behind them.

The categories available for selection were*: Too time-consuming, Too expensive/resource-intensive, Lack of staff, Lack of certified components, Difficulty accessing proprietary/confidential information, Does not reach adequate assurance, Does not address all threats/vulnerabilities, Results not consistent, Not independent,* and *Other*.

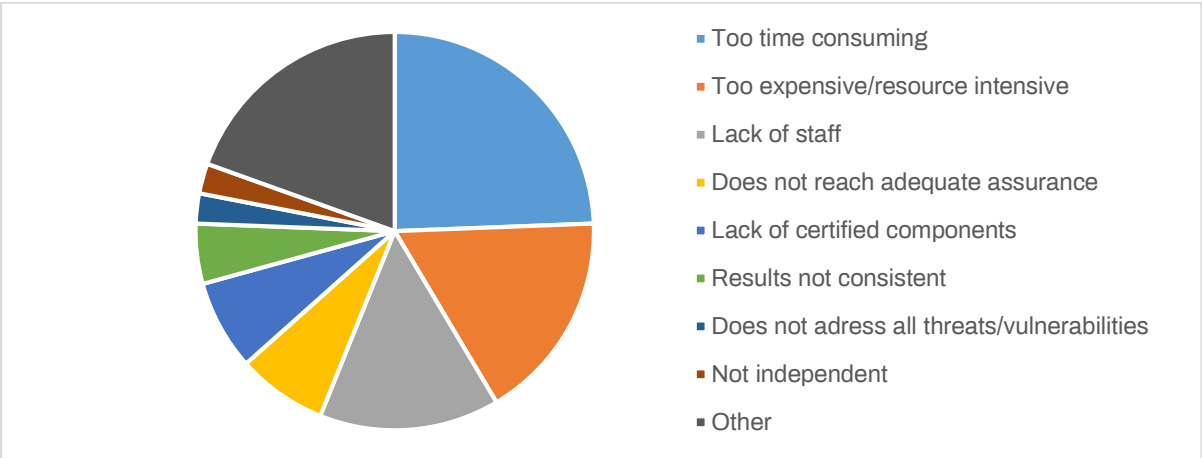

Figure 1. The overall issues reported as one of the three most important

A visualisation of responses given is provided in Figure 1. It shows that the aspect of taking too much time was described as an important concern by a large number of respondents. This overview also shows that costs and resource requirements and a lack of staff are also seen as challenges. The high number of answers that fall under 'Other' indicates that the issues are not purely homogeneous but that, depending on the country or organisation, challenges may be present which were not covered by the predefined categories of the questionnaire.

Figure 2 represents the concern in accreditation described as the most important, thus visualising the primary concern of the respondents. The most common reply addressed issues surrounding time ('Too time-consuming'), especially stating that the accreditation process is too time-consuming, with varying reasons. Some respondents indicated, that the second most commonly indicated issue, the 'Lack of staff' is partially or in some cases directly related to the issue of time, as will be discussed below.

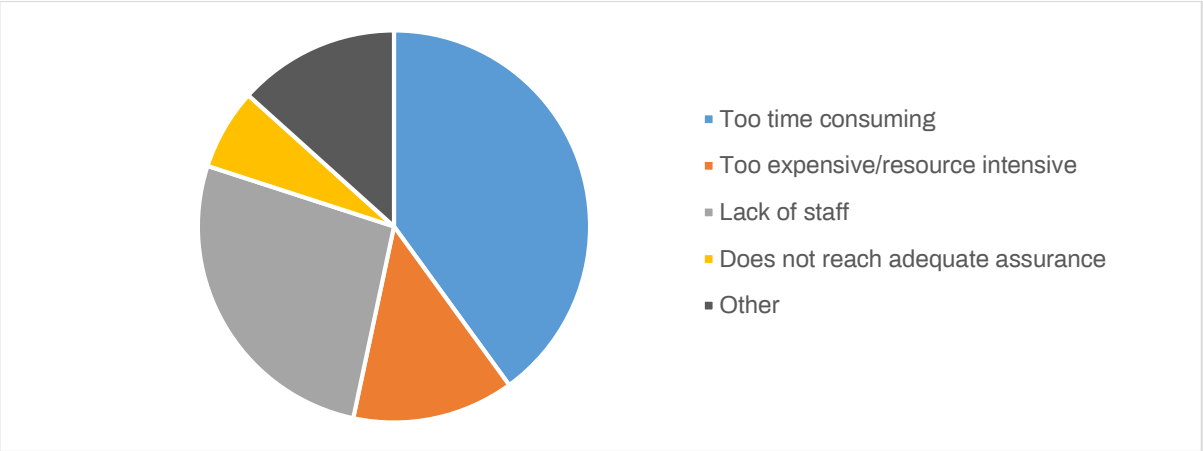

Figure 2. The issues reported as most important

Issues of cost and resource intensity were also mentioned including, for example, the cost of TEMPEST components [5] that are not available as commercial off-the-shelf (COTS) products and the high administrative effort behind the accreditation process. Issues falling under the category 'Does not reach adequate assurance' deal, for example, with questions of how to verify the effectiveness and completeness of the security measures and results of the accreditation framework. The category 'Other', making up a large portion of the issues, is comprised of many individual issues such as challenges of keeping up with emerging threats, a lack of certified components, discrepancies in the interpretation of rules and regulations for security requirements, the multitude of security requirements for bilateral or international systems, upfront communication and collaboration with vendors.

