Textbook for security response organisation（SOC/CSIRT）

～ using X.1060 ～

Ver. 3.2.1 (en)

2025.10.17

NPO Japan Network Security Association (JNSA)
Information Security Operation providers Group Japan (ISOG-J)

© 2025 ISOG-J

Revision history

2016/11/25	Ver.1.0
2017/10/03	Ver.2.0
2018/03/30	Ver.2.1
2023/2/13	Ver.3.0 ・align with ITU-T recommendation X.1060
2023/10/17	Ver.3.1
2024/10/17	Ver.3.2
2025/10/17	Ver.3.2.1 (en) English version

Disclaimer

- The copyright of this document belongs to the Information Security Operation providers Group Japan (ISOG-J).
- Quotations are permitted under the Copyright Law to the extent that they are justifiable for the purpose of quotation. The quoted portion should be clear and the source clearly indicated, for example.
- In cases where the quotation is believed to exceed the permitted scope, **ISOG-J may be contacted** at info(at)isog-j.org.
- Company names, product names, and service names appearing in this document are generally registered trademarks or trademarks of the respective companies. The ®, TM and © marks are not indicated in this document.
- Neither ISOG-J nor the authors assume any responsibility for this guide document. Use at your own risk.

© 2025 ISOG-J

Table of Contents

Executive Summary 1
1. Introduction 3
2. Purpose of a Security Response Organisation 5
  2.1. Defining "Security Response Organisation"? 5
  2.2. The Significance of Security Response Organisations 7
  2.3. The Role of Security Response Organisations 8
  2.4. Practical examples 11
  2.4.1. Examples of security response organisations in Japan 11
  2.4.2. The Necessity of Security Response Organisations in the Supply Chain 14
3. Cycle of security response organisations 18
  3.1. Overall view of the cycle 18
  3.2. Building a security response organisation 20
  3.2.1. Overview of the build process 20
  3.2.2. Define a service catalogue 21
  3.2.3. Define a service profile 23
  3.2.4. Define a service portfolio 24
  3.3. Management of security response organisations 25
  3.3.1. Overview of management process 25
  3.3.2. Phases and cycles in the management process 26
  3.4. Evaluation of security response organisations 29
  3.4.1. Overview of evaluation process 29
  3.4.2. Gap analysis and review 30
  3.4.3. Examples of timing of review 30
4. Categories in security response organisations 33
  4.1. Overview of categories 33
  4.2. Categories in cycles of CDC management process 33
5. Services in security response organisations 36
  5.1. Overview of the services 36
  5.2. CDC/CSC service recommendation level 41
  5.2.1. Consideration of Recommendation Levels in X.1060 41
  5.2.2. Examples of how services are selected 42
6. Service assignment and structure for security response organisation 45
  6.1. Relationship between SOC, CSIRT and services in Japan so far 45

© 2025 ISOG-J

6.2.Approach to role assignment in security response ... 47
6.3.Organisational pattern for security response ... 50
6.4.Service assignment for security response ... 51
6.5.Structure of security response organisation ... 53
6.5.1. Example for flat structure organisation ... 53
6.5.2. Example of general pattern for assignment on X.1060/JT-X1060 ... 55
6.6.Number of members for security response organisation ... 57
7. Relations between categories and services ... 60
7.1.Flow in incident response ... 61
7.1.1. Example: “Damage caused by ransomware” ... 65
7.1.2. Example: "Theft of personal information from web services" ... 66
7.1.3. Example: ”Incident in the supply chain” ... 68
7.2.Activities during normal operations ... 69
7.2.1. Vulnerability management（e.g., patch application） ... 70
7.2.2. Event analysis ... 70
7.2.3. Awareness and training ... 71
7.2.4. Alerts and advisories ... 72
7.2.5. Other incident-related activities (e.g., drills and simulations) ... 73
8. Security response organisation assessment ... 74
8.1.Purpose of assessment ... 74
8.2.Assessment workflow ... 75
8.3.Service scores ... 75
8.4.Service portfolio sheet for security response organisation ... 77
8.5.Service portfolio self-check sheet for security response organisation ... 77
9. at the end ... 82
References ... 82
Appendix 1 Categories and service list ... 83
Category ... 83
A. strategic management of CDC/CSC ... 83
B. real-time analysis ... 83
C. deep analysis ... 83
D. incident response ... 83
E. checking and evaluation ... 83
F. collection, analysis and evaluation of threat intelligence ... 83
G. development and maintenance of CDC/CSC platforms ... 84
H. support of internal fraud response ... 84

© 2025 ISOG-J

I. active relationship with external parties 84
service list 85
A. Strategic management of CDC/CSC 85
B. Real-time analysis 89
C. Deep analysis 91
D. Incident response 92
E. Checking and evaluation 95
F. Collection, analysis and evaluation threat intelligence 98
G. Development and maintenance of CDC platforms 100
H. Support of internal fraud response 105
I. Active relationship with external parties 106
Appendix 2 handbook for self-assessment 108
Appendix 3 mapping to FIRST CSIRT Services Framework ver.2.1.0 109

© 2025 ISOG-J

Executive Summary

The "Textbook for Security Response Organisations" (hereinafter referred to as "this document") is a comprehensive resource that organises a wide range of cybersecurity activities and responsibilities, focusing on how an organisation can establish and maintain an effective security structure. The series of security-related activities outlined in this document encompass several key areas: preventive measures conducted routinely to manage risk and prevent incidents, monitoring to detect early signs of potential incidents, and processes for containment and rapid response to prevent incident escalation.

For these activities to be effective, coordination with various departments and partner organisations is essential, in addition to the Security Operations Centre (SOC) for monitoring and the Computer Security Incident Response Team (CSIRT), which plays a central role in incident response.

This document defines "Security Response Organisation" as an entity that oversees and orchestrates this comprehensive set of security activities across the organisation. This term is synonymous with the "Cyber Defence Centre/Cyber Defence Centre(CDC/CSC)" defined in the international standard ITU-T Recommendation X.1060/JT-X1060, which incorporates Japanese-developed expertise and practices.

The Ministry of Economy, Trade and Industry's "Cybersecurity Management Guidelines Ver3.0" explicitly states that it is a corporate social responsibility and a managerial duty to embed cybersecurity risks within organisational management, evaluate these risks, and to mitigate them to an acceptable level. Under corporate governance, a consistent and robust approach to security is required.

This guidance addresses not only incident preparedness, as outlined in the "Directives 7 and 8" of the Cybersecurity Management Guidelines, but also the establishment of governance-based management systems (referenced in "Directives 1, 2, and "3"). Furthermore, this guidance supports comprehensive supply chain security measures (as per "Directive 9"), serving as a procedural reference in line with the international standards set forth by X.1060/JT-X1060. This facilitates its adoption as a common language both within organisations and across corporate and global boundaries.

Contributors to this document included security professionals who support client security activities as well as those responsible for internal security initiatives. Their collective knowledge and expertise from the industry have been incorporated into this version. It is hoped this document will contribute to enhancing the security activities within your organisation.By leveraging this document, practitioners and executive

© 2025 ISOG-J

management, can establish a strategically oriented organisational framework for comprehensive cybersecurity practices.

© 2025 ISOG-J

1. Introduction

In the contemporary business environment, addressing cybersecurity has become essential for all organisations. Common terms such as CSIRT (Computer Security Incident Response Team) and SOC (Security Operations Centre) are often used to refer to security response organisations, yet the actual structure and responsibilities vary from one organisation to another, making a universal definition challenging. However, from a broader perspective, there are many shared principles and approaches regarding cybersecurity that transcend organisational boundaries, providing a foundation for how entities should strategize and implement security measures.

The "Textbook for Security Response Organisations" was first published in 2016 to organise and provide guidance on various security-related tasks—such as incident response, security operations, and vulnerability assessments—that were often addressed separately at the time. This document offered a comprehensive direction for organisations, including guidance on whether to insource or outsource, to address cybersecurity in a holistic manner. Subsequently, it was updated to Version 2.0 in 2017 (and Version 2.1 in 2018) to incorporate concepts of maturity and self-assessment tools, enabling organisations to elevate their cybersecurity response as a continual effort. As a result, this textbook has been referenced in official guidelines, such as the Ministry of Economy, Trade and Industry's "Cyber-Physical Security Measures Framework" and the Information-technology Promotion Agency's (IPA, Japan) "Practices for Implementing Cybersecurity Management Guidelines Ver 2.0." It also served as a valuable resource for establishing and operating cybersecurity organisations for events like the Tokyo 2020 Olympics and Paralympics[1][2].

The content of this document was further reviewed by the International Telecommunication Union's Standardization Sector (ITU-T), and many of its key concepts were adopted into ITU-T Recommendation X.1060 ("Framework for the creation and operation of a cyber defence centre"), which was recognised as an international standard in 2021. Its Japanese version has been published domestically as "JT-X1060" by the Telecommunication Technology Committee (TTC).

---

[1] ONISHI Masaki, HOSODA Naofumi, NAKANISHI Katsuhiko, IBAYASHI Hiroaki: "Cyber Security Operations for the Tokyo 2020 Games", The journal of institute of electronics, information and communication engineers, Vol. 105 No.8pp. 1035-1041 (2022-8)

[2] TAKEI Shigenori: "Applying a Reference Document of the Organisational Structure for Cyber Security Operation", The journal of institute of electronics, information and communication engineers, Vol. 105 No.8pp. 1054-1056 (2022-8)

The X.1060/JT-X1060 provides a framework for constructing and managing a Cyber Defence Centre/Cyber Security Centre (CDC/CSC) as a central entity responsible for managing cybersecurity risks within an organisation's business activities.

Reflecting this move toward international standardization, ISOG-J has revised the "Textbook for Security Response Organisations" to Version 3.0, incorporating new insights from the X.1060 to make it an even more practical guide for effective security response. As noted, the ideal structure for a security response organisation differs among entities; however, it is hoped that this textbook serves as a guide to help organisations build their security framework strategically and systematically, without having to rely on trial and error.

The following perspectives, categorised by role, may offer new insights:

Executives and Senior Management

This document aids in understanding the full scope of security functions, supporting their managerial decisions on whether to insource or outsource these functions. Additionally, the self-assessment results can help you gauge your organisation's current level of security response and serve as a reference for developing your next security strategy.

Managers

This document helps in understanding the various services needed for security response, providing insights into implementing specific services within the organisation and enhancing collaboration across departments. This document also includes recommendations for staffing levels for highly specialized security functions, which may help in communicating these needs to senior leadership.

