Continuous improvement on maturity and capability of Security Operation Centres

Cengiz Acar Türk 1,3 | Murat Ulubay 2 | Efe Erdur 1

1 Cyber Security Graduate Program, Middle East Technical University, Ankara, Turkey
2 Department of Management, Yildirim Beyazit University, Ankara, Turkey
3 Cognitive Science Graduate Program, Middle East Technical University, Ankara, Turkey

Correspondence
Efe Erdur, Cyber Security Graduate Program, Informatics Institute, Middle East Technical University, 06800 Ankara, Turkey. Email: efe.erdur@metu.edu.tr

Abstract
This study addresses maturity and capability assessment of Security Operation Centres (SOC). It aims to contribute to continuous improvement for SOCs by proposing a complementary methodology that provides SOCs a self-assessment capability. The method basically involves an assessment of the gaps between the current and the desired states of the organization and facilitates determining critical aspects that have priority. The proposed methodology is based on the define, measure, analyze, improve, and control methodology of the Six Sigma approach and offers a service-oriented improvement process for SOCs. The applicability of the methodology is demonstrated by a case study. We evaluated subject matter experts’ reviews using simplified conversation analysis as a qualitative, content-analysis approach.

1 INTRODUCTION

Technological developments in information and communication technologies have a major impact not only on individual lifestyles but also in business conduct by introducing new fronts. These developments are accompanied by novel strategies, techniques and procedures that aim at preventing cyber security threats against valuable information assets [1]. A sustainable protection against cyber security threats depends on cyber security teams’ continuous improvement (CI) and their fast adaptation to precautions in new fronts. On the other hand, a systematic alignment is required between business processes and business strategies that are subject to dynamical changes [2]. The present study aims at investigating the adaptation of Security Operation Centre (SOC) organizations to the dynamic environment of cyber security by methods of systematic improvement.

The responsibility of an SOC is to protect the institution against cyber security threats by providing cyber defence [3]. Recently, SOCs enrich their capabilities by including novel approaches in cyber defence, such as threat intelligence, threat hunting and cognitive security. However, the research on the architectural management and CI of SOCs are not in a mature state, possibly due to limited awareness [4].

According to Hewlett Packard Enterprise examination, which was conducted in 2017 over 140 SOCs in more than 180 assessments around the globe, the majority of cyber defence organization’s maturity remains below target levels [5]. They report that 82% of SOCs fail to meet the criteria and fall below the optimal maturity level. In addition, 27% fail to achieve even minimum security monitoring capabilities. This finding indicates an intense presence of cyber security vulnerabilities that may result in compromises that prevent running business services. The straightforward solution to this issue is to develop methodologies for CI of SOC teams, as well as developing methodologies that monitor the improvement. Maturity models are such tools that address those challenges.

Maturity models aim at identifying project-specific or organizational strengths, weaknesses and benchmarking information [6]. More generally, maturity and capability assessment models are useful for an organization in self-assessment of its current maturity and capabilities, as well as revealing what to improve. A drawback of maturity models is that they do not aim at further answering the question how to improve. On the other hand, CI approaches focus on the how-to-improve question. The present study aims at combining the CI approach and the maturity and capability assessment models to propose a methodology that is able to provide a sustainable framework for the improvement of SOCs.

The following section introduces the background and relevant work. In Section 3, the methodology of the framework is presented. Section 4 presents a case study that demonstrates
the implementation of the model. Section 5 presents the findings. Finally, in Section 6, we evaluate the findings and propose future work.

2 BACKGROUND AND RELEVANT WORK

Recently, relatively limited research is available on the measurement of maturity and capability of SOCs compared to research in other cyber security domains. Van Os presents an investigation of common maturity integration models, as well as suggesting a framework and a self-assessment tool for SOC organizations for the assessment of maturity levels [4]. Although the study provides satisfying results for self-assessment, organizational improvement methods are not covered. Several domain-specific frameworks that are employed by cyber security enterprises, which provide security operation or consulting services are publicly available. For example, Aujas, an IT security company, announced a measurement framework to measure maturity of information security incident management [7]. Another cyber security company, namely CREST, provides a similar assessment tool for incident response (IR) service [8]. These frameworks are based on incident management services rather than the whole SOC organization. However, they serve as models for other assessment domains, too.

The aforementioned frameworks offer practical methodologies to assess maturity and capability of SOCs. On the other hand, they are limited in presenting a systematic improvement methodology. The lack of a systematic improvement methodology may lead to a lack of systematic procedures that make the organization open to cyber security threats which may have an impact on the quality of service outputs. The focus of the present study is to propose a CI methodology for a specific team, SOC. There exist relevant research studies that may help investigating current CI frameworks, as well as specific methodologies and tools that are used in such frameworks [9]. As a first step in the development of the proposed framework, the available frameworks have been comparatively analysed in terms of their usage areas and evaluation of their advantages and disadvantages to understand which framework would be the best fit for the purpose of the present study. Next, we investigated current capability and maturity models for SOC organizations, since the assessment of the organization is a major part in CI process.

An analysis of the existing service-oriented CI methodologies reveals numerous SOC services that could be examined. In the present study, we limit our scope to the Incident Handling and Response (IHR) service, which is a core service that is provided by SOCs. Accordingly, the present study includes maturity and capability assessment methods for this specific service. The authors present more background on the CI models, maturity and capability assessment in SOC, and IHR assessment and improvement.

2.1 Continuous improvement models

A CI model is defined as ‘a broad change program, planned, organized and systematic, and distinguished from project-based models of change’ [10]. American Society for Quality defines CI as the ongoing improvement of products, services or processes through incremental and breakthrough improvements [11]. These definitions show that CI is an improvement process, and it can be applied to products, services or processes. In the present study, we focus on applying CI over services and processes rather than products, based on findings and appropriate models in the research literature. There exist numerous CI approaches. For example, de Mast and Lokkerbol investigated the Six Sigma define, measure, analyze, improve, and control (DMAIC) method from a problem-solving perspective. They have selected five problem-solving methodologies from relevant literature and studied the efficiency of DMAIC in these five domains [12]. Sokovic, Pavletic and Pipan reported a comparison of plan do check act (PDCA), Radar Matrix, DMAIC (Six Sigma) and DMADV (Design for Six Sigma [DFSS]) [13]. Figure 1 shows the comparison of the steps that are used by these methodologies. Their work does not only present a process-based comparison among the improvement methodologies but also presents likely domains of use for each methodology in terms of products, processes and services in organizations. Their findings show that PDCA cycle is a simple but effective methodology for the CI process, which could be used by large number of people in the organization. Another benefit is that after the completion of the ‘act’ stage, the cycle can start again for forthcoming improvements [13]. On the other hand, it oversimplifies improvement process which makes it not the best option for large-scale complex changes. Additionally, in PDCA cycle, it is assumed that all improvement starts with planning. Plan, as a word, has a limited meaning, and it does not cover analysing

![Continuous improvement methods’ comparison](image)
process specifically which is a core component for proactive improvements. Considering its disadvantages, PDCA may not be the best model for whole SOC improvement process; however, the simplicity and adaptation to rapid changes in functionality make it a proper methodology for service level of CIs in SOCs.