Several respondents pointed out that it is hard to know how long the accreditation process will take since it is dependent on the kind of system and many factors such as size, context, complexity and early involvement of security authorities have to be considered. When asked to estimate the time for security accreditation of a system or network for storing and transmitting or sharing classified documents, the estimations from nations and organisations varied between 27 days and 18 months. For the estimation of accreditation time for a military command and control system including radio transmission, the estimates ranged from one to 12 months. Respondents were also asked to estimate the time for security accreditation for mobile devices such as laptops and phones, to which the replies ranged from one to 36 months. Although these numbers are an illustration of the time that can be considered for accreditation processes, many respondents made it clear that these are general estimates and that there can be significant variations from case to case. These deviations can be attributed to several factors such as the extent to which certified components are used or the availability and quality of documentation provided. In addition, there are national or organisation-specific time requirements for certain processes within their accreditation. While some countries and organisations specify low periods of exact days, sometimes one to two months, others reported comparatively long periods ranging from one to several years.

Through several responses, however, it is clear that many respondents agree that there are aspects of security accreditation that are simply lengthy. These are by their very nature time-consuming and can only be speeded up with great difficulty, if at all, and are inevitable components of security accreditation, such as creating, editing and reviewing numerous documents and the testing and evaluation processes.

[5] *TEMPEST* equipment are computers, other electronic devices and enclosures designed to eliminate or reduce emission of electromagnetic waves that may reveal information being processed (*compromising emanations*).

In the remainder of this section, the issues raised by the respondents are grouped into the interconnected categories *Funding, Competence, Changing Technology, Client* and *Requirements*. The categories represent an identification of root causes for the issues based on the indications by the respondents in their descriptions and our analysis. Quotes used in the following sections are those of the respondents to the questionnaire, with only some identifiers removed that would otherwise compromise the anonymity of the respondents and typographical errors corrected.

3.1 Funding

Insufficient funding, meaning issues associated with budget or high costs of development and implementation of national security systems, seem to harm the accreditation process. In some situations, additional security requirements have to be added that were initially not foreseen in the financing plan for a system. One respondent mentioned the state's procurement and budgeting system, which can be slow and inflexible, as an additional hurdle.

> *"From the side of the [client], the budget doesn't provide financial resources to ensure the sustainability of CIS security."*

In some cases, the recurring costs of compliance with security regulations are not included in the budget, and this is particularly relevant when accreditation procedures are cyclical and systems need to be reviewed after a certain period. This means that budgeting is not always conducted in a manner that allows sustainability for the systems.

The costs of expensive certified products, which are often significantly higher than other COTS products, were also specifically mentioned by the respondents. This becomes especially relevant for establishing security areas, encryption solutions and implementation of emission security (TEMPEST).

The costs associated with audits and the funding of human resources were also mentioned by the accreditation authorities. While the issue of staffing will be examined in more detail in the following section, one respondent stated that there was insufficient funding to employ enough personnel for the accreditation process. Another issue noted under the section 'Too expensive/resource-intensive' is that there is a discrepancy between the number of dedicated personnel and the number of systems to be analysed.

3.2 Competence

Skilled staff are difficult to hire, both because of a general lack of experienced people and because of job market competition with the private and civilian sectors. In addition, the rapid increase in the complexity of technology, addressed in the next section, and systems that require not only regulations but also technical skills to be updated rapidly cause difficulty.

> *"Too many systems with too few dedicated analysts to perform security accreditation processes on them."*

Difficulties in recruiting and retaining well-trained employees were reported by several respondents. Private industry is mentioned several times as a competitor in the recruitment market and appears to pay more competitive salaries than the government sector. Thus, the strong demand for security experts in the private sector is believed to be playing a major role in staffing issues.

> *"Risk management and security considerations is a craft. Apart from good knowledge in security issues and technique, a deep understanding of the organisation, processes, regulations and the operation is needed. There are too few with those skills."*

The issue of staff training also seems to play an important role. One respondent stated that it takes a lot of patience and time to gain the skills necessary to work in the field and that many pursue other career paths. The complexity of the field means that it is not easy to become proficient and once an institution has made the necessary investments in terms of education and training of staff, there seems to be an observed tendency to leave to work in the private sector.