On-the-Ground Personnel

Whether you work as part of a CSIRT, as a SOC operator, as a cloud or network system administrator, or as a vulnerability assessor, personnel in these roles are encouraged you to consider where your role fits within the broader security response framework and the mission it entails. This document can also provide insights for your career planning, helping you decide whether to continue in your current role or pursue other opportunities in the future.

This document aims to contribute to enhancing the security response capabilities of each company and organisation and that it helps elevate their level of cybersecurity readiness.

© 2025 ISOG-J

2. Purpose of a Security Response Organisation

2.1. Defining “Security Response Organisation”?

This section defines the term "Security Response Organisation." While this term has been used since Version 1.0 of this document, it has not been strictly defined. For example, the "Introduction" section in Version 1.0 describes it as follows:

> This document, the ″Textbook for Security Response Organisations,″ summarises the necessary functions, roles, and personnel required within security response organisations, such as the Security Operation Centre (SOC) and the Computer Security Incident Response Team (CSIRT).

The intention here was to use "Security Response Organisation" as an overarching term encompassing various security-related organisational functions, with CSIRT and SOC as representative examples.

Now, how is this nuance expressed within the international standard "X.1060"? It is defined as "CDC/CSC (Cyber Defence Centre/Cyber Security Centre)" in the following way:

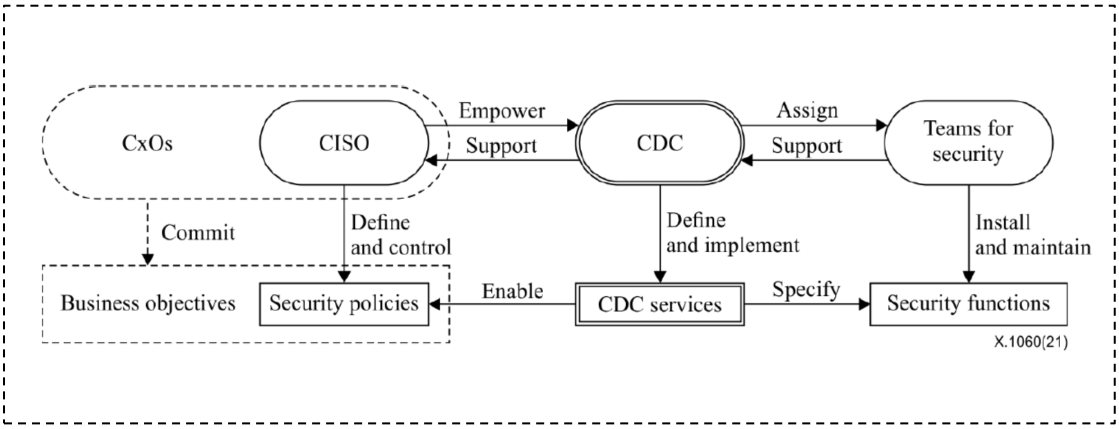
> cyber defence centre (CDC): An entity within an organisation that offers security services to manage the cybersecurity risks of its business activities.

This description may be challenging to understand intuitively. To clarify its meaning, the concept is explained further below. The "X.1060/JT-X1060" standard explains the concept of a CDC/CSC using the following conceptual diagram[3].

---

[3] International Telecommunication Union Telecommunication Standardization Sector (ITU-T) recommendation X.1060 “Framework for the creation and operation of a cyber defence centre”
https://www.itu.int/rec/T-REC-X.1060-202106-I

© 2025 ISOG-J


CxOs
CISO
Empower
Support
CDC
Assign
Support
Teams for security
Commit
Define and control
Define and implement
Install and maintain
Business objectives
Security policies
Enable
CDC services
Specify
Security functions
X.1060(21)

A CDC/CSC (Cyber Defence Centre/Cyber Security Centre) operates under the direction of the CISO, with the role of identifying the necessary CDC/CSC services[4] for the organisation and ensuring their implementation by the security team[5] to uphold the organisation's security policies. Below are two key points illustrated by this diagram.

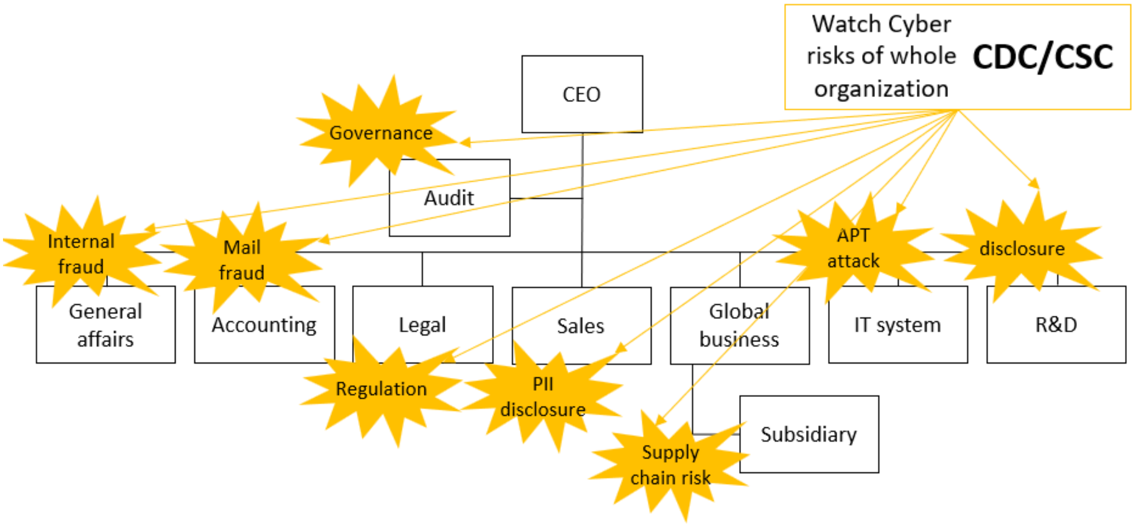

Watch Cyber risks of whole organization
CDC/CSC
CEO
Governance
Audit
Internal fraud
Mail fraud
APT attack
disclosure
General affairs
Accounting
Legal
Sales
Global business
IT system
R&D
Regulation
PII disclosure
Supply chain risk
Subsidiary

Figure 1: Cyber risks spread across the organisation and the role of the CDC/CSC

A CDC/CSC operates under the direction of the CISO, with the role of identifying the necessary CDC/CSC services for the organisation and ensuring their implementation by the security team to uphold the organisation's security policies.

---

[4] CDC services can be more easily understood when interpreted as "various security-related tasks."

[5] The security team refers to on-the-ground personnel in each department who handle practical security-related tasks.

Two key points are illustrated by this diagram:

1. The CDC/CSC serves as an overarching entity that coordinates all cyber security efforts within the organisation. As shown in Figure 1, cyber risks are dispersed throughout the organisation and must be addressed with a comprehensive, high-level perspective.
2. It is not necessary to establish the CDC/CSC as a new department or team. Most companies already have some form of structure in place to plan and implement cyber security measures, regardless of the size or format of these entities. Representative examples include CSIRTs and SOCs.

From these two points, the concept of the CDC/CSC encompasses a broader scope, including CSIRTs and SOCs, which implement various security tasks (CDC/CSC services) within the organisation. In other words, the CDC/CSC, as defined, is equivalent to what this document has referred to as a "Security Response Organisation." Therefore, this document will continue to use the term "Security Response Organisation."

While this document takes a bottom-up approach by organizing the tasks of CSIRTs and SOCs, "X.1060/JT-X1060" adopts a framework based on a top-down, overarching perspective. In the following chapters, the document will reorganize the overall picture of "Security Response Organisations," incorporating this overarching perspective to address their construction and management comprehensively.

2.2. The Significance of Security Response Organisations

The motivations for establishing a security response organisation, including SOCs and CSIRTs, vary by company. These motivations might include responding to an information leakage incident, following the example of industry peers, a directive from an executive, pressure from a parent company or regulatory body, or the promotion of digital transformation. Similarly, the organisational positioning of a security response organisation also differs, ranging from being directly under the CEO, operating as an independent department, or being a subunit within a specific division.

The diversity in these structures stems from differences in each company's business strategies and their respective security strategies. Consequently, there is no single uniform model for a "security response organisation," leading to challenges in consolidating best practices and systematically acquiring the knowledge necessary to implement effective security responses.

© 2025 ISOG-J

On the other hand, there are commonalities among security response organisations. Their shared objective is "reducing and appropriately managing security risks in business operations." When such risks materialize, they are referred to as "incidents." To achieve risk reduction, security response organisations generally share two key responsibilities:

- ✧ **Prevention of incident occurrence**
- ✧ **Minimization of damage in the event of an incident**

Achieving these objectives is the common purpose of all security response organisations. However, as organisations promote digital transformation and the scope of assets requiring protection expands, it is crucial to avoid extreme security measures that compromise productivity and flexibility, which could negatively impact organisational performance.

Traditionally, information security has focused on maintaining "CIA" (Confidentiality, Integrity, Availability). However, when considering security across the entire organisation, it becomes equally important to protect "CPA" (Creativity, Productivity, Agility) in the context of business operations.

2.3. The Role of Security Response Organisations

Throughout this document, the Cyber Defence Centre/Cyber Security Centre (CDC/CSC) defined in X.1060/JT-X1060 is referred to as the security response organisation. In X.1060/JT-X1060, the organisational positioning is illustrated in the following diagram.

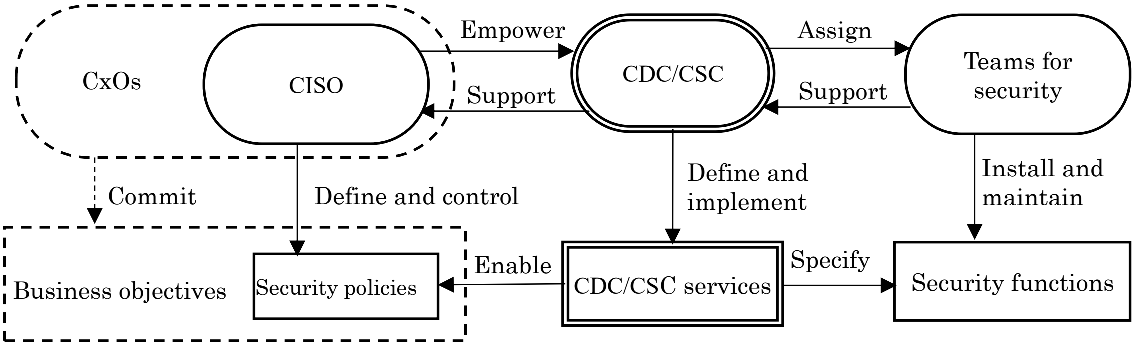

CxOs
CISO
Empower
Support
CDC/CSC
Assign
Support
Teams for security
Commit
Define and control
Define and implement
Install and maintain
Business objectives
Security policies
Enable
CDC/CSC services
Specify
Security functions

Figure 2: Stakeholders and Their Roles in the Operation of the CDC/CSC as Defined in X.1060/JT-X1060 [6]

---

[6] ITU-T recommendation X.1060 “Framework for the creation and operation of a cyber defence centre”, Figure 1

© 2025 ISOG-J

In X.1060/JT-X1060, the creation and operation of the CDC/CSC are defined using a simplified organisational structure as an example, with the CDC/CSC positioned at the centre of the diagram.