DFSS is a methodology that includes all the required functionalities from the onset of design. Therefore, this approach was suggested as a best fit for new products or processes [13]. The main objective of DFSS is designing right at the first time. The focus of the present study is SOC teams that are already active and providing ongoing services to their customers where interruptions or re-constructions in the services are out of question unless there are crucial problems in the core architecture of the current service. Therefore, in the present study, we did not employ the DFSS methodology.

Another methodology is RADAR, which is also defined as a strategic, systematic, fact-based and data-driven methodology. Since it is designed as a data-driven model, assessment and measurement comprise a crucial part of DMAIC at the initial define (D) phase. A process cannot be measured unless it is defined properly; therefore, it is not possible to utilize DMAIC in improvement actions [13]. This requirement of the methodology fits well to the problem that is defined in the present study, since maturity and capability assessment of current organization are key points to improve any SOC organization. Another characteristic of DMAIC is that it can be used to create gated processes, in a cycle as it is shown in Figure 2. SOC organization has multiple ‘services’ which can be accepted as individual projects of organization; therefore, this characteristic of DMAIC will be also useful for designing service-oriented CI for SOC. The following section presents measurement methodologies for maturity and capability in SOC organizations.

2.2 Maturity and capability assessment in SOC

Capability and maturity assessment models are used for assessments at an organizational level. A maturity and capability model is defined as a tool that facilitates assessing the current effectiveness of a person or a group and figuring out what capabilities they need to acquire next in order to improve their performance [14]. A maturity and capability in the domain of cyber security is a framework for measuring the maturity of a security programme and guidance on what to do to reach the next level.

Although there exist capability and maturity models defined for all of cyber security, information security and IT domains, there is no maturity model or common framework currently available and specific to security operation teams. As stated by the Open Web Application Security Project (OWASP, 2020), which is an open project for improving security of software application, there is no framework available from governmental, non-governmental or commercial organizational sources, recently [15]. In Section 3, we introduce the literature work that addresses the development of capability and maturity models in relevant domains.

Jacobs, Arnab and Irwin propose a classification of the levels of process maturity in security operations centres, based on an investigation of industry-accepted maturity levels and frameworks, such as Control Objectives for Information Technology (CoBIT), Information Technology Information Library (ITIL) and also security frameworks such as ISO/IEC 27001 [16]. They offer six levels of maturity, which have alignment with other specification in the literature (Table 1).

More specifically, van Os followed a proactive research methodology and proposed a continuous representation for capability and maturity levels for SOC organization in their study [4]. Their methodology defined an organizational model for SOC including 23 aspects in five domains (business, people, process, technology and services), and it included a tool to measure maturity and capability levels of an SOC organization. The following section presents the concepts of IHR assessment, which will play a bridging role in the development of our proposed model.

2.3 Incident handling and response assessment

According to a survey conducted by Van Os [4] among 16 common SOC organization activities, the most critical three
TABLE 1  Process maturity comparison [16]

| Level | Name                           | Alignment                                                                 |
|-------|--------------------------------|---------------------------------------------------------------------------|
| 0     | Non-existent                   | CoBIT 0 etc.                                                              |
| 1     | Initial                        | CoBIT, SSE, ITIL: Initial CERT: Exists                                   |
| 2     | Repeatable                     | (CoBIT, ITIL, SSE-CMM and CERT/CSI)                                      |
| 3     | Defined process                | (CERT/CSI)/well-defined (SSE-CMM), defined process (CoBIT), common practice (CITI-ISEM) |
| 4     | Reviewed and updated           | (CERT/CSI, quantitatively controlled (SSE-CMM), managed and measurable (CoBIT) and continuous improvement (CITI-ISEM)) |
| 5     | Continuously optimized          | Optimized (CoBIT), continuously improving (CITI-ISEM), continuously improving (SSE-CMM) |

Abbreviations: CERT, computer emergency response team; CITI-ISEM, Citigroup’s Information Security Evaluation Model; CMM, capability maturity model; CoBIT, Control Objectives for Information Technology; CSO, company security officer; ITIL, Information Technology Information Library; SSE, systems security engineering.

processes were specified as ‘Security Incident Management’, ‘Security Monitoring’ and ‘Security Analysis’ (Figure 3). These processes can be defined as the components of a more generic service, namely IHR, which is also the scope of the present study. Nevertheless, the proposed methodology can be applied to other services as well.

A closer look at IHR maturity assessment frameworks in the literature reveals two major frameworks, namely the Information Security Incident Management (IS-IM) Framework Maturity Measurement Model and the framework by CREST, as introduced below. The IS-IM Framework Maturity Measurement Model was proposed by AUJAS. The AUJAS is a global IT risk management company that offers a demonstration version of IS-IM framework – a Microsoft Office Excel tool – for maturity management. Their maturity model is built in line with the CoBIT, ISO 27035 and National Institute of Standards and Technology (NIST) 800-83 standards as a base for guidance [7]. In this framework, the maturity of IS-IM is measured across six domains – Governance, Process, People, Technology for Monitoring, Prevention against malicious code and Networking. For each domain, the tool asks the user to fill in a questionnaire using a number from 1 to 5 for estimated maturity level for the capability that belongs to the relevant domain. After the user provides all estimated maturity levels, the tool shows the maturity score under the ‘score’ sheet as shown in Figure 4.