> *"We think the IT knowledge is more valuable at the civilian side and the engineering level is even more respected and the government is not able to 'fight' with these salaries. We have to find a solution via training programs to target the youth generation to start their carrier in the military and keep them as long as possible."*

The challenge of not having enough personnel in a very complex work environment was raised by many of the respondents. However, the challenge of competitive payment may often be beyond the control of the security authorities themselves. Offering interesting careers and retention plans were discussed and, in particular, providing training may be part of this. Some respondents simply stated that there is a shortage of staff, but without indicating whether it is due to a lack of qualified candidates, lack of interest or an institutional decision to allocate fewer resources. One respondent noted that there is not only a lack of trained personnel on the accreditation body side, but also on the client-side.

3.3 Changing Technology

A large number of respondents expressed their observation of rapid changes in information technology, and that as systems become more complex the number of systems also increases. This can lead to more time being needed to consider vulnerabilities and effects on existing systems and setting up appropriate security measures. This observation also ties into personnel needing to keep up not only with emerging threats, but also rapidly changing and increasingly complex technology all the while often working with a small number of personnel on issues, as described in the previous section. The increased number of dynamic and complicated systems and their technology may therefore lead to increased times in the accreditation process.

> *"As modern IT systems become increasingly dynamic and flexible, we experience that the accreditation process does not meet this demand and thus becomes very time-consuming for both clients and authorities."*

The growing complexity of national, bilateral and multinational frameworks and requirements adding to the increasing complexity of the systems themselves does not seem to simplify coordination and communication:

> *"Due to rapid changes in information technology, existing guidelines are failing to keep up with the pace of technological innovation, and it takes more time to establish appropriate security measures as the current guidelines do not fully reflect changes in the IT environment."*

According to some respondents, there appears to be a discrepancy between rapidly evolving technology and security regulations. The requirements and audit criteria addressed in security regulations need to keep up with the pace of technology to provide sufficient security standards.

One option to address these issues, according to some respondents, would be to rely on certified components or automated tools which could make the accreditation process scalable and simpler. In some cases, however, certified components may not be sufficient. Even if suitable certified components were available in every category needed, the focus on individual components may overlook how they operate and interact with other components as part of the system.

> *"In combination, lack of certified components, expensive resources and lack of staff. This stems from the core issue that technology is moving faster than security evaluations."*

The topic of changing technology shows that the issues described by the respondents are complex and interconnected and cannot be reduced to just one root cause. The responses also show that respondents attribute the cause of the issues to varying problems. While some see the lack of personnel as an elementary issue, others focus on the lack of funding or the policy framework and processes.

3.4 Client

Another aspect of time involved in accreditation appears to be associated with the relationship and communication between the accreditation authorities and their clients. According to some respondents, clients of accreditation bodies sometimes lack understanding of how long processes can take and, accordingly, requests are made late or without prior anticipation of time.

> *"[The a]ccreditation process is too much decorrelated from the CIS development process. Therefore, it is frequent that the CIS owner starts the accreditation process late when the system development is already pretty advanced. The accreditation, once started, points out changes that must be implemented before an ATO may be granted."*

In some cases, the discrepancy between accreditation authority and clients leads to further delays because changes have to be made even though the implementation or development is already at an advanced stage. However, this does not mean that the respondents blame their clients for long procedures; according to some, better coordination in the processes and earlier participation by the SAA would reduce problems of this kind.

Addressing security issues at the design stage of systems that need to be accredited would reduce potential difficulties, but some respondents were aware that there are many processes for clients to coordinate and that security can often fall behind as a priority.

> *"The current system is heavily dependent on an early cooperation by the organisations developing/providing the system. Occasionally [information security] is not one of the main design factors, leading to [information security] related requirements being implemented late in the project phase."*

A customer-centric approach seems to be able to mitigate some issues and contribute to an earlier and better dialogue. Communication and sharing of information between the stakeholders seem to be key in avoiding delays. Some respondents believed that there is not enough time planned for the accreditation process by the client, while others said that sometimes required documentation was initially missing and would therefore need to be produced at a late stage of a project. To have realistic anticipation from the client and the necessary documentation or files ready for the accreditation process, raising awareness of clients (and manufacturers, as addressed in the next section) was proposed by one respondent.

Many respondents were aware that national accreditation strategies and frameworks may be vast and complex. Accordingly, early cooperation and coordination with the clients generally seem to have a positive time impact on the process. As there is awareness of the issues involved, some nations are working on the processes and the communication between accreditors and clients and are also developing example material and documents for educational purposes.

3.5 Requirements

The relationship between private industry and civil society has been mentioned above. Another aspect of this concerning complex requirements is mentioned by one respondent:

> *"Insufficient cooperation and awareness between the public and economic sectors and complicated regulations in the field of classified information for obtaining a CIS security accreditation."*

It was often said that the accreditation process is very extensive and requires a lot of documentation. The processes may be facilitated if clients or manufacturers consider the preparation of documentation in anticipation or along other stages rather than at the end of the development process and engage with the appropriate authorities early in the process.