In practice, the establishment of a security response organisation begins with the executive management and CISO, represented on the left side of the diagram, considering cybersecurity as part of business risk and making decisions on the appropriate response.

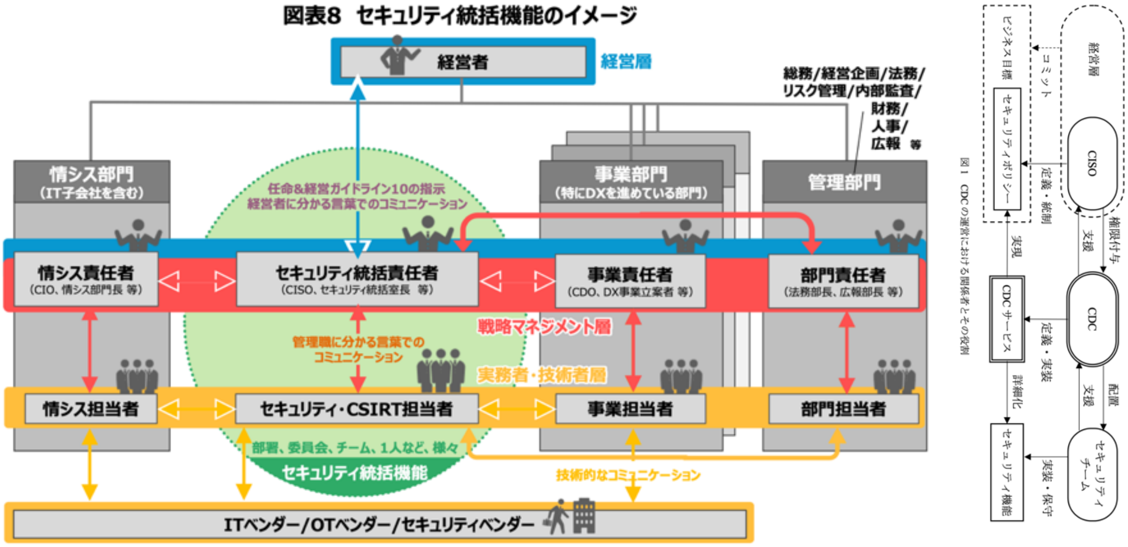

図表8　セキュリティ統括機能のイメージ
経営者
経営層
総務/経営企画/法務/リスク管理/内部監査/財務/人事/広報 等
情シス部門（IT子会社を含む）
事業部門（特にDXを進めている部門）
管理部門
任命&経営ガイドライン10の指示
経営者に分かる言葉でのコミュニケーション
情シス責任者（CIO、情シス部門長 等）
セキュリティ統括責任者（CISO、セキュリティ統括室長 等）
事業責任者（CDO、DX事業立案者 等）
部門責任者（法務部長、広報部長 等）
戦略マネジメント層
管理職に分かる言葉でのコミュニケーション
実務者・技術者層
情シス担当者
セキュリティ・CSIRT担当者
事業担当者
部門担当者
部署、委員会、チーム、1人など、様々
セキュリティ統括機能
技術的なコミュニケーション
ITベンダー/OTベンダー/セキュリティベンダー
経営層
CISO
CDC
セキュリティチーム
コミット
定義・統制
権限付与
支援
定義・実装
配置
支援
実装・保守
ビジネス目標
セキュリティポリシー
実現
CDCサービス
詳細化
セキュリティ機能
図1　CDCの運営における関係者とその役割

Figure 3: Concept of Security Oversight Functions in the Cybersecurity Management Guidelines[7]

A concept comparable to the positioning of the CDC/CSC in Japan can be found in the Cybersecurity Management Guidelines Ver3.0 by the Ministry of Economy, Trade and Industry. Appendix F, "Guidelines for Establishing a Cybersecurity System and Securing Human Resources," includes Figure 8, which illustrates the security oversight functions of the Security Oversight Office.

---

https://www.itu.int/rec/T-REC-X.1060-202106-I

[7] Modified "Cybersecurity Management Guidelines Ver.3.0 Annex F Guidance for establishing a cybersecurity system and securing human resources Ver 2.0" （Ministry of Economy, Trade and Industry） （https://www.meti.go.jp/policy/netsecurity/mng_guide.html） Right side figure is from Fig.1 JT-X1060(TTC)

Executive management views cybersecurity as one of the business risks to address. To that end, they prioritise cybersecurity measures alongside other risks and decide on the appropriate responses. The CISO establishes the security response organisation to implement these measures, defines the policies as part of the security strategy, and delegates authority to enable the execution of various security responses.

Executive management must also quantitatively measure the effectiveness of the implemented security measures and evaluate their contribution to the overall business. Examples of how to demonstrate their impact on business indicators include the JNSA CISO Handbook and the CISO Dashboard.

Once the decision to establish a security response organisation is made, services are defined and assigned based on the guidelines in X.1060/JT-X1060. However, in practice, there may be cases where a parent-subsidiary relationship exists, or multiple business divisions have their own SOCs or CSIRTs. In the construction chapter of this document, the process begins with the simplified organisational structure presented in X.1060/JT-X1060.

On the right side of Figure 2, the security team is shown. The security team is assigned services defined by the CDC/CSC and is responsible for their implementation, maintenance, and operations. Naming the team that performs these services—such as SOC or CSIRT–depends on the specific practices of each organisation. In some cases, the security response organisation itself may also be referred to as SOC or CSIRT.

In X.1060/JT-X1060, specific operational procedures for the security team are not addressed. This aspect is instead covered by various existing guidelines and manuals[8] that provide instructions for specific tasks. X.1060/JT-X1060 defines the services that comprise an organisation's overall security, but the detailed operations and procedures can refer to these existing resources.

Organisations that have already established their operations and procedures can use them as a basis to map which services they are currently performing and identify gaps or areas for improvement.

---

[8] In Japan, there are various documents from JPCERT/CC and the Nippon CSIRT Association, and overseas from FIRST, NIST, ENISA and various others related to security.

© 2025 ISOG-J

2.4. Practical examples

2.4.1. Examples of security response organisations in Japan

In Japan, security response organisations initially began with the establishment of CSIRTs as security teams dedicated to incident response and SOCs for incident monitoring. Over time, their scope of responsibilities expanded to include areas such as product management and preventive measures.

Each organisation or company has independently defined its own SOC or CSIRT operations, resulting in unique structures and responsibilities across different entities. Consequently, the activities undertaken by SOCs or CSIRTs vary widely among organisations. What matters most is not the name of the organisation but the actual tasks it performs.

Through their security response organisations, companies and organisations should strive to grasp the overall picture of the services and operations required for security. They should also clearly identify what security measures are implemented and what measures are not within their scope of operations.

To this end, utilizing X.1060/JT-X1060 and this document can provide a unified understanding of the full spectrum of security responsibilities and serve as a common language for discussing and managing security tasks.

Recently, it has become necessary to monitor and respond to incidents not only for internal organisational or corporate systems but also for systems supporting business operations managed by business divisions. In some companies, the scope of SOCs and CSIRTs has suddenly expanded due to factors such as subsidiary integration or M&A activities, requiring collaboration among multiple security response organisations. Regarding supply chains, collaboration may also extend beyond overseas branches to include the security response organisations of business partners.

In other words, while organisations initially operated with a single SOC or CSIRT managing internal security, today's landscape requires SOCs and CSIRTs to exist for each business division's services, coordinate between parent and subsidiary organisations, and collaborate with SOCs and CSIRTs across the supply chain and with business partners.

© 2025 ISOG-J

Given this environment, where SOCs and CSIRTs may already exist in various locations, there is a growing need for a top-down approach to security oversight. This requires a centralized organisation, such as a CDC/CSC or a security response organisation, to coordinate security efforts and provide support across these distributed entities.

As described above, the scope of security services, tasks, and organisational structures has become increasingly complex across various organisations.

Figures 10 and 11 in Appendix F of the Ministry of Economy, Trade and Industry's Cybersecurity Management Guidelines Ver3.0, "Guidelines for Establishing a Cybersecurity System and Securing Human Resources," classify security oversight functions and outline types of organisational placements within companies[9].

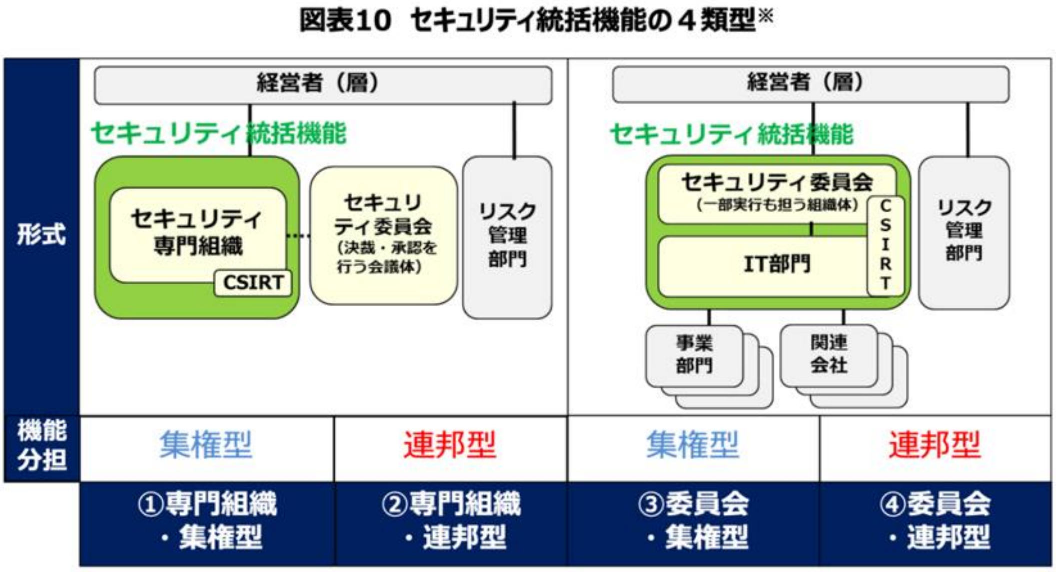

図表10　セキュリティ統括機能の４類型※
形式
経営者（層）
セキュリティ統括機能
セキュリティ専門組織
CSIRT
セキュリティ委員会（決裁・承認を行う会議体）
リスク管理部門
経営者（層）
セキュリティ統括機能
セキュリティ委員会（一部実行も担う組織体）
IT部門
CSIRT
リスク管理部門
事業部門
関連会社
機能分担
集権型
連邦型
集権型
連邦型
①専門組織・集権型
②専門組織・連邦型
③委員会・集権型
④委員会・連邦型