The CREST is a non-for-profit organization that focuses on creating technical knowledge to security world [8]. Similar to AUJAS, they provide a measurement assessment tool for cyber security IR. The tool collects data from the user in three phases: Prepare, Respond and Follow-up. The user enters the data in terms of the representation of the configuration state (the target state) and the representation of the assessment state (the current state), then the maturity scores are displayed in a radar chart to the user. Figure 5 shows an example radar chart as an output of the CREST framework, where the blue, green and orange line represent the current maturity scores of the three phases defined as Prepare, Respond and Follow-up correspondingly, and grey lines represent the target maturity levels of the corresponding services. Relevant studies in IHR service improvement are presented in the next section.

![Number of Participants Specified as 'Critical']

| Security Incident Management | 9 |
| Security Monitoring          | 8 |
| Security Analysis            | 4 |
| Security Operations          | 3 |
| Log Management               | 2 |
| Vulnerability Management     | 2 |
| Policy & Compliance          | 1 |

![Security Operation Centre process activities – criticality of services](image)

![Maturity results of assessment from Information Security Incident Management framework](image)

2.4 Incident handling and response service improvement

Specific methods of incident handling by cyber security teams is a popular topic in the cyber security world. In the present study, we focus on improving how the IHR service is offered rather than focusing on the methods on handling specific incidents. The improvement highly depends on internal resources of the organization, such as goals of the organization, customer expectations, business requirements, among other parameters. In our presentation of the topic below, we include
cyber security experts’ reviews on blogs or web pages in addition to academic resources.

A proposal for improving IR service is automation [17]. Wichman proposes that automation of repetitive manual tasks is a critical improvement for this service, and it makes the SOC team detect, analyse and respond high-risk incidents faster. Brown, in this study for Optiv research, claims that the average time for handling an incident decreases about 96% with proper methods of automation [18]. Another improvement that Wichman suggests is the orchestration which enables the organization to use their human resources properly in the automation of the process [17]. Accordingly, orchestration aligns people, processes and technologies to satisfy service requirements. CyberSponse, a cyber security company, emphasizes the importance of collecting metrics to improve detection parameters and improvement of the service, among other parameters [19]. They also emphasize the importance of orchestration to improve service quality. According to Holloran [20], it is crucial to define and use metrics to improve an IR service. He claims that an improvement as such helps the team avoid alert fatigue and start responding to incidents that are of priority.

In Table 2, the authors present the relationship between IHR service and required actions to improve the service in a SOC security model, based on the previous research reported in the literature.

In summary, a review of the literature for CI models, maturity and capability models, and IHR improvement reveal the picture that we present in Figure 6 for SOC teams. Improving a service – IHR service in this case – depends on people, processes and technology in general. In the following section, we present the proposed methodology in more detail.

3 | METHODOLOGY

Six Sigma and other CI approaches focus on ‘how’ to improve a service or a product but they cannot provide what to improve. On the other hand, the capability and maturity models for SOC organizations provide the visibility of ‘what’ to improve by reporting current maturity levels of organizational services and calculating the gap between the current state and the desired state of each service of the organization.

The focus of our methodology is on combining those approaches to provide a full scope of CI methodology for SOC organizations. The methodology employs the DMAIC methodology of the Six Sigma approach at an organizational level in order to satisfy this requirement. Additionally, the improvement of each service in the whole organization is a specific task that must be evaluated and processed separately. For this, the PDCA cycle was used for service-level improvements due to its simplicity and adaptation to the dynamicity of the system.

In short, the methodology defined in this study aims to propose a guideline in order to apply CI on SOC processes using the Six Sigma DMAIC methodology and the PDCA cycle combined, as shown in Figure 6.

3.1 | Six Sigma in the service industry

Although Six Sigma was initially designed for the manufacturing industry, it rapidly expanded to different domains, such as marketing, engineering, purchasing, servicing and administrative support, as the organizations noticed the benefits of the approach [21]. In service-oriented business, it has been used in financial services, healthcare industry,
telecommunication services, utility companies and airline industry, among others [22]. Table 3 shows the potential applications of Six Sigma within service processes.

As a more specific example, Aazadnia and Fasanghari have applied Six Sigma to Information Technology Service Management by considering CI [9]. They combined ITIL — which includes set of guidelines that specify what an IT organization should do — and DMAIC of Six Sigma in order to provide a better methodology for improving the quality of IT service.

### 3.2 Applying Six Sigma DMAIC to SOC improvement

The DMAIC methodology of Six Sigma approach has been defined in five steps, namely problem definition (D), measurement of the problem (M), data analysis (A), improvement process (I) and controlling (C) or monitoring process to prevent recurring problems [9]. Figure 7 shows the flow of the methodology.

In the present study, each phase of DMAIC was applied to SOC organization by considering the characteristic functionalities of the specific security service (IHR). DMAIC is an iterative process and the deliverables of each phase provide input to the next phase. Therefore, the suggested deliverable list for each phase of the process is specified, which are gathered from the literature and optimized for the benefit of SOC organizations. The phases of the proposed model are presented in the next sections.

#### 3.2.1 Phase 1 – Define

In this phase, the first step is to define the scope and objectives of the organization. For an SOC team, the scope definition starts with determining which services are being provided currently or expected to be provided in the future by the organization. The number and type of services that are provided by an SOC could vary. For example, van Os has defined seven services for SOC which are Security Monitoring, Security Incident Management, Security Analysis and Forensics, Threat Intelligence, Threat Hunting, Vulnerability Management and Log Management [4]. MITRE, on the other hand, has defined the services of an SOC listed as Real-Time Analysis, Intel and Trending, Incident Analysis and Response, Artefact Analysis, SOC Tool Life-Cycle Support, Audit and Insider Threat, Scanning and Assessment, Outreach [23]. Although the service types could vary in different sources, some of the services are named differently by convention although they are practically the same or very similar to each other. For example, ‘Security Monitoring’ (Van Os) maps to ‘Real-Time Analysis’ (MITRE). Similarly, ‘Threat Intelligence’ (Van Os) maps to ‘Intel and Trending’ (MITRE) and ‘Security Incident Management’ (Van Os) maps to ‘Incident Analysis and Response’ (MITRE). Finally, ‘SOC Tool Life-Cycle Support’ (MITRE) has no exact mapping in Van Os [4,23]. Those similarities help the improvement of the model by reducing the space of likely services given by SOC teams.

The next step is to identify the stakeholders. Any people or organization that is affected by SOC could be defined as a stakeholder. However, they could be prioritized regarding the authority they have over the project and their interests to the project. The matrix in Figure 8 was proposed for the prioritization of stakeholders by the authors of [24].