According to some respondents, stronger cooperation between parties, better communication of requirements and a focus on the requirements of security agencies on the part of the private industry could have a problem-solving effect. For the full effect the security agencies, their government clients and the private industry all have to participate in this exchange.

Also included in this category are concerns that the accreditation process focuses too much on compliance and not enough on actual security. If the accreditation regulations are not strong enough, this could lead to systems being compliant with the regulations when they are, in fact, insecure.

The alignment of processes is also interesting, as some respondents pointed out that certain accreditation procedures are cyclical and systems need to be reviewed after a certain period. In such cases, it may be advantageous if clients already plan the design of their system in such a way that they are prepared for the cyclically designed accreditations.

> *"There is no single set of security requirements that are applicable to all systems. It is very challenging to evaluate and accept residual risks in international or bilateral systems."*

On the topic of international or bilateral cooperation, some respondents said that coordination between partners may be slow and complicated and that sometimes regulations can be interpreted differently and approaches to information security may vary.

4. Recommendations

This chapter will present some recommendations for nations and organisations to consider when addressing the issues raised in the previous chapter. The recommendations are based on the observations made by the respondents to the questionnaire and the analysis of the causes detailed in the previous chapter.

There is no universal answer to the question of how to make the process of security accreditation of national security systems more effective and efficient because the accreditation situations of each nation in terms of budget, human resources, available time and required security levels are all different. The recommendations presented in this chapter are general and should therefore be applied selectively after a comprehensive review of whether they fit into the situations of each nation.

We provide a total of seven recommendations, each of which addresses one or more of the categories of issues previously described. Table 1 shows which of the recommendations will address, at least in part, each category of issue.

	R1	R2	R3	R4	R5	R6	R7
Funding			✓				
Competence			✓		✓	✓	✓
Changing Tech	✓		✓		✓	✓	✓
Client		✓		✓			
Requirements	✓					✓	✓

Table 1. Mapping of recommendations to categories of causes

R1 Define Clear Security Requirements

The types and scales of national security systems vary widely depending on the circumstances of each nation. The national security system's scope can vary from specific cryptographic equipment to large-scale information and communication infrastructure, and the types of technologies used in the national security system will vary from conventional Windows or UNIX systems to state-of-art 5G and IoT networks. Such diversity and complexity issues have led many nations to adopt a strategy to stipulate only fundamental security principles for national security systems, such as confidentiality, integrity, availability and accountability, and then to validate and verify compliance with the principles at the time of accreditation.

This strategy, however, does not provide detailed criteria at the beginning of the accreditation process, often leading to clients' or vendors' arbitrary interpretation and application of the security principles. This could result in modifications being required if the delivered system fails to meet the accreditation criteria, which in turn results in an increase in overall time and cost for accreditation.

Another problem with this strategy is that the accreditation results may vary depending on the competence of the accreditor. There should be a review by a senior accreditor or technical manager for each accreditation, but even such a review cannot completely exclude the involvement of the accreditor's subjective judgement.

To overcome this, nations need to have a set of definitions of types of national security systems. For each type of system, a clear scope for accreditation should be established, and individual components that make up the system identified. For the individual components, security requirements could be expressed in a similar way to Protection Profiles that are used in the Common Criteria scheme.[6] However, as there are typically many components in the national security system, security requirements for system integration and customisation must also be defined for the interface between components and overall operation and management at a system level.

The requirements for the national security system will first define specific functional security requirements, but also need to encompass assurance requirements which are necessary to encourage vendors to develop trustworthy products by asking them to apply a secure development lifecycle and to build a secure environment against supply chain attacks, and to provide evidence that these principles have been applied. Assurance requirements will also help accreditors and vendors communicate with each other regarding the trust they have in the security of the system. However, if the assurance requirements are excessive, it could result in a situation where vendors have to invest too much effort in documentation and accreditors have to spend too much time reviewing such documents.

One important factor to be remembered when establishing national security system requirements is that the risk-based approach can be a useful tool to improve the outcome as it considers assumptions related to the operation of the system, various types of threats that may arise, and security measures commensurate with identified threats. Without risk management, important security measures could be omitted from consideration and improper measures that do not meet the risk level could be introduced.

R2 Make Vendors Specify Systems Cleary

Another challenge many nations reported is that it takes a lot of time for accreditors to understand the system under accreditation. In some cases, accreditors are involved from the development stage of the national security system, but in many, they are likely to encounter the system only when its development is complete and an application for accreditation is submitted. It generally takes a certain amount of time for a third party to fully understand a complex system, and in the worst case, accreditation may need to be performed without a complete understanding of the system if there is a limit on the time allowed for accreditation.

To address this, accreditors should require vendors to write and submit a system specification document in a standardised format for individual components of national security systems and the entire system. The specification document should as a minimum include a description of the system components, the operational environment, the risks facing the system, and the security measures implemented to mitigate those risks. A standardised format would mean that vendors would use predefined common terminology so that the specification document can be understood and reviewed without misunderstanding. It could be similar to a Security Target document used in the Common Criteria[6] scheme. This standardisation would not only help accreditors improve their understanding, but also help them ensure the objectivity of results so that the same results can be obtained regardless of which accreditor performs the accreditation.