Figure 4: Cyber Security Management Guidelines four types of security oversight functions

Security oversight functions are categorized into four types in this framework, broadly divided into Specialized Organisational Type and Committee Type. If there is no existing department capable of assuming security oversight functions, the Specialized

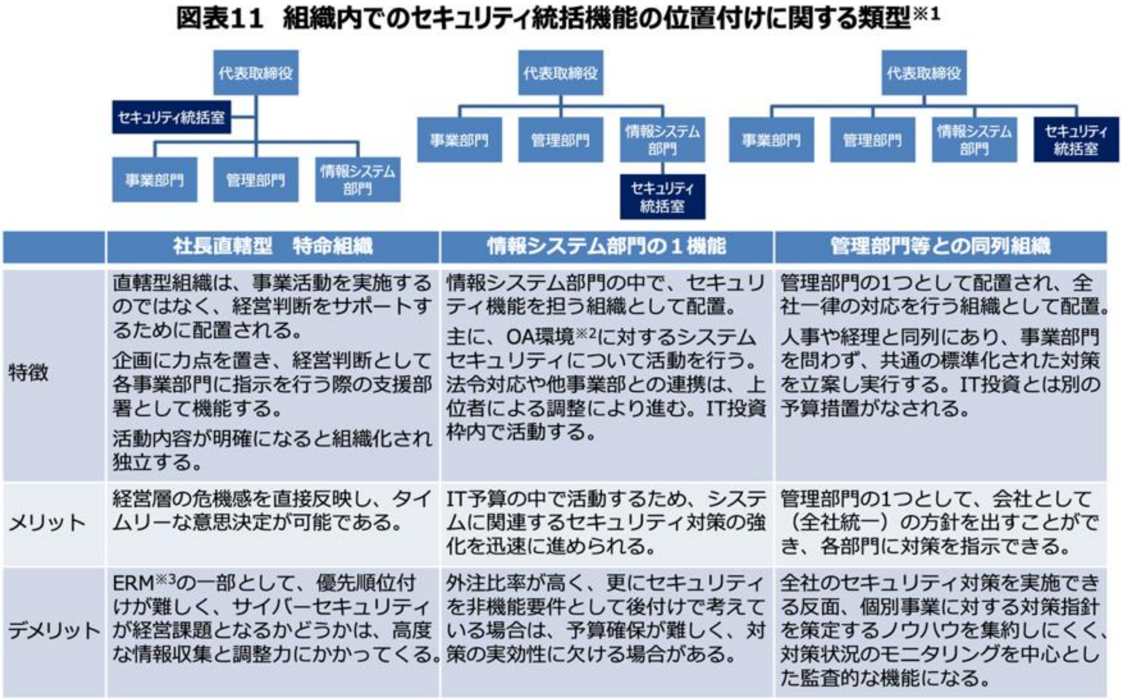
---

[9] From "Cybersecurity Management Guidelines Ver.3.0 Annex F Guidance for establishing a cybersecurity system and securing human resources Ver 2.0"（Ministry of Economy, Trade and Industry）, Figure 10 （https://www.meti.go.jp/policy/netsecurity/mng_guide.html）

© 2025 ISOG-J

Organisational Type is recommended, with Figure 11 illustrating how to establish such a structure.

In cases where an IT department or a similar unit already assumes some security oversight responsibilities, the Committee Type is suggested. This type divides security oversight functions between a security committee and the IT department.


代表取締役
セキュリティ統括室
事業部門
管理部門
情報システム部門
代表取締役
事業部門
管理部門
情報システム部門
セキュリティ統括室
代表取締役
事業部門
管理部門
情報システム部門
セキュリティ統括室

図表11　組織内でのセキュリティ統括機能の位置付けに関する類型※1

	社長直轄型　特命組織	情報システム部門の１機能	管理部門等との同列組織
特徴	直轄型組織は、事業活動を実施するのではなく、経営判断をサポートするために配置される。 企画に力点を置き、経営判断として各事業部門に指示を行う際の支援部署として機能する。 活動内容が明確になると組織化され独立する。	情報システム部門の中で、セキュリティ機能を担う組織として配置。 主に、OA環境※2に対するシステムセキュリティについて活動を行う。法令対応や他事業部との連携は、上位者による調整により進む。IT投資枠内で活動する。	管理部門の1つとして配置され、全社一律の対応を行う組織として配置。 人事や経理と同列にあり、事業部門を問わず、共通の標準化された対策を立案し実行する。IT投資とは別の予算措置がなされる。
メリット	経営層の危機感を直接反映し、タイムリーな意思決定が可能である。	IT予算の中で活動するため、システムに関連するセキュリティ対策の強化を迅速に進められる。	管理部門の1つとして、会社として（全社統一）の方針を出すことができ、各部門に対策を指示できる。
デメリット	ERM※3の一部として、優先順位付けが難しく、サイバーセキュリティが経営課題となるかどうかは、高度な情報収集と調整力にかかってくる。	外注比率が高く、更にセキュリティを非機能要件として後付けで考えている場合は、予算確保が難しく、対策の実効性に欠ける場合がある。	全社のセキュリティ対策を実施できる反面、個別事業に対する対策指針を策定するノウハウを集約しにくく、対策状況のモニタリングを中心とした監査的な機能になる。

Figure 5: Cyber Security Management Guidelines position of security oversight function[10]

Figure 11 in Appendix F of the Cybersecurity Management Guidelines outlines various placement models for establishing a specialized organisation, detailing the characteristics, advantages, and disadvantages of each type of structure.

When considering CDCs/CSCs or security oversight functions, the selection of services and the organisational structure will vary depending on the specific needs of each organisation. It is essential to recognise these differences and build a structure tailored to your organisation. In doing so, it is recommended to refer to X.1060/JT-X1060 and Appendix F of the Cybersecurity Management Guidelines Ver3.0.

---

[10] From “Cybersecurity Management Guidelines Ver.3.0 Annex F Guidance for establishing a cybersecurity system and securing human resources Ver 2.0”（Ministry of Economy, Trade and Industry）, Figure 11 （https://www.meti.go.jp/policy/netsecurity/mng_guide.html）

2.4.2. The Necessity of Security Response Organisations in the Supply Chain

In recent years, responding to attacks targeting supply chains has become an urgent issue. These attacks may exploit connections within organisations, such as between parent companies and subsidiaries or among overseas branches and offices. They may also target services and products through business partners, leading to widespread damage across the entire supply chain. Consequently, it is now essential to verify whether each company involved in the supply chain has implemented appropriate security measures.

At present, there are no specific guides or directives detailing the scope, responsibilities, and procedures for assessing supply chain risk management. The risks inherent to a company's group entities and its business partners naturally differ, as do the perspectives, scope of assessment, and the information that can be shared.

Currently, organisations are relying on existing frameworks and international standards related to internal security to define and assess items on a trial-and-error basis. However, these differences may lead to miscommunication regarding the measures in place and their level of maturity. To address this challenge, leveraging X.1060/JT-X1060 and this document is recommended. By doing so, stakeholders can align their understanding of the services, maturity levels, and organisational frameworks to ensure effective collaboration and accurate assessments.

■Perspective on Scope and Coverage

Consider the example of Company A Group:

Company A is a corporation consisting of multiple group companies and is responsible for managing and monitoring its internal infrastructure. Some overseas group companies have independently established their own internal infrastructure, which is connected to the broader network. Systems used to deliver services to customers by Company A and its group companies are built, operated, and monitored in compliance with Company A's and the group companies' security policies. However, some tasks,

© 2025 ISOG-J

including interactions with customers, are performed via Company A's internal infrastructure.

Company A Group has received a request from Company D as part of supply chain risk management to confirm the state of its security measures. The request covers not only the network environment for systems dedicated to Company D but also the security measures of Company A’s internal infrastructure. Furthermore, through an Attack Surface Management tool, observations have been made regarding the security measures of services provided to other customers by Company A and its group companies.

Addressing such a situation requires careful consideration and a structured approach.