According to the matrix model presented in Figure 8, the stakeholders with high power and high interest are more directly engaged to the project compared to the other quadrants. Therefore, the roadmap of the projects should be determined together with these stakeholders. The other quadrants in the stakeholder matrix may be determined as lower priority, and they should be satisfied, informed or allowed to monitor the updates in the project regarding their positions on the power-interest grid.

An SOC team can be in-house or external. An in-house SOC is a team that belongs to the company, whereas an external SOC refers to an outsourced service. The difference between these two organization types does not affect processes, services or outputs of the SOC significantly. However,
TABLE 3  Potential applications of Six Sigma within service processes [22]

| Type of service function       | Potential areas where Six Sigma may be employed                                                                 |
|--------------------------------|---------------------------------------------------------------------------------------------------------------|
| Banking                        | Wire transfer processing time, number of processing errors, number of customer complaints received per month, number of ATM breakdowns, duration of ATM breakdowns etc. |
| Healthcare                     | Proportion of medical errors, time to be admitted in an emergency room, number of successful surgical operations per week, number of wrong diagnoses, waiting time to be served at the reception in a hospital etc. |
| Accounting and finance         | Payment errors, invoicing errors, errors in inventory, inaccurate report of income, inaccurate report of cash flow etc. |
| Public utilities               | Late delivery of service, number of billing errors, waiting time to restore the service after a fault has been reported, call centre of the utility company etc. |
| Shipping and transportation    | Wrong shipment of items, wrong shipment address, late shipment, wrong customer order etc.                      |
| Airline industry               | Baggage handling, number of mistakes in reservation, waiting time at the check-in counter etc.                |

FIGURE 7  Six Sigma methodology [9]

it may have impact on the scope of the project, stakeholder definitions and budget of the project. In an in-house SOC, the stakeholders may be senior executives, cyber security experts or analysts. whereas in an outsourced SOC, the customer has to be included into the stakeholder list, as well.

Stakeholder expectations and metrics together are called as critical to quality (CTQ) definitions [25]. In other words, CTQ includes which services or processes are critical to SOC team, and what are the target requirements of the organization. For this reason, defining stakeholders correctly is the key stage of CTQ definitions.

As a result of the steps taken in the first phase of the model (viz. Define), the expected deliverables are as follows:

- Scope and goals
- Stakeholder analysis
- Budget planning
- CTQ outline

3.2.2  Phase 2 – Measure

The items in the CTQ outline (a deliverable of the previous phase) may be high in number and they might be defined as title summaries only. The prioritization and elaboration of the CTQ outline should be investigated in this phase. In particular, if the SOC is providing an outsourced service, the CTQs regarding the customer side should be prioritized.

As it was stated earlier, the DMAIC methodology highly depends on statistical measurements. Therefore, the second step of this phase is to determine what to measure and how to measure [22]. For an SOC team, two types of statistical data must be studied: metrics, and maturity and capability assessment. Operational metrics, also called the quantification of security service, are the significant components of efficiency, effectiveness and satisfaction (meaningfulness) [26]. Maturity and capability assessment, on the other hand, is the main component to investigate how processes or elements in an organization perform [4]. These two items combined produce holistic data to define process capability and performance which satisfies one of the key deliverables of this phase [9]. Although the results of assessment are going to be investigated in detail in the following phase, the gaps between goals and current states are also supposed to be determined in this phase of the methodology.

Finally, the scope and goals from the previous phase should be reviewed in line with the measurement results, and
The objectives of the CI process should be defined [12]. The deliverables created at this phase are as follows:

- Determined CTQ definitions and details
- Process capability and performance
- Determined gaps for improvement
- Objectives

### 3.2.3 | Phase 3 – Analyse

This is the phase where the results of measurement are analysed, and a roadmap of the improvements is created. The vital services and component of the organization are highlighted considering the results of capability and maturity result analysis, metrics and other measurement factors, if defined. Another important aspect of this prioritization is to financially quantify the improvement for the organization [22]. The cost of the required improvements for the services and components should be calculated, and prioritization of the improvement components should be re-analysed.

The next step is to define a cause–effect diagram for expected improvements. Most of the services in an SOC are directly or indirectly connected to each other; therefore, it is not possible to evaluate each of them independently for improvement. The connections between different services in an SOC are described constitutively in the best practices. For example, the ‘IHR’ service is directly influenced by the ‘Threat Intelligence’ service [27,28]. On the other hand, some interactions between services and other components could vary from one organization to another. This interaction diagram should be defined/drawn/created, and risk assessment should be studied in order prevent possible interruptions in SOC services in the improvement phase.

Finally, considering all the parameters defined above, the roadmap of the planned improvement process is documented and financial requirements for determined improvements are calculated and specified.

The deliverables created at this phase are as follows:

- Prioritization of services/components to be improved
- Determining root causes of the problems in services/components
- Cause–effect diagram
- Financial details of improvement costs

### 3.2.4 | Phase 4 – Improve

In the previous phases of the methodology, the components and services are determined and planned for the improvement. The Improve phase is basically the implementation phase. As an initial stage, a risk assessment has to be conducted to identify potential problems. In the regular DMAIC process, the implementation starts after the risk assessment. However, SOC teams are multi-serviced organizations and making the improvement is not an action in isolation. Therefore, in this step of the methodology, another simple and effective CI approach (PDCA) is applied. The PDCA approach has its own planning, assessment, improvement and control steps. Figure 9 illustrates how the Improve phase of DMAIC will be handled using PDCA.

Similar hybrid approaches that entail combination of different CI models have previously been proposed in the literature of continuous improvement / total quality management. These combinations might be different from each other depending on the requirements of the implementation field. In these studies, similar to the proposed combination in this study, one cycle of one model might constitute the sub-steps (or cycles) of a single step in another model. [13,29–31].

The SOC service(s) that are part of the improvement are then determined, and they are improved by applying each step of the PDCA cycle, as presented below.

The Plan phase includes identifying the problem that is specific to corresponding service and defining targets of improvement. For example, given that our reference service is the “IHR Service”, a specific maturity and capability assessment could be performed to understand current status of the service [7,8].

Another data that should be collected is the metrics related to this service. Afterwards, the results are analysed, and the improvement parts of the service are determined in the Plan phase.