It is also important to inform and train vendors on this standardised way of writing the specification document to ensure that they can meet the required level of quality in the specification document. This education should also include practices and techniques to implement security functional requirements and assurance requirements. Wherever internationally accepted or commonly used standards could be adopted should be considered, making the documentation that vendors need to produce as widely

[6] The *Common Criteria for Information Technology Security Evaluation* is a framework for evaluating security requirements specified in a *Security Target*, which may conform to a more generic *Protection Profile*. [17]

useable as possible, thus also reducing the training requirements. In NATO, the Security Requirement Statement (SRS) [3] is one such standardised document.

R3 Secure Sufficient Number of Competent Accreditors

Many nations also raised a concern about the number and competence of accreditation personnel. One problem with the accreditation task is that the leadership may regard it as repeated routine work, even though the accreditation is fundamental to the security of national security systems. This could make the leadership assign a low priority to the accreditation task, resulting in a shortage in the number of accreditors.

A critical success factor for security accreditation is the full support of the leadership to secure sufficient personnel properly supported to maintain the highest level of competence. Having enough competent accreditors can be difficult because the demand for accreditation is variable over time, and the speed of advances in information technology is fast.

To address this, consideration may also be required for outsourcing all or part of the accreditation task. Given the sensitivity and secrecy of the national security system, there may be negative views on outsourcing. Those concerns may partially be overcome through an in-depth background check of outsourced personnel and the establishment of a non-disclosure agreement with them, although this requires resources for the appropriate government authorities. It would be beneficial to enact and operate a national qualification system for each detailed technology field to ensure that outsourced accreditors are sufficiently competent, and it will also be worthwhile to consider designating testing laboratories as partners in accreditation. The outsourced tasks need to be performed under oversight from the competent authority, and particularly sensitive tasks and systems should always be managed by the SAA itself.

Another important factor in maintaining the required level of competencies for accreditors is periodic training and education to maintain competencies and obtain new knowledge for state-of-art technologies. It can also be useful in establishing and disseminating common accreditation techniques and methodologies that all accreditors should apply equally.

R4 Define the Role of the Client

It could happen that the procuring agency, as a client of the accreditation service, just selects a vendor and initiates a procurement process without consultation with the SAA, or that the application for accreditation is urgently submitted at a late stage of the development or procurement. In the worst case, the client might simply introduce a vendor to the SAA without having performed any security reviews. If the client is just sitting on the side-lines, all burdens will then be transferred to the accreditor, which in turn leads to a delay in accreditation.

The client should act as a gatekeeper that performs initial screening and validation of the security of the system by reviewing the vendor's proposal and checking the security implementation status during the procurement process while providing information to the accreditor on the plans for system installation and operation. The roles and responsibilities of clients should be clearly defined so that they can perform them appropriately. Leadership in the client must be aware of the importance of cybersecurity, the security accreditation process and their responsibilities. Periodic training should be provided to IT security personnel of client organisations to help them acquire and maintain up-to-date security knowledge, and those responsible for IT procurement should receive training to gain an understanding of the accreditation process and their role in it.

R5 Establish an Efficient and Effective Accreditation Continuity Strategy

Accreditation of a specific national security system is not a one-time task, rather it must be continuously carried throughout the lifecycle of the system. It is because updates and patches can occur at any time until its disposal, and the changes in the system will likely be more frequent as information technology changes more rapidly. However, this ongoing accreditation will lead to increased workload for accreditors and delays in system modification, or even operation of systems without current accreditation.

Therefore, the accreditation resources need to be allocated efficiently and effectively by carefully categorising the changes into matters that require re-accreditation, matters that require partial validation through the accreditation validity maintenance process and matters that can be accepted without validation. However, in reality, such distinctions can be difficult since even very minor changes could produce critical vulnerabilities. The types of change allowed without re-accreditation should be formalised and agreed upon between the SAA and the client. When in doubt, the client should always consult the SAA before going ahead with changes that may compromise the security of the system.

If a vendor intentionally or accidentally omits some changes when it applies for accreditation validity, accreditors may not identify all of them unless they conduct a full inspection by comparing the configuration of the accredited system with that of the changed system. Accreditors should consider using automated tools to identify changes and impose strong sanctions if vendors fail to report them.

For those changes that do not require formal re-accreditation, sufficient processes and controls must be implemented with the client organisation and the vendor to ensure that the security posture of the system does not suffer. Measures to be taken would include assessment of the potential effect of changes, code reviews, continuous security testing and continuous monitoring of production systems. All these activities will also benefit from being automated to the greatest extent possible.

Managing changes efficiently would not only allow modifications to systems to be put into production more quickly, but would also offload work from the accreditors allowing them to focus on new systems and major changes.