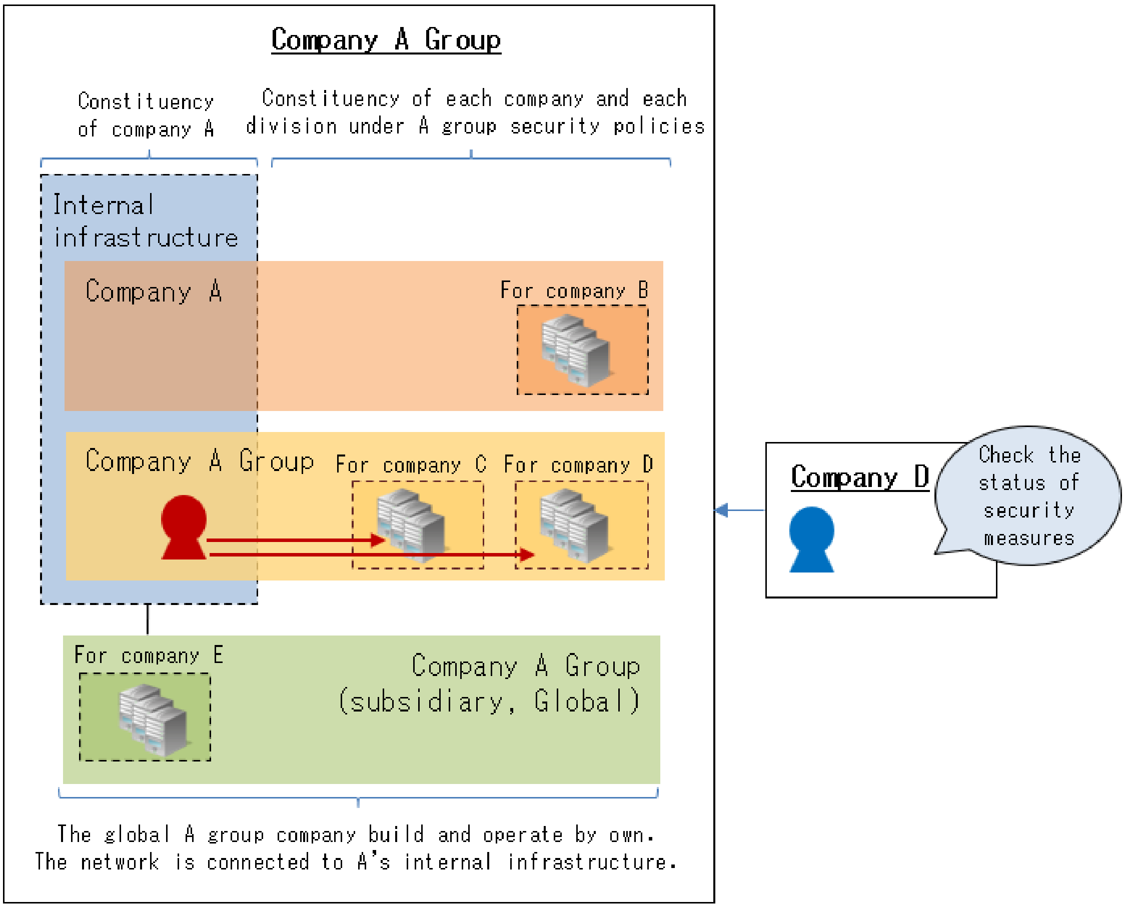

Company A Group
Constituency of company A
Constituency of each company and each division under A group security policies
Internal infrastructure
Company A
For company B
Company A Group
For company C
For company D
Company D
Check the status of security measures
For company E
Company A Group (subsidiary, Global)
The global A group company build and operate by own. The network is connected to A's internal infrastructure.

Figure 6: example of a scope of company A group

© 2025 ISOG-J

At present, there is no definitive solution to such a situation. Given that there are areas unclear to Company A Group alone, the security response organisation must collaborate with Company A Group to facilitate coordination.

For the systems and network environments related to Company D, it is naturally necessary to confirm the state of security measures. However, what about Company A's internal infrastructure? Since Company A Group companies utilize the same environment, there is a viewpoint that it should also be included as a confirmation target. However, determining how much of Company A's internal infrastructure to include, whether the scope should extend to the overseas group companies' infrastructure connected via the network, and addressing requests with varying scopes and ranges for each customer present practical challenges. Moreover, if the discussion extends to systems for other customers, Company A Group lacks the authority to make decisions and must adhere to confidentiality obligations, further complicating matters.

To address these challenges, it is essential to narrow down the scope of the targeted systems and networks. In this case, defining the security measures and monitoring in place for Company A's internal systems could validate that breaches in other customer systems or those within Company A's overseas group companies do not impact or minimally affect Company A. Such assurances could exclude these elements from the scope.

Additionally, if Company A states that it operates its SOC to monitor its internal infrastructure, discrepancies between "Company A's understanding" and "Company D's expectations" may arise. To address such situations, it is advisable to refer to categories such as Category G (as defined in X.1060/JT-X1060) to deepen mutual understanding regarding the service list and recommended levels.
For example, clarifying whether Company A's SOC monitoring focuses solely on networks, includes endpoints and cloud systems, has a platform for analyzing logs generated by products, and maintains a setup for detailed investigations could facilitate alignment. Verifying whether the systems related to Company D fall within the monitoring scope can also help ensure mutual understanding. Aligning both parties' perspectives enables more detailed discussions to proceed effectively.

© 2025 ISOG-J

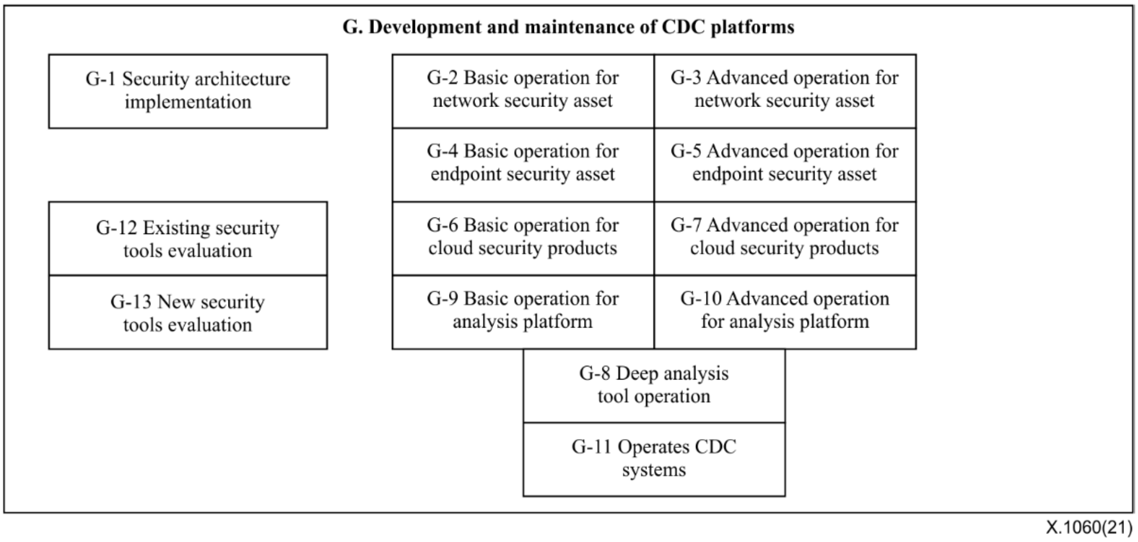

G. Development and maintenance of CDC platforms
G-1 Security architecture implementation
G-2 Basic operation for network security asset
G-3 Advanced operation for network security asset
G-4 Basic operation for endpoint security asset
G-5 Advanced operation for endpoint security asset
G-12 Existing security tools evaluation
G-6 Basic operation for cloud security products
G-7 Advanced operation for cloud security products
G-13 New security tools evaluation
G-9 Basic operation for analysis platform
G-10 Advanced operation for analysis platform
G-8 Deep analysis tool operation
G-11 Operates CDC systems
X.1060(21)

Figure 7: example of Category G

One of the benefits of X.1060/JT-X1060 is its ability to organize services, maturity levels, and organisational structures into a common language. This facilitates mutual understanding within the supply chain and aids in mapping connections and relationships while considering service lists and recommended levels.

The framework is also expected to be useful in building relationships with business partners, as referenced in the report issued by the Japan Fair Trade Commission, "Toward Building Partnerships with Business Partners to Enhance Cybersecurity Across the Supply Chain." [11]

Looking ahead, the development of systems such as a rating framework for evaluating organisational maturity would enable organisations to demonstrate their current security measures more universally. This would also accelerate the implementation of measures focused on supply chain security, fostering greater responsiveness and efficiency.

---

[11] Japan Fair Trade Commission, “Toward Building Partnerships with Business Partners to Enhance Cybersecurity Across the Supply Chain” https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html

© 2025 ISOG-J

3. Cycle of security response organisations

3.1. Overall view of the cycle

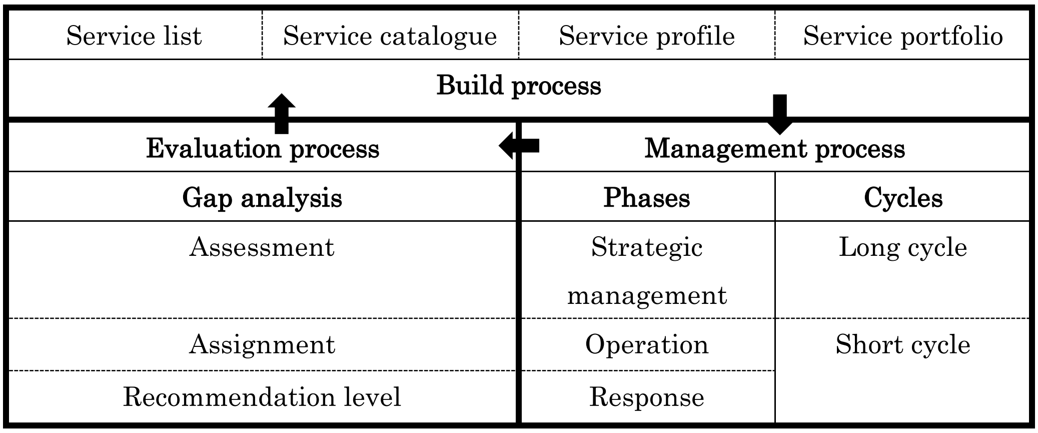
For companies and organisations, it is crucial to determine how to structure and launch a security response organisation and, further, how to continuously improve its operations. Addressing these challenges requires a practical approach. In response to such issues, this document leverages the X.1060/JT-X1060 framework to organize the cycle from planning and constructing a security response organisation to its operation.

The framework for constructing and operating a security response organisation as defined by X.1060/JT-X1060 is structured around three major processes:

- ✧ **Build process**
- ✧ **Management process**
- ✧ **Evaluation process**

The following diagram illustrates the activities conducted in each of these three processes and the relationships between them.

In X.1060/JT-X1060, the framework emphasizes continuous improvement by utilizing the results of the evaluation process to inform the subsequent construction process.



<table>
<tr><td>Service list</td><td>Service catalogue</td><td>Service profile</td><td>Service portfolio</td></tr>
<tr><td colspan="4">Build process</td></tr>
<tr><td colspan="2">Evaluation process</td><td colspan="2">Management process</td></tr>
<tr><td colspan="2">Gap analysis</td><td>Phases</td><td>Cycles</td></tr>
<tr><td colspan="2">Assessment</td><td>Strategic management</td><td>Long cycle</td></tr>
<tr><td colspan="2">Assignment</td><td>Operation</td><td rowspan="2">Short cycle</td></tr>
<tr><td colspan="2">Recommendation level</td><td>Response</td></tr>
</table>

Figure 8: Framework for the creation and operation of a Cyber defence centre[12]

Several terms related to services appear throughout this document, but their definitions

---

[12] ITU-T recommendation X.1060 "Framework for the creation and operation of a cyber defence centre", Figure 2
https://www.itu.int/rec/T-REC-X.1060-202106-I

© 2025 ISOG-J

may differ from those in other frameworks. To clarify:

When discussing IT-related services, readers might associate these terms with ITIL (Information Technology Infrastructure Library), a series of best practice guides for IT service management. In ITIL, a Service Catalogue refers to a list of currently offered services. A Service Portfolio includes not only currently offered services but also future potential services and those that have been discontinued.