The next phase is the Do phase. When the potential solution is determined, it should be applied to a small-scale test project and results should be analysed whether the solution works or not. In the next step, namely the Check phase, the measurement data are updated, and the results are compared. The first three steps of this cycle – Plan-Do-Check – can be conceived as an internal cycle, and it can loop as long as needed until the results of the improvement become satisfactory.

The next phase is Act, where the planned solutions are applied to all the processes. The results are documented, all the relevant stakeholders are notified about changes, as well as the suggestions for the following PDCA cycles.
Finally, the deliverables of the Improve phase are as follows:

- Defining brainstorming results of possible solutions
- Risk assessment of potential solutions
- Defining and implementing best solutions
- Re-evaluation of the impact of performed improvements

### 3.3 Phase 5 – Control

This is the final phase of the methodology where the results are verified, processes are adjusted in order to provide sustainability of the improvements [32]. Standards and procedures are developed/improved in alignment with the updates in the system, and all the improvements are documented. The deliverables created at this phase are as follows:

- Control verification documentation
- Standard and procedure documentation

In the following section, we present the application of the proposed methodology in a case study.

### 4 CASE STUDY

In this section, a use case scenario is reported to illustrate how the proposed methodology works. In its described form, the methodology includes a large number of documents as deliverables which are beneficial for the sustainability of the improvements. However, in this case study, documentation-related outputs are omitted for simplicity. The specified scenario covers data-oriented measurements and decision-making steps in the methodology, as presented below:

The first phase is the Define phase. The outline of the organization is shown in Table 4 and expected maturity and capability levels for the components of this organization is defined considering budget and expectations of the project as shown in Figure 10. Also, in this case study, we assumed that the organization wants to compliance with NIST 800-83, which is defined as a framework for malware incident prevention for desktop and laptops [33].

In the Measure step, the maturity and capability assessment framework from [4] is used to assess the current maturity and capability levels of the organization. The resulting radar map is shown in Figure 11.

The next step is the Analyse phase, where the results of the assessment are analysed. In this scenario, all the services are assumed to have some score in the prioritization scale, and the

---

**TABLE 4 Outline of the organization definitions**

| Organization type | In-house                          |
|-------------------|----------------------------------|
| SOC model         | Centralized                      |
| Geographic operation | Regional                  |
| Stakeholders      | Security Operations Executive   |
|                   | SOC Manager                      |
| Services [4]      | Cyber Security Experts           |
|                   | Security Monitoring              |
|                   | Security Incident Management     |
|                   | Security Analysis and Forensics  |
|                   | Threat Intelligence              |
|                   | Threat Hunting                   |
|                   | Vulnerability Management         |
|                   | Log Management                   |

---

**FIGURE 9** Applying PDCA on Improve phase of DMAIC. DMAIC, define, measure, analyze, improve, and control; PDCA, plan do check act

---

**Diagram:**

- Define
- Measure
- Analyse
- Improve
- Control

DMAIC for Organisation

Plan

Do

Act

Check
The cost of the required improvements are omitted for simplicity. In real situations, those parameters have to be taken into consideration, as well.

Combining the expected maturity levels (Figure 10) and the current status of the organization (Figure 11), it can be concluded that the CI must be applied to ‘Security Monitoring’ and ‘Security Incident Management’ firstly, since the gap is larger. These two services are complementary components of the ‘IHR Service’, which is also the service that we focus in the present study.
The next phase is the Improve phase, where the PDCA cycle is applied to the “IHR Service” in sub-steps that are described in the previous section.

The first of these sub-steps is the ‘plan’. In this sub-step, in a similar way to maturity assessment of whole organization, a more specific incident management measurement framework – AUJAS IS-IM Framework Maturity Measurement framework – is used to learn about the current maturity levels of the service in terms of governance, people, process and technology [7]. This tool includes questionnaire-based assessment approach per each domain. The user is expected to assign a maturity score from 0 to 5 per each question of the corresponding domain, and the tool calculates average of the maturity scores for each domain. A sample set of questions from the ‘process’ domain assessment of the tool are illustrated Table 5.

The resulting scores of the detailed assessment that are presented in Table 6 are similar to ‘Security Monitoring’ and ‘Security Incident Management’ maturity results that were presented in Figure 11. Nevertheless, we have used a more detailed assessment tool to get more detailed information about likely causes of the issues at hand.

In the example provided in Table 6, the resulting scores for the maturity assessment for IHR suggest that an improvement should be applied to the ‘Process’ category at first, then the ‘Malicious Code’ part of the ‘Technology’ category.

In this case study, which is presented as a pedagogical example, the items in the questionnaire that are assessed by a ‘0’ score means that the organization does not have a functionality as such. For example, the answer scores of the questions from ‘Incident Logging – Service Desk’ category in the ‘Process’ domain are determined as ‘0’ meaning that this organization does not have service-desk-related process at all. About the other categories, it can be deduced that the organization has coverage at a certain level of maturity.

Additionally, it is likely that some of the items in the questionnaire may not be applicable to the organization. For example, in this case study, we assumed that the organizational goal is a compliance to all required items for NIST up to expected levels, but not ISO-27035 (Information Security Incident Management Standard). In cases like this, the score values are tagged as N/A in the questionnaire meaning that we want to exclude them from assessment hence such requirement is out of scope. Excluding the ISO-27035 specific capabilities from the questionnaire has only slightly updated the maturity result, because core requirements exist in multiple compliance sources. For example, in our case study, the maturity of the service has increased from 1.19 to 1.57 for process domain as shown in Table 7; however, it is still below the expectations. The expected target of the organization for ‘process’ domain of this service is defined as ‘4’ earlier; besides, the organization wants to satisfy compliance requirements of NIST-8083. At this step, the items in the list are investigated, the missing items or the items with lower scores has been analysed, the requirements of the improvement are determined and roadmap for improvements is created.

Following the assessment procedure introduced in the previous section, the next steps in the assessment include the application of the Do, Check, and Act actions, as reported below.

At the “Do” step, the improvement items are applied to a small set of the incidents, thus being applied to specific category of incidents with lower value. At the “Check” step, for this example, we assume that no risks or problems occurred in the processes, therefore the service specific assessment is measured again in applying the improvements to whole system. The results in Table 8 (maturity = 3.57) show that the maturity would be close to the expectations if the improvements can be applied successfully.