R6 Utilise Automated Validation/Verification Tools

Automated tools would reduce the burden on accreditors and the time required for accreditation. For accreditors to use automated tools for accreditation tasks, they must first establish a process to verify that the results from those tools have sufficient levels of reliability. Although fully automated tools that can replace the task of human accreditors are not yet available, they could appear soon with the help of advances in artificial intelligence.

As mentioned in R5, automation can also greatly facilitate making sufficient checks when upgrading systems to avoid having to make big re-accreditation efforts frequently. Doing those tasks manually would not only take too long to keep up with the agility in development, but would also involve a high risk of mistakes being made.

R7 Cooperate with Allies to Share Security Measures and Vulnerabilities

Although the scope and use of national security systems vary by nation, there are common types of systems and components among nations. Mutual exchanges of information between allies and partners regarding risks and security measures of these systems could reduce the workload and time for accreditation. Such exchanges are becoming more important as information technologies change rapidly and it will be more difficult for a single nation to tackle all security issues within an appropriate

time frame. However, unlike general IT systems that handle unclassified information, sharing information regarding national security systems can be much more difficult. Therefore, building sufficient trust between nations has to be the first step towards such information sharing. The sharing party needs to trust that sensitive information will be appropriately protected by the recipient; the recipient needs to be able to trust the accuracy of the information received. Building trust takes time, so information sharing should be built up step by step.

The exchange of information and ideas could also extend to efficient and effective security accreditation practices and results from assessments of off-the-shelf components and systems which could remove some of the burden of review from those who receive the information.

5. Conclusions

In this report, we have looked at general factors that impede rapid security accreditation and recommendations on how to overcome them. Since the situations surrounding security accreditation are different for each nation, tactics and strategies for tackling the challenges will also vary. Therefore, the recommendations given here may not fit every situation. Rather, they should be regarded as a starting point for further investigation. An awareness of the challenges being, in principle, universal may be an incentive to increase the sharing of experiences. Such input from others, even if not directly relevant, may be adapted for the situation at hand and may spark new ideas. We hope that this report may be a small step in that direction and will inspire further cooperation in the field of efficient and effective security accreditation.

Some factors affect the effective application of the current processes but there are also challenges to applying these processes to new and agile ways of developing software. Making sure that both SAAs and their clients have the right resources for the job and creating awareness of what needs to be done may go a long way to overcoming these challenges. To address the latter type of problems, new processes and procedures may need to be developed. Increased use of automation may be an important part of this but further research is needed to fit automation effectively into the processes. It may also be that SAAs need to trust the work of others more, whether it is outsourced assessments, the results of automated processes or security checks done by the development team. The philosophy of security being everybody's responsibility is essential, but ways for the SAA to efficiently supervise also need to be developed.

There is precious little public research that looks at the metrics of the security accreditation process, whether regarding the resource requirements and time consumption or the actual security and assurance levels achieved. More could be useful, even if performed in a less sensitive domain to remain shareable with the broader community.

If processes are slow and cumbersome, there will always be an inclination to cut corners. Cutting corners in the security domain will always lead to the introduction of vulnerabilities. Therefore, research and development on how we can best assess and approve the cybersecurity of national security systems must continue and must be strengthened.

Abbreviations

5G	Fifth-generation technology for broadband mobile networks
ATO	Approval to Operate
CC	The Common Criteria for Information Technology Security Evaluation
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CIS	Communication and Information Systems
COTS	Commercial Off-The-Shelf
IoT	Internet of Things
IT	Information Technology
SAA	Security Accreditation Authority
SRS	Security Requirement Statement
TEMPEST	The investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment (strictly speaking a codename, not an acronym).

References

[1] "Communication and Information System Security", Enclosure "F" to *Security Within the North Atlantic Treaty Organization*, C-M(2002)49-REV1, North Atlantic Council, 2014.Available: https://nsm.no/getfile.php/136535-1624522152/Demo/Dokumenter/NATOs%20sikkerhetsreglement/C-M_2002_49_REV1.pdf

[2] *Primary Directive on CIS Security,* AC/35-D/2004-REV3, NATO Security Committee, 2013. Available: https://nsm.no/getfile.php/136550-1624522360/Demo/Dokumenter/NATOs%20sikkerhetsreglement/AC-35-D-2004-REV3.pdf

[3] *Management Directive on CIS Security,* AC/35-D/2005-REV3, NATO Security Committee, 2015. Available: https://nsm.no/getfile.php/136553-1624522396/Demo/Dokumenter/NATOs%20sikkerhetsreglement/AC-35-D-2005-REV3.pdf

[4] K. Wrona, F. M. Scharf and M. Jarosz, "Security Accreditation and Software Approval with Smart Contracts," *IEEE Communications Magazine,* vol. 59, no. 2, pp. 56-62, February 2021.