However, the definitions in this document differ from ITIL's. For clarity, the specific definitions used throughout this document are provided below:

- Service List:
  - ➢ A list of services in the context of the security response execution cycle.
- Service Catalogue:
  - ➢ Using the service list and recommended levels determined by each organisation, this defines which services will be implemented and to what recommended degree.
- Service Profile:
  - ➢ For each service defined in the service catalogue, this determines whether it will be executed insourcing, outsourcing, or in a hybrid manner.
- Service Portfolio:
  - ➢ An assessment of each service assigned in the service profile, evaluating the current level of implementation and the desired future level.

The build, management, and evaluation processes are described in the following sections:

- ➢ **Section 3.2:** Building a security response organisation
- ➢ **Section 3.3:** Managing a security response organisation
- ➢ **Section 3.4:** Evaluating a security response organisation

© 2025 ISOG-J

3.2. Building a security response organisation

3.2.1. Overview of the build process

This section explains the overall structure of the build process based on X.1060/JT-X1060. In X.1060/JT-X1060, the process of building a security response organisation is broadly defined in three phases.

- **Phase1: define a service catalogue (decide what to do)**
- **Phase2: define a service profile (decide who will do it)**
- **Phase3: define a service portfolio (determine the goals to be achieved)**

The overall structure illustrating the relationships among these three phases is shown in the following diagram.
In X.1060/JT-X1060, the building of a security response organisation is outlined as a sequential implementation of each phase based on a general service list.

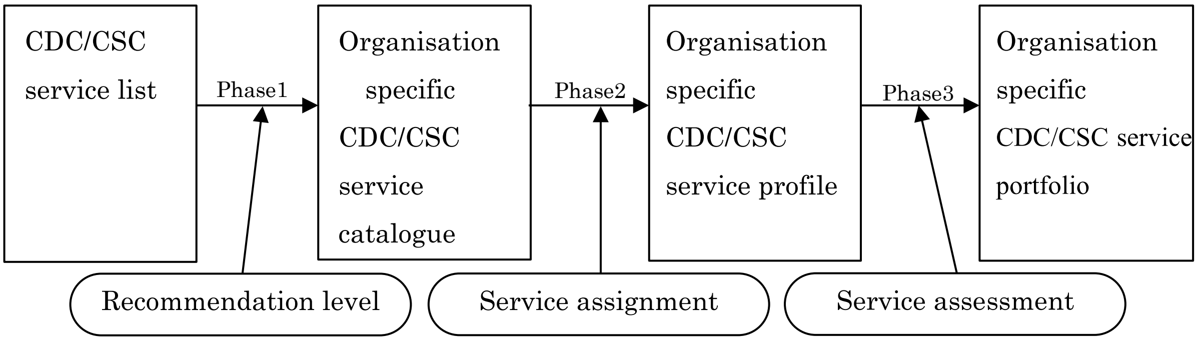

CDC/CSC service list
Phase1
Organisation specific CDC/CSC service catalogue
Phase2
Organisation specific CDC/CSC service profile
Phase3
Organisation specific CDC/CSC service portfolio
Recommendation level
Service assignment
Service assessment

Figure 9: phase of building CDC services of X.1060/JT-X1060[13]

By implementing these three phases, a service portfolio can finally be created. As a concrete example, X.1060/JT-X1060 provides a service matrix that encompasses the service portfolio, as illustrated below.

---

[13] ITU-T recommendation X.1060 “Framework for the creation and operation of a cyber defence centre”, Figure 3
https://www.itu.int/rec/T-REC-X.1060-202106-I

© 2025 ISOG-J

Service	Recommendation level	Service assignment	Service score	
			As-Is	To-Be
Service ex.1	Basic	Insourcing (AB Dept.)	3	5
Service ex.2	Standard	Outsourcing (Z-MSSP)	2	4
Service ex.3	Advanced	Unassignable	1	2

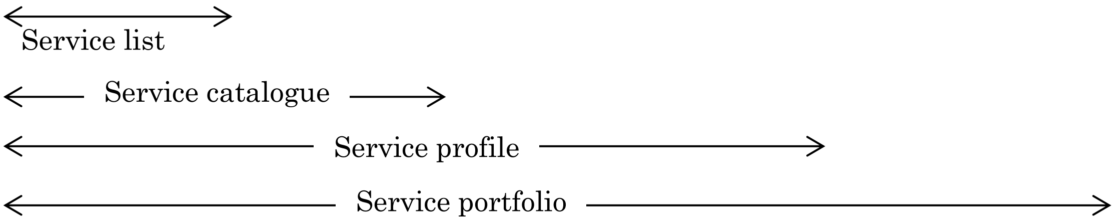


Figure 10: Service matrix of CDC services[14]

The contents of each phase are outlined below. By completing the service matrix, which encompasses the service portfolio, for each phase, the resulting service portfolio can be consolidated during the construction process.

3.2.2. Define a service catalogue

The service catalogue created in Phase 1 of the build process is developed using the service list outlined in the subsequent section, "5. Security Response Organisation Services," and the recommended levels determined by each organisation (detailed in "5.2 Recommended Levels for Services"). This catalogue determines which services to implement and to what recommended degree.

In this document version 2.1, nine functions and 54 roles were defined. However, in X.1060/JT-X1060, these are defined as nine categories and 64 services. Moving forward, the terms categories and services will be used in alignment with X.1060/JT-X1060.

Services are selected from the service list in X.1060/JT-X1060, which represents best practices. However, depending on the industry or business type, some organisations may find that the list does not fully align with their needs. In such cases, it is acceptable to independently define any additional services deemed necessary.

---

[14] ITU-T recommendation X.1060 “Framework for the creation and operation of a cyber defence centre”, Figure 4
https://www.itu.int/rec/T-REC-X.1060-202106-I

© 2025 ISOG-J

Details regarding the categories and services can be found in "4. Categories of Security Response Organisations" and "5. Security Response Organisation Services." The concept and application of recommended levels are explained in "5.2 Recommended Levels for Services" in subsequent sections.

Table 1: categories and services

9 categories	64 services	
A. strategic management of CDC/CSC	A1 - A13	13 services
B. real-time analysis	B1 - B4	4 services
C. deep analysis	C1 - C4	4 services
D. incident response	D1 - D7	7 services
E. checking and evaluation	E1 - E9	9 services
F. collection, analysis and evaluation of threat intelligence	F1 - F5	5 services
G. development and maintenance of CDC platforms	G1 - G13	13 services
H. support of internal fraud response	H1 - H2	2 services
I. active relationship with external parties	I1 - I7	7 services

↓

Table 2: selected services（e.g. selected 22 services in 64 services）

9 categories	64 services	
A. strategic management of CDC/CSC	A1 - A9	9 services
B. real-time analysis		4 services
C. deep analysis	unselect (no service)	
D. incident response	D1	1 service
E. checking and evaluation	E1 - E7	7 services
F. collection, analysis and evaluation of threat intelligence	unselect (no service)	
G. development and maintenance of CDC platforms	G1 - G4	4 services
H. support of internal fraud response	unselect (no service)	
I. active relationship with external parties	I1 - I7	7 services

© 2025 ISOG-J

Based on this example, the recommended levels of the selected services are determined and recorded in the service matrix, as shown below. Due to space constraints, some entries are omitted.

Table 3: write down service catalogue into service matrix

Service	recommendation level	Service assignment	Service score	
			As-Is	To-Be
Service A1	Basic			
(skip, A2-9)				
Service B1	Basic			
(skip, B2-4)				
Service D1	Basic			
Service E1	Standard			
(skip, E2-7)				
Service G1	Basic			
(skip, G2-4)				
Service I1	Basic			
(skip, I2-7)				

3.2.3. Define a service profile

The service profile defined in Phase 2 of the build process determines whether each service identified in the service catalogue will be implemented insource, outsource, or through a hybrid approach. It also specifies which insourcing team, department, or outsourcing contractor will execute each service.

The approach to assigning services—whether insource or outsource—remains consistent with the methodology outlined in this document version 2.1.

Details regarding the allocation of services can be found in the subsequent section, "6.2 Approaches to Role Allocation in Security Response."

© 2025 ISOG-J

Continuing from the previous example, the determination of which organisation will execute each service is made and recorded in the service matrix, as shown below. Due to space constraints, some entries are omitted.

Table 4: write down service profile into service matrix

Service	Recommendation level	Service assignment	Service score	
			As-Is	To-Be
Service A1	Basic	Insourcing CSIRT		
(skip, A2-9)				
Service B1	Basic	Insourcing SOC		
(skip, B2-4)				
Service D1	Basic	Outsourcing		
Service E1	Standard	Outsourcing		
(skip, E2-7)				
Service G1	Basic	Insourcing Information System Division		
(skip, G2-4)				
Service I1	Basic	Insourcing CSIRT		
(skip, I2-7)				

3.2.4. Define a service portfolio

The service portfolio created in Phase 3 of the build process involves assessing each service allocated in the service profile. This assessment determines the current level of implementation and the desired future level of maturity.

This service portfolio corresponds to what was previously defined as maturity in Version 2.1. During the development of X.1060, this concept was reframed as an 'assessment' rather than a 'score'. This change reflects its nature as a self-evaluation tool intended for internal use, not for external audits. The evaluation criteria and definitions remain unchanged, so they should continue to be used as before.

Details regarding assessments are provided in the subsequent section, "8. Assessment of Security Response Organisations." The numerical scores for "As-Is" (current state) and

© 2025 ISOG-J

"To-Be" (desired state) for each service are described in "8.3 Execution Levels of Each Service."

Continuing from the previous example, the assessment results are recorded in the matrix, as shown below. Due to space constraints, some entries are omitted. Once the matrix is completed, it becomes possible to visualize which services are selected and implemented at what recommended level, their allocation, and their "As-Is" and "To-Be" scores.

Table 5: write down service portfolio into service matrix

Service	Recommendation level	Service assignment	Service score	
			As-Is	To-Be
Service A1	Basic	Insourcing CSIRT	3	5
(skip, A2-9)				
Service B1	Basic	Insourcing SOC	2	4
(skip, B2-4)				
Service D1	Basic	Outsourcing	4	5
Service E1	Standard	Outsourcing	4	5
(skip, E2-7)				
Service G1	Basic	Insourcing Information System Division	3	5
(skip, G2-4)				
Service I1	Basic	Insourcing CSIRT	4	5
(skip, I2-7)				

3.3. Management of security response organisations

3.3.1. Overview of management process

This section explains the management process based on X.1060/JT-X1060.