Next, in the ‘Act’ stage, the planned requirements are implemented through all processes in the service. Afterwards, the maturity of the service is re-assessed using same framework and results are shown in Table 8.
5 | EVALUATION OF THE METHODOLOGY

To evaluate and verify the validity of the suggested methodology, evaluation of actual managers of SOC is preferred. Perspectives and experiences of subject matter experts of cyber security domain, more specifically, SOC, are invaluable sources to detect whether a proposed methodology has flaws which might render it unimplementable or counterproductive. For assessing the impact of a DMAIC project, several evaluation techniques have been used in the literature, like surveys with participants [34] in the organization or expert evaluations of performance [35], after the projects completed. Our approach of examining the implementability of the proposed method before the implementation is a novel contribution.

For this purpose, qualitative analysis approach has been used. In this context, the interviews with experienced subject matter experts were conducted, transcribed and results were analysed using a simplified conversation analysis (CA) method as an implementation of content analysis.

CA is an inductive, micro-analytic and predominantly qualitative method for studying human social interactions [36]. It is well established as a highly effective method for the investigation of interaction [37]. CA does not use reduced or coded set of representations; on the contrary, it includes casual and detailed conversation details which allow the analyst to identify different perspectives and subtleties that is not realized previously. The main goal of evaluating the methodology that was suggested in this study was better understanding the perspectives and experiences of subject expert matters. Consequently, the characteristics of CA match perfectly with the goal of the analysis of the methodology.

The conversational analysis process that was performed on the suggested methodology and case study is presented under three main stages:

- Subjects: The interviewee requirements were defined. The interviewees that were meeting the requirements and participated in this study were identified.
- Method: Details of how the conversational analysis methodology was performed.
- Results: Conversation results are analysed, and the analysis results are presented.

5.1 | Subjects

Determining the subjects – the interviewees – was the first step of conversational analysis. For this purpose, the following characteristics have been defined as the required qualifications of the subject candidates:

- Advance knowledge and experience in cyber security domain.
- Experience on team management or product management on cyber security domain.
- Has interest on SOC processes and technologies.

In accordance with these requirements, four of the candidates were determined as subjects to perform interview. The names and other personal information about the subjects were
The subjects are mentioned via abbreviations as S1, S2, S3 and S4 correspondingly in the rest of the report.

5.2 Method

As a methodology, conversational analysis is largely concerned with the analysis of the verbal communicative practices that people routinely use when they interact with one another [37]. Before the interviews were performed, this study was sent to subjects and sufficient time was provided for them to investigate the methodology and use case scenario. During the interviews, although the format of the interviews was unstructured and free-flowing conversation, couple of specific questions about the methodology was determined previously and such questions were used to start and to carry on the conversation. In this way, it was ensured that conversation was not diverged from the main topic and focus point of the conversation is assured throughout the interview.

The responses were then collected, translated by the authors and interpreted to make inferences.

5.3 Results

The results of conversations with subjects were interpreted and categorized as supportive comments and developmental comments. The supported comments were declaring that the suggested methodology is applicable, and it seems like a guiding resource for the future works in this subject as indicated by the excerpts:
S1: I see this approach as a promising methodology. After applying some improvements, this can be confidently used in any type of SOC organizations.

S2: When a technical concern occurs in the cyber security world, there is a good chance to find many resources to investigate. However, it is hard to find sufficient number of sources that focus on the management aspect of security operation teams. I think the reason is that the attack vectors are changing and improving rapidly, and security teams are using all their efforts to discover such new techniques and to adapt them. In any way, this study makes a good point as the problem it covers, and the methodology seems a guiding resource for future works.

S3: Maturity assessment and security metrics are the key points for understanding and controlling SOC organizations, which is the only way of improving it properly. In this connection, Six Sigma seems as a very good basis for continuous improvement process for SOC organizations.

S4: This methodology seems reasonable and applicable to my opinion.

In addition to supportive inferences, five major areas of concern were also identified by the interpretations of the interview results.

First of all, subjects S1, S2 and S4 have agreed about extending each phase of the methodology by defining roles and responsibilities of each SOC position in the CI process as indicated by the excerpts:

S1: Continuous improvement is a long-term and ongoing process. It includes many components, and it mostly requires the contribution of all members of the organization. If everyone in the team understands the importance of improvement process and aware of their roles and responsibilities in the process, then the success rate will be higher; otherwise, it is inevitable to face some interruptions or contingencies during improvement process.

S2: In business life, unassigned tasks or responsibilities can create some problems. Many people might try to work on the same issue, or no one wants to take that responsibility. Communication among team members is very important in order to overcome such problems. But more importantly, assigning the tasks to appropriate people before starting a new process can be very useful to prevent such possible problems proactively. This methodology can be improved by adding such definitions as well.

S4: I would like to understand which parts of this improvement process are in my responsibility. Which tasks should I assign to my team, and what kind of outputs will be expected from me by my managers?

In such way, applicability of the methodology can be increased which can result in better benefits from the improvement process.

In addition to defining roles and responsibility details, S1 also indicated that automation and orchestration has an important role in the improvement process:

S1: Automation is a very important concept for security operation teams. It is not always easy to answer the question ‘what to automate?’, but there are trending approaches or technologies that draw attention to this topic. For example, SOAR (Security Orchestration, Automation and Response) products. They aim to solve many possible problems in a SOC organization such as alert fatigue, hardship of using many security products together, communication problems or many other possible problems that I do not recollect right now. The methodology should not be focusing on improving the products or processes that currently exist, but it should be also focusing on the importance of automation and orchestration.

SOAR platforms are increasing their popularity in security operations domain by claiming to decrease alert fatigue, which results in more available time for security analysts to focus on most important alerts in the system. As suggested by S1, the methodology can be extended with placing SOAR technology in it. In such way, the methodology – especially the maturity assessment part – can provide inputs to SOAR about primary automation points. In return for this, the automation processes can increase the efficiency and effectiveness of the SOC services, which results in a mutual advantage between two concepts.

As another concern, S1 and S2 stated their concerns about the business aspect of the methodology as indicated by the excerpts:

S1: The scope is limited with the technical perspective of the problem. Excluding the business perspective could be very useful or misleading depending on the situation. It could be a good idea to study the same problem in business perspective in the future. In this way, the results can be compared, and the methodology can be improved.
S2: As an executive, I have to think about the business side of improvement procedure as well. Extending this methodology in business perspective would provide depth to it.