[5] The Council of the European Union (2013, 23 September), *2013/488/EU*, *Council Decision on the security rules for protecting EU classified information,* Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013D0488

[6] Agreement Between the Government of The Kingdom of Sweden and the Government of The Republic of Korea on the Protection of Classified Military Information, 2009. Available: https://www.regeringen.se/49c82c/contentassets/1e3e10ad7adc41f49c74e8d288c6b011/avtal-med-republiken-korea-om-skydd-av-forsvarsrelaterad-hemlig-information

[7] Security Agreement Between the Government of The Kingdom of Sweden and the Government of The Grand Duchy of Luxembourg on the Reciprocal Exchange and Protection of Classified Information, 2013. Available: https://www.regeringen.se/49c826/contentassets/15193b2652e948348ab805cac1825a0b/sakerhetsskyddsavtal-med-storhertigdomet-luxemburg-om-omsesidigt-utbyte-och-skydd-av-sakerhetsskyddsklassificerade-uppgifter

[8] *Security Agreement Between the Government of Ukraine and the North Atlantic Treaty Organization,* 1995. Available: http://old.mfa.gov.ua/mediafiles/sites/nato/files/security_agreement.pdf

[9] Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union, 2011. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:42011A070(01)

[10] R. Richards, “Automated Rapid Certification Of Software (ARCOS).” Defense Advanced Research Projects Agency, https://www.darpa.mil/program/automated-rapid-certification-of-software (Accessed 29 April 2021).

[11] K. Buszta, “Challenges in Certification and Accreditation,” *IT Pro,* pp. 56-59, May/June 2008.

[12] “Navy Aims for ‘Compile to Combat in 24 Hours’, CHIPS Magazine, July-September 2018. Available: https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=10501

[13] F. Moyón, P. Almeida, D. Riofrío, D. Mendez and M. Kalinowski, “Security Compliance in Agile Software,” in *46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, 2020.

[14] *Guide for the Security Certification and Accreditation of Federal Information Systems,* NIST SP 800-37, National Institue of Standards and Technology, May 2004. Available: https://csrc.nist.gov/publications/detail/sp/800-37/archive/2004-05-20

[15] L. Rising and N. S. Janoff, “The Scrum Software Development Process for Small Teams,” *IEEE Software*, July/August 2000. Available: http://csis.pace.edu/~marchese/CS616/Agile/Scrum/IEEEScrum.pdf

[16] T. B. Klein, “The DevOps: A Concise Understanding to the DevOps Philosophy and Science,” Sandia National Lab, Albuquerque, New Mexico, SAND2021-6250R, 2021. Available: https://www.osti.gov/servlets/purl/1785164

[17] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

Annex A Questions Asked in the Survey

- **Respondent**

  A1.1 Organisation:

  A1.2 Country:

  A1.3 Point of contact (title and name):

  A1.4 Means of contact (e.g. e-mail address):

  A1.5 May we publish in our summary report the fact that your nation/organisation has responded to this questionnaire?

- **Security accreditation organisation and schemes**

  A2.1 Please briefly describe your nation's or organisation's scheme(s) for security accreditation of national security systems:

  A2.2 What processes do you have to maintain the security accreditation of systems, i.e. to make sure that the security is adequate even as changes are made over time?

  A2.3.1 Do you have collaborations/agreements with other nations or international organisations to do certification or security accreditation jointly or to rely on the other party's evaluations/certifications?

  A2.3.2 Please describe:

- **Concerns with current scheme(s)**

  In the following, please describe your main concerns with the current security accreditation scheme(s) in order of importance.

  The most important concern:

  A3.1.1 Concern: (Choose from this list: *Too time-consuming, Too expensive/resource-intensive, Lack of staff, Lack of certified components, Difficulty accessing proprietary/confidential information, Does not reach adequate assurance, Does not address all threats/vulnerabilities, Results not consistent, Not independent, Other*)

  A3.1.2 Please describe the issue:

  A3.1.3 What is in your opinion the reason for this?

  The second most important concern:

  A3.2.1 Concern: (Choose from the same list as above)

  A3.2.2 Please describe the issue:

  A3.2.3 What is in your opinion the reason for this?

  The third most important concern:

  A3.3.1 Concern: (Choose from the same list as above)

  A3.3.2 Please describe the issue:

  A3.3.3 What is in your opinion the reason for this?

- **Time consumption for security accreditation**

  For the types of systems described below, please try to estimate the typical time for a security accreditation of such a system using your security accreditation scheme:

  Type of CIS: *'System/network for storing and transmitting/sharing classified documents.'*

  A4.1.1 Estimated time for security accreditation: (in months)

  A4.1.2 Please describe which part of the process is most time-consuming:

  Type of CIS: *'Military command and control system including radio transmission.'*

  A4.2.1 Estimated time for security accreditation: (in months)

  A4.2.2 Please describe which part of the process is most time-consuming:

  Type of CIS: *'Mobile device (laptop/phone)'*

  A4.3.1 Estimated time for security accreditation: (in months)

  A4.3.2 Please describe which part of the process is most time-consuming:

- **Delays in the process**

  A5.1 What are in your opinion the main reasons for delays in the security accreditation process? Are there for example any external factors causing delays?