Before delving into the detailed categories and services of security response organisations, including SOCs and CSIRTs, it is important to first understand the overall execution cycle and management process necessary to operate these organisations effectively. Specifically, it involves three phases executed through two types of cycles.

© 2025 ISOG-J

X.1060/JT-X1060 illustrates the management process with the following diagram. What was previously referred to as "Implementation" in Version 2.1 has been updated to "Strategic Management" in accordance with X.1060/JT-X1060. This aligns with what was originally defined in Japan as the "Strategic Management Layer."

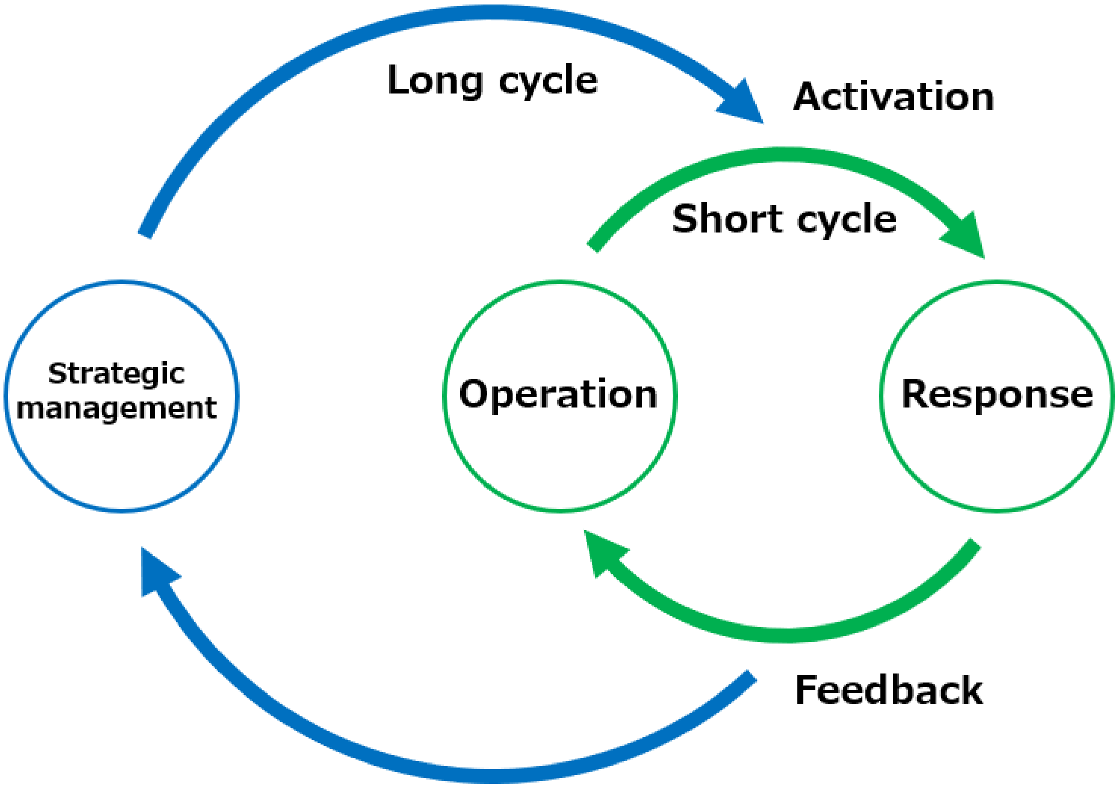


Figure 11: CDC management process – two cycles

3.3.2. Phases and cycles in the management process

This section describes the three phases and two types of cycles presented in the management process. These are explained as follows:

- Strategic management

In X.1060/JT-X1060, it is stated that "Strategic management has responsibility and accountability for all strategic services relevant to definitions, design, planning, management, certification, etc. that ensure the long-term development of CDC/CSC. "

© 2025 ISOG-J

As a concrete example, this involves tasks such as reviewing security response policies, identifying areas for improvement in the long-term cycle based on short-term cycle evaluations, and examining and building the mechanisms (such as organisational structures, business processes, and systems) necessary for their execution.

- **Operation**

In "Operation", the regular execution and maintenance of the implemented mechanisms are carried out. This generally corresponds to routine activities during normal periods. Tasks include analysis for incident detection, monitoring, and maintenance of security response systems. Organisations responsible for such analytical operations are often referred to as SOCs.

- **Response**

In “Response”, the incident response is carried out for events detected by analysis in “Operation”. This is generally the contingency operation. The organisation responsible for incident response is often called a CSIRT. Input is not limited to “Operation”, but also includes responses triggered by reports from outside the own organisation or notifications from external organisations.

- **Short cycle**

"Operation" and "Response" activities are conducted on a daily basis. Within these activities, issues in business processes and challenges in security response systems inevitably arise. It is essential to regularly review these problems and address them through short-cycle improvements within the implemented mechanisms.

Examples of such improvements include simple automation of routine tasks, enhancements to tools to improve analytical accuracy, or revisions to report items. These reviews are limited to the allocated resources (personnel, budget, and systems).

Although not explicitly illustrated, there are also internal review processes within each of the "Strategic Management", "Operation" and "Response" stages.

- **long cycle**

In the "short-cycle" review process, if issues are identified that cannot be resolved within the implemented mechanisms, they should be addressed with a long-term perspective and planning. Examples include the introduction of new security products, significant

© 2025 ISOG-J

revisions to security response policies, or major reconfigurations of operational infrastructure. These types of reviews often require the allocation of new resources.

In recent CSIRT development efforts, there are many cases where organisations focus primarily on the "Response" phase to build their security response framework. However, isolating and organizing around only this phase can lead to various issues. For instance, "Operations" may not function effectively, resulting in missed incidents, or security products may be selected without a clear understanding of what the organisation or company truly wants to protect. Such shortcomings often stem from failures at the "Strategic Management" stage.

To avoid these pitfalls, it is essential to maintain focus on the axes of "Strategic Management", "Operation", and "Response", while embracing the concept of continuous "execution" and "review" cycles.

© 2025 ISOG-J

3.4. Evaluation of security response organisations

3.4.1. Overview of evaluation process

This section explains the evaluation process based on X.1060/JT-X1060. The evaluation process is a newly added component in X.1060/JT-X1060.

The evaluation process is carried out by reviewing each of the following three phases conducted during the construction process:

- ✧ **Phase1: Gap analysis of the recommended levels in the service catalogue**
- ✧ **Phase2: Gap analysis of service allocation in the service profile**
- ✧ **Phase3: Gap analysis of service assessments in the service portfolio**

The following figure illustrates an overview of the evaluation process as outlined in X.1060/JT-X1060.

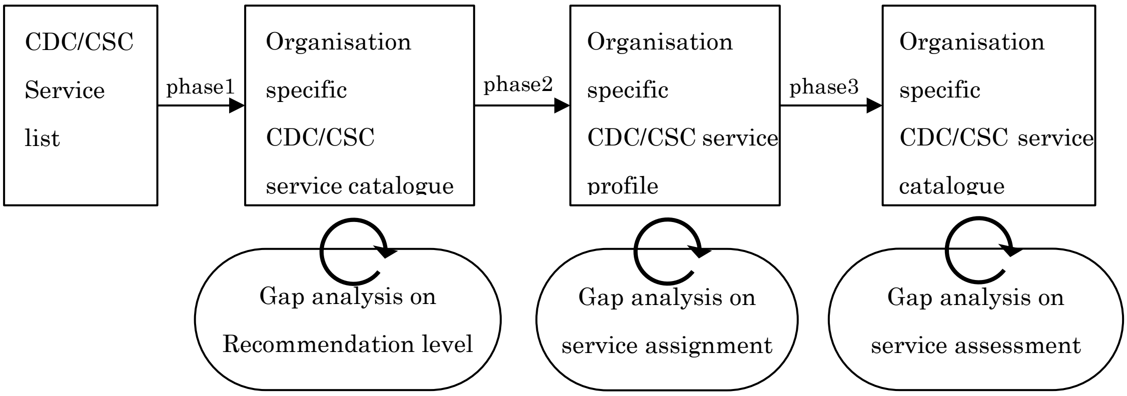

CDC/CSC Service list
phase1
Organisation specific CDC/CSC service catalogue
phase2
Organisation specific CDC/CSC service profile
phase3
Organisation specific CDC/CSC service catalogue
Gap analysis on Recommendation level
Gap analysis on service assignment
Gap analysis on service assessment

Figure 12 evaluation process for CDC in X.1060/JT-X1060[15]

In the evaluation process, a gap analysis is performed for each of the three phases conducted during the build process.

One example of the order for conducting the gap analysis is to follow the same sequence as the build process, reviewing whether the results of each phase—from Phase 1

---

[15] ITU-T recommendation X.1060 "Framework for the creation and operation of a cyber defence centre", Figure 7
https://www.itu.int/rec/T-REC-X.1060-202106-I

© 2025 ISOG-J

onward—are reasonable. Alternatively, the reverse order can be used, starting with the gap in the current assessment scores in Phase 3 and analyzing why such results were obtained.

3.4.2. Gap analysis and review

By conducting a gap analysis in the evaluation process, the strengths and weaknesses of the established system are made visible. Using these results, it is essential to return to the construction process to make improvements that lead to better security responses. To ensure comprehensive organisational improvements, sufficient authority must be granted to the CISO, security oversight functions, and the security response organisation. Careful attention must be paid to avoid relying solely on isolated team-level improvements or the efforts of individual personnel.

Given the rapid pace of changes in business environments and surrounding conditions, it is inevitable that even well-established systems will gradually become outdated. For example, many companies that previously operated primarily in protected intranet environments suddenly had to transition to remote work due to COVID-19. At the same time, security response organisations themselves likely had to adapt to working remotely. Similar abrupt changes in the external environment—affecting both the assets to be protected and the operational environment of the security response organisation—are likely to continue occurring in the future.

This is precisely why the X.1060/JT-X1060 framework emphasizes the continuous repetition of the build, management, and evaluation processes. To prevent the undesirable adherence to outdated precedents or organisational rigidity in security response efforts, it is crucial to make effective use of the evaluation process. By maintaining an awareness of the management process and implementing necessary reconstructions, organisations can adapt and improve their security response systems dynamically.

3.4.3. Examples of timing of review

In today's complex threat landscape surrounding corporate and organisational cybersecurity, it is essential for companies and organisations to maintain effective security measures. However, over time, changes in organisational environments and threat scenarios often render traditional service portfolios insufficient to provide adequate protection.