The scope of this study was limited with technical aspects of the problem. The interview results showed that the business aspect of the problem could be studied in terms of improvement, and the methodology could be extended in such manner as well.

Another concern that was stated in the interviews was about simplicity of case study.

S1: Measuring the effectiveness and efficiency of such extensive methods is not easy. A good option would be studying a detailed case study which covers all the services in the organization including completing all challenging tasks such as implementing risk assessment or defining cause-effect diagrams.

S3: I would really like to see an example of fully covered case study. It would be useful to evaluate it more easily.

S1 and S3 has declared that a fully covered case study on an active SOC team should be performed in order to measure effectiveness and efficiency of the methodology.

Finally, S4 has stated his concerns about the service-based approach to the problems as indicated in the following excerpt:

S4: This methodology seems to be defined with a service-based improvement approach. The interactive relations between services are already mentioned in the methodology briefly, but it could be more complicated than expected in some situations.

Although possible effects of improving one service over other services was briefly mentioned in this study, it can be concluded that this interactive relation could create some problems during in the implementation phase. Therefore, the relationship diagram for SOC services can be created and the methodology should be reviewed by assessing such interrelationship diagram to prevent possible problems in implementation period.

In summary, the interviews revealed that this study provides a promising methodology for the future. It is described by the interviewees as a complementary and comprehensive methodology which forms a basis for the future studies in this specific domain.

Additionally, the interviews also revealed that there are some concerns that need to be studied as well in order to improve the methodology. Those concerns were interpreted and presented under five main topics. The first concern was about the roles and responsibilities of SOC members in the CI process. The second was automation and orchestration of the technology core of the organization. The third concern was implementing a fully covered case study to measure the effectiveness of the methodology. The fourth concern was about the business aspect of the methodology. And the last concern was about the service-based improvement approach of the methodology.

6  |  CONCLUSION

The originality of this study is based on the presence of limited research in maturity assessment and CI practices on SOC organizations. The main goal of this study was to suggest a complementary methodology to combine both approaches by answering ‘what to improve’ and ‘how to improve’ in an SOC. For that purpose, a CI methodology suggested by capability and maturity assessment results has been developed.

This study can be summarized under two topics, assessment and improvement. For the assessment part, while the maturity model which was suggested by Van Os has limitations in terms of applicability to be used as a CI model, the updated version of it was suggested by this study in order to overcome that problem by offering a service-oriented improvement model. For the improvement part, DMAIC methodology of Six Sigma approach was used to provide new insight to SOC teams to detect and improve required capabilities confidently. Additionally, the methodology was illustrated with a use case scenario in order to support applicability of the methodology. Finally, the methodology is evaluated by interviewing subject matter experts on a use case scenario and analysing their response using CA method.

The evaluation results indicate that this methodology suggests a complementary and applicable perspective which can be used to increase organizational maturity. Consequently, it can be claimed that this methodology provides answers to research question of this study.

Although the results of evaluation were supporting the applicability of the methodology, this study has also limitations that need to be addressed in future research works. First of all, the effectiveness of the methodology was not measured in this study with quantitative data because of the difficulties in utilization of the methodology with real-life scenarios. Applying this methodology to a real SOC requires high volume of sensitive information which is challenging to collect and publish. Additionally, such study requires contribution of many people in an organization, high number of meetings and documentations. Therefore, such study is defined as a future work.

Another limitation of the methodology is directly related to limitation of Six Sigma from a problem-solving perspective [22]. When defining the target maturity and capability levels of the organization, the required and collected data to be interpreted is such as budget limitations for improvement, customer expectations and CTQ definitions. However, eventually, determining the target values is still based on subjective judgement of the stakeholders.
As it was discussed in the qualitative research results, the methodology can be extended with automation and orchestration (SOAR) technologies as a future work. Brewer has noted the importance of SOAR in SOC processes, and in his report, the possible benefits of SOAR to importance SOC skills has been discussed [38]. Additionally, Donevski and Zia has discussed using machine learning and automation to counter cyber security challenges, which could be a guiding paper to start studying on automation [39].

Another inference of the evaluation results was the concern about service-oriented architecture of the methodology. The scope of this study is limited with ‘IHR’ service. Separate literature research for other services in a SOC can be investigated and the methodology can be extended by defining other services. Additionally, the interrelationship diagram between SOC services could be studied and the methodology can be improved using such mapping.

As a final suggestion for future work, the methodology can be extended with defining roles and responsibilities of each position in the SOC in this CI process and it can also be improved by studying business perspective of the problem.

To conclude, although analysis results show that this study can be suggested as a guiding resource for the future searches in this domain, it is important to further expand the study to develop a more optimized methodology by conducting future works that are defined above.

**ORCID**

Cengiz Acartürk  https://orcid.org/0000-0002-5443-6868
Murat Ulubay  https://orcid.org/0000-0002-9775-5754
Efe Erdur  https://orcid.org/0000-0001-6896-0014