  A5.2 What measures do you see that could be put in place to reduce those delays?

- **Projects and initiatives**

  A6.1 Do you currently have, or have you in recent time had, any projects/initiatives aiming to change your security accreditation practices in order to reduce time to reach a security accreditation or to address the issues mentioned above?

  A6.2 Number of such projects/initiatives:

  A6.3 Describe initiative briefly:

- **Any other relevant information**

  A7.1 Any other information about your security accreditation scheme(s) or projects/initiatives that you would like to provide that could be relevant for our study.

Annex B List of Projects and Initiatives

For information on how to get in contact with the projects listed below, please contact CCDCOE.

Risk Assessment Using the Critical Security Controls

General Intelligence and Security Service (SGRS) Cyber Accreditation, Belgium

Risk management is often a compliance-focused exercise and ineffective. The project aims for an effective Cyber Risk Management process from evaluating the current state of control effectiveness, closing gaps identified using a prioritised list of controls.

The new process is to be more security-focused rather than compliance-focused and to evaluate the effectiveness of the implemented security controls

With the new approach the periodical risk management process should become a continuous process

- **Primary Concern addressed**

  Assurance inadequate.

- **Scope and approach**

  The scope of the project is to revise the Defence homologation strategy to provide CIS Operating Authority with a prioritised list of security controls and to continuously evaluate the effectiveness of implemented security controls.

- **Main goal or objective**

  To reach adequate assurance, reduce time and administrative burden.

- **Status**

  Status of project/initiative: Pre-study

  Start date (approximate): 4 January 2022

  Projected end date (approximate): 6 September 2022

- **Documentation**

  The project references the CIS Controls https://www.cisecurity.org/controls/

Cyber Security Defence Preparedness Analytics Capability (CSDPAC)

Directorate of Information Management Security (DIM Secur), Canada

The CSDPAC pilot aims to explore the ingest and processing of a variety of information feeds, while eventually hosting multiple workflows based on Department of National Defence (DND) processes within a modular framework allowing easy addition and integration of interdependent workflows. CSDPAC is an initiative to explore accelerated and automated risk assessment based on evidence of system instrumentation and key controls. Information collected may be correlated and analysed to capture DND's cyber vulnerabilities, risks and overall security posture which can be used for continuous monitoring, and to perpetually improve that cybersecurity posture. The first trial to be hosted on the CSDPAC solution will be an optimised and integrated Security Assessment and Authorisation (SA&A) workflow mapped with all applicable DND security controls. The re-engineered SA&A process will be more efficient and made easier to use by automating as many of the security controls as possible and mapping better correlation with other related processes.

- **Scope and approach**

  The initial phase will provide automation of SA&A of all DND IT systems, and a repository for IT risk management data, and risk compliance functions. Additional phases have been proposed to include additional security functionality including automation of physical security functions, incorporation of departmental change and service management functions, and others.

  Provide Information Risk Management (IRM) functionality through the incorporation of the manual SA&A process into a workflow process, with identified stakeholder inputs and sub-processes/deliverables managed through this workflow. Integration of data feeds from various DND sources with associated search and analytics functions to support this process and compliance tracking, and overall risk management.

- **Primary Concern addressed**

  The current SA&A process is time-consuming, and it is difficult to manage both the process and the information generated.

- **Main goal or objective**

  To improve throughput of the departmental SA&A programme, provide improved risk management information to the DND/Canadian Armed Forces chain of command.

- **Status**

  Status of project/initiative: In pilot/trial use

  Start date (approximate): 1 March 2021

- **Documentation**

  Lead developer is Sphyrna Security https://sphyrnasecurity.com/

An Assessment of Required Changes to the Legislation Around Security Audits and Security Auditors

Ministry of Finance, Finland

The target is to identify shortfalls and other development requirements for legislation around security audits. The project's main deliverables are 1) a report on the current state and its shortfalls and suggestions on improvement in relevant laws, and 2) implementing the changes in legislation.

- **Primary Concern addressed**

  Roles and responsibilities are not entirely clear between different participants of the auditing process and there are partial mismatches between security requirements and auditing criteria.

- **Scope and approach**

  The scope of the project is legislation concerning security audits and auditors. A set of interviews of parties that are currently involved with security audits: public sector, both public and private auditors, and service providers.

- **Main goal or objective**

  Identify improvements in structures and practices around security auditing. Develop a plan on what changes should be implemented and implement them in law.

- **Status**

  Status of project/initiative: In development

  Start date (approximate): 1 September 2020

  Projected end date (approximate): 31 December 2022

- **Documentation**

  Project is part of a security programme whose public website is https://vm.fi/hanke?tunnus=VM174:00/2020 (in Finnish and Swedish)