**REFERENCES**

1. Park, C.-S., Jang, S.-S., Park, Y.-T.: A study of effect of Information Security Management System (ISMS) certification on organization performance. Int. J. Comput. Sci. Netw. Secur. 10(3), (2010)
2. Nassar, P.B. et al.: Securing Collaborative Business Processes: A Methodology for Security Management in Service-Based Infrastructure. IFIP International Conference on Advances in Production Management Systems, pp. 480–487. Springer, Berlin, Heidelberg (2011)
3. Shah, A., Ganesan, R., Jaiodla, S.: A methodology for ensuring fair allocation of CSOC effort for alert investigation. Int. J. Inf. Secur. 18(2), 199–218 (2019)
4. Van Os, R.: SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers, Master Thesis, Information Security Program, Luleå University of Technology (2016)
5. Hewlett Packard Enterprise, Palo Alto, CA (2017). https://www.hpe.com/us/en/newsroom/press-release/2017/03/hewlett-packard-enterprise-report-reveals-trials-and-errors-of-security-operations.html
6. Judgev, K., Thomas, J.: Project management maturity models: the silver bullets of competitive advantage? Proj. Manag. J. 33(4), (2002)
7. Suryawanshi, C.P: Security operations center maturity – A step-by-step DIY guide. CACHE Peripherals Blogs (2019). https://blog.cacheperipherals.com/security-operations-center-maturity-a-step-by-step-diy-guide, http://www.cacheparipherals.com/blogposts.php?id=1
8. CREST. https://www.crest-approved.org/ -UK (2018). Accessed 28 June 2019
9. Aazadnia, M., Fasanghari, M.: Improving the information technology service management with six sigma. Int. J. Comput. Sci. Netw. Secur. 8(3), (2008)
10. Lindberg, P., Berger, A.: Continuous improvement: design, organisation and management. Int J Technol. Manag. 14(1), 86–101 (1997)
11. American Society for Quality: Continuous improvement. Quality Resources, [Online]. Available: https://asq.org/quality-resources/continuous-improvement American Society for Quality; (2020).
12. de Mast, J., Lokkerbol,: An analysis of the Six Sigma DMAIC method from the perspective of problem solving. Int. J. Prod. Econ. 604–614 (2012)
13. Sokovic, M., Pavletic, D., Pipan, K.K.: Quality improvement methodologies – PDCA cycle, RADAR matrix. J. Achiev. Mater. Manuf. Eng. 43(1), 474–483 (2016)
14. De Bruin, T., et al.: Understanding the main phases of developing a maturity assessment model. In: Australasian Conference on Information Systems (ACIS), Sydney. (2005)
15. OWASP: SOC - Security Operations Centers Framework Project. OWASP The Open Web Application Security Project. https://www.owasp.org/index.php/OWASP_Security_Operations_Center_SOC_Framework_Project (2019).
16. Jacobs, P., Amalz, A., Irwin, B.: Classification of Security Operations Centers. Proceedings of the Information Security for South Africa, pp. 1–7. IEEE (2013). https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6641054
17. Wichman, J: 3 Key Ways To Improve Your Incident Response. Blog. https://www.optiv.com/blog/3-key-ways-improve-your-incident-response. Explore Optiv Insights. OPTIV (2018). https://www.optiv.com/explore-optiv-insights/blog/3-key-ways-improve-your-incident-response
18. Brown, W., et al.: Security automation and orchestration briefing. https://www.optiv.com/sites/default/files/2018-09/ScurityAutomation_TechnologyPartnerReview.pdf Technology and Partner Review. OPTIV (2018). Accessed 15 November 2019 https://www.optiv.com/sites/default/files/2020-07/ScurityAutomation_TechnologyPartnerReview.pdf
19. CyberSponse.: 5 ways to improve your cybersecurity incident response plan. https://cybersponse.com/5-ways-to-improve-your-cyber-security-incident-response-plan/ (2018) https://t.co/nriCTFOPza?amp=1
20. Holloran, D: How to improve incident management: trust the process. Blog. https://victorops.com/blog/how-to-improve-incident-management-trust-the-process. VictorOps (2018). https://victorops.com/blog/how-to-improve-incident-management-trust-the-process
21. Kwaka, Y.H., Anbari, F. T.: Benefits, obstacles, and future of Six Sigma approach. Technovation. 26, 1–8 (2006)
22. Antony, J.: Six Sigma for service processes. Bus. Proc. Manag. J. 12(2), 234–248 (2006)
23. Zimmerman, C.: Ten Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation, Bedford, MA (2014). https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf
24. Jüni, A.C.P., et al.: Project stakeholder management: a case study of a Brazilian Science Park. J. Technol. Manag. Innovat. 10(1), (2015)
25. Singh, B.J., Khanduja, D.: Essentials of D-phase to secure the competitive advantage through Six Sigma. Int. J. Bus. Excell. 5(1/2), (2012)
26. Savola, R.M.: Quality of security metrics and measurements. Comput. Secur. 37, 78–90 (2013)
27. Ruefle, R., et al: Computer security incident response team development and evolution. IEEE Secur. Priv. Mag. 12(5), 16–26 (2014)
28. Kime, B: Cyber Threat Intelligence Support to Incident Handling. SANS Institute Information Security Reading Room. SANS Institute (2017). https://www.sans.org/reading-room/whitepapers/threatintelligence/cyber-threat-intelligence-support-incident-handling-30150
29. Futterer, S., Elshehawy, A.K.: Implementation of TQM and Lean Six Sigma tools in local government: a framework and a case study. Total Qual. Manag. Bus. Excell. 16(10), 1179–1191 (2005)
30. Chinigai, C., Dafaoui, E.-M., Mhamedi, A.E.: An approach for enhancing process and process interaction capability. In: 19th International Conference on Production Research, pp. 1–6. (2007)
31. Nedra, A., et al.: A new Lean Six Sigma hybrid method based on the combination of PDCA and the DMAIC to improve process performance: application to clothing SME. Ind. Text. 70(5), 447–456 (2019)
32. De Koning, H., De Mast, J.: A rational reconstruction of Six Sigma’s breakthrough cookbook. Int. J. Qual. Reliab. Manag. 7, 766–787 (2006)
33. Souppaya, M., Scarfone, K.: Guide to Malware Incident Prevention and Handling for Desktops and Laptops. NIST Special Publication 800-83 Revision 1, Computer Security, National Institute of Standards and Technology, U.S. Department of Commerce (2013). https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-83r1.pdf
34. Batal, L.M.B., Kifor, C. V., Bondrea, L.: Assessing the impact of DMAIC-knowledge management methodology on Six Sigma projects: an evaluation through participant's perception. In: Knowledge Science, Engineering and Management, pp. 349–356. Springer International Publishing (2014)
35. Dumitrescu, C., Dumitrache, M.: The impact of Lean Six Sigma on the overall results of companies. Econ. Seria Manag. 14(2), 535–544 (2011)
36. Hoey, E.M., Kendrick, K.H.: Conversation analysis. In: Research Methods in Psycholinguistics: A Practical Guide. (2017)
37. Chatwin, J.: Conversation analysis as a method for investigating interaction in care home. Dementia. 13(6), 37–746 (2014)
38. Brewer, R.: Could SOAR save skills-short SOCs? Comput. Fraud. Secur. 2019(10), 8–11 (2019)
39. Donevski, M., Zia, T.: A survey of anomaly and automation from a cybersecurity perspective. In: 2018 IEEE Globecom Workshops (GC Workshops). (2018)

How to cite this article: Acartürk C, Ulubay M, Erdur E. Continuous improvement on maturity and capability of Security Operation Centres. IET Inf. Secur. 2021;15:59–75. https://doi.org/10.1049/ise2.12005