© 2025 ISOG-J

For this reason, the following examples illustrate when companies and organisations should review their service portfolios. Continuously revisiting and updating the portfolio in response to changing conditions is crucial to ensuring robust security.

Example 1: When Business Environments Change
  - 1.1 Launch of a new business or acquisition
  - 1.2 Downsizing or withdrawal from a business
  - 1.3 Organisational restructuring
  - 1.4 Changes in laws or regulations
  - 1.5 Shifts in economic conditions
  - 1.6 Customer demands
  - 1.7 Supply chain requirements

Example 2: When Technological Advancements Occur
  - 2.1 Expansion of mobile device usage
  - 2.2 Increased adoption of cloud services
  - 2.3 Proliferation of IoT devices
  - 2.4 Changes in IT environments, such as the adoption of Zero Trust models
  - 2.5 Utilization of AI and big data

Example 3: When Changes in Attack Techniques Occur
  - 3.1 Emergence of new threats and vulnerabilities
  - 3.2 Increased sophistication of attack methods

Example 4: When the Current State of Security Measures is Assessed
  - 4.1 Vulnerability assessments
  - 4.2 Security exercises
  - 4.3 Security audits
  - 4.4 Security awareness surveys
  - 4.5 Occurrence of a security incident

Example 5: When Resource Conditions Change
  - 5.1 Changes in the security budget
  - 5.2 Changes in the number or skill level of security personnel
  - 5.3 Changes in the functionality or performance of security devices
  - 5.4 Changes in the services provided by Managed Security Service Providers

© 2025 ISOG-J

(MSSPs)

Example 6: When Operational Changes are Made

- 6.1 Changes in business processes
- 6.2 Changes in system operations

Example 7: Regular Reviews

- 7.1 At intervals specified by certifications held
- 7.2 At intervals mandated by laws or regulations
- 7.3 At intervals determined by internal security policies or rules
- 7.4 At the time of regular contract renewals

Using these examples as guidance, organisations and companies should choose an approach tailored to their specific needs and review their service portfolio at appropriate times. By doing so, they can continuously improve their security organisations.

© 2025 ISOG-J

4. Categories in security response organisations

4.1. Overview of categories

When building a security response organisation, the service list from X.1060/JT-X1060 was utilized to create the service catalogue. This service list outlines the functional areas that a security response organisation should address, along with the specific activities to be performed within each area. It is categorized into nine categories and includes 64 services.

The nine categories defined in X.1060/JT-X1060 are as follows:

Table 6: Categories in X.1060/JT-X1060

Categories
A. strategic management of CDC/CSC
B. real-time analysis
C. deep analysis
D. incident response
E. checking and evaluation
F. collection, analysis and evaluation of threat intelligence
G. development and maintenance of CDC/CSC platforms
H. support of internal fraud response
I. active relationship with external parties

Details of each category are provided in "Appendix 1 Categories and service list".

4.2. Categories in cycles of CDC management process

When mapping each category to the phase of the security response execution cycle as shown in "Figure 11: CDC management process – two cycles", the relationships are summarised in the following diagram.

In the diagram, the phases within each execution cycle—Strategic Management, Operation, and Response—are overlaid with the categories to indicate which process each service category corresponds to. Use this as a reference to understand which selected categories relate to specific phases within the execution cycle.

© 2025 ISOG-J

Note that Categories E, F, and G are associated with all three phases, which is why their scope is broader. Specifically, Category G overlaps with the upper layer of the processes, as the CDC platform planned during Strategic Management is utilized within the Operation and Response cycles.

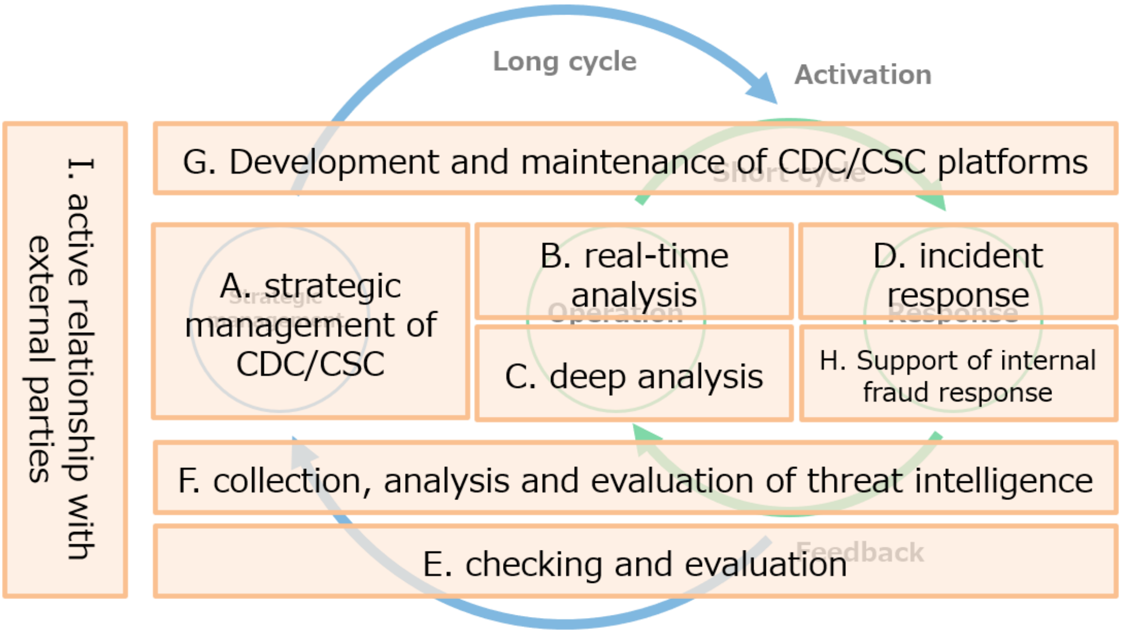

Long cycle
Activation
I. active relationship with external parties
G. Development and maintenance of CDC/CSC platforms
Short cycle
A. strategic management of CDC/CSC
Strategic
B. real-time analysis
Operation
C. deep analysis
D. incident response
Response
H. Support of internal fraud response
F. collection, analysis and evaluation of threat intelligence
E. checking and evaluation
Feedback

Figure 13: Relationship between categories and management process

Based on the policies determined in "A. Strategic Management of the CDC/CSC," the purpose-driven system implementation in "G. Development and Maintenance of the CDC/CSC Platform" enables the execution of security responses. Utilizing this system, organisations perform "B. Real-Time Analysis" and, when necessary, "C. Deep Analysis." If an incident is identified, actions such as "D. Incident Response" or "H. Support for Internal Fraud Response" are undertaken.

These operational and response outcomes, along with "F. Threat Intelligence Collection, Analysis, and Evaluation," help the organisation understand the threats it faces. At the same time, "E. Diagnosis and Evaluation" assesses the organisation's defensive capabilities. Based on this evaluation, improvements that can be immediately implemented are addressed in a short cycle. For more fundamental changes, decisions are made anew in "A. Strategic Management of the CDC/CSC," followed by the next round of "G. Development and Maintenance of the CDC/CSC Platform," forming a long-

© 2025 ISOG-J

term cycle of improvement.

It is not always necessary for a single organisation to encompass all categories and execute the entire cycle internally. In practice, it is common for different categories to be executed in collaboration with other internal or external organisations. However, when collaborating across organisations, maintaining a highly coordinated and close relationship is essential.

© 2025 ISOG-J

5. Services in security response organisations

5.1. Overview of the services

The services described in this chapter are based on the definitions provided in X.1060/JT-X1060.

Details of each service are provided in ” Appendix 1　Categories and service list”.

Table 7: services in X.1060/JT-X1060

Category	Service
A. strategic management of CDC/CSC	A-1. Risk management A-2. Risk assessment A-3. Policy planning A-4. Policy management A-5. Business continuity A-6. Business impact analysis A-7. Resource management A-8. Security architecture design A-9. Triage criteria management A-10. Counter measures selection A-11. Quality management A-12. Security audit A-13. Certification
B. real-time analysis	B-1. Real-time asset monitoring B-2. Event data retention B-3. Alerting and warning B-4. Handling enquiry on report
C. deep analysis	C-1. Forensic analysis C-2. Malware sample analysis C-3. Tracking and tracing C-4. Forensic evidence collection

© 2025 ISOG-J

Category	Service
D. incident response	D-1. Incident report acceptance D-2. Incident handling D-3. Incident classification D-4. Incident response and containment D-5. Incident recovery D-6. Incident notification D-7. Incident response report
E. checking and evaluation	E-1. Network information collection E-2. Asset inventory E-3. Vulnerability assessment E-4. Patch management E-5. Penetration test E-6. Defence capability against APT attack evaluation E-7. Handling capability on cyberattack evaluation E-8. Policy compliance E-9. Hardening
F. collection, analysis and evaluation of threat intelligence	F-1. Post-mortem analysis F-2. Internal threat intelligence collection and analysis F-3. External threat intelligence collection and evaluation F-4. Threat intelligence report F-5. Threat intelligence utilization

© 2025 ISOG-J

Category	Service
G. development and maintenance of CDC/CSC platforms	G-1. Security architecture implementation G-2. Basic operation for network security asset G-3. Advanced operation for network security asset G-4. Basic operation for endpoint security asset G-5. Advanced operation for endpoint security asset G-6. Basic operation for cloud security products G-7. Advanced operation for cloud security products G-8. Deep analysis tool operation G-9. Basic operation for analysis platform G-10. Advanced operation for analysis platform G-11. Operates CDC/CSC systems G-12. Existing security tools evaluation G-13. New security tools evaluation
H. support of internal fraud response	H-1. Internal fraud response and analysis support H-2. Internal fraud detection and reoccurrence prevention support
I. active relationship with external parties	I-1. Awareness I-2. Education and training I-3. Security consulting I-4. Security vendor collaboration I-5. Collaboration service with external security communities I-6. Technical reporting I-7. Executive security reporting

The arrangement of service categories and services, as well as the management process, holds significance in the "Figure 8: CDC/CSC Service Categories" diagram in both X.1060 and JT-X1060. The vertical alignment in the diagram corresponds to the management processes: Strategic Management, Operation, and Response.

When selecting services, this diagram can serve as a reference for determining which part of the management process should address each service.

Categories E, F, and G are involved in all management processes. However, the specific process in which each service within these categories is addressed may vary. The diagram is intended as a reference, and there is no strict requirement to follow it exactly.

© 2025 ISOG-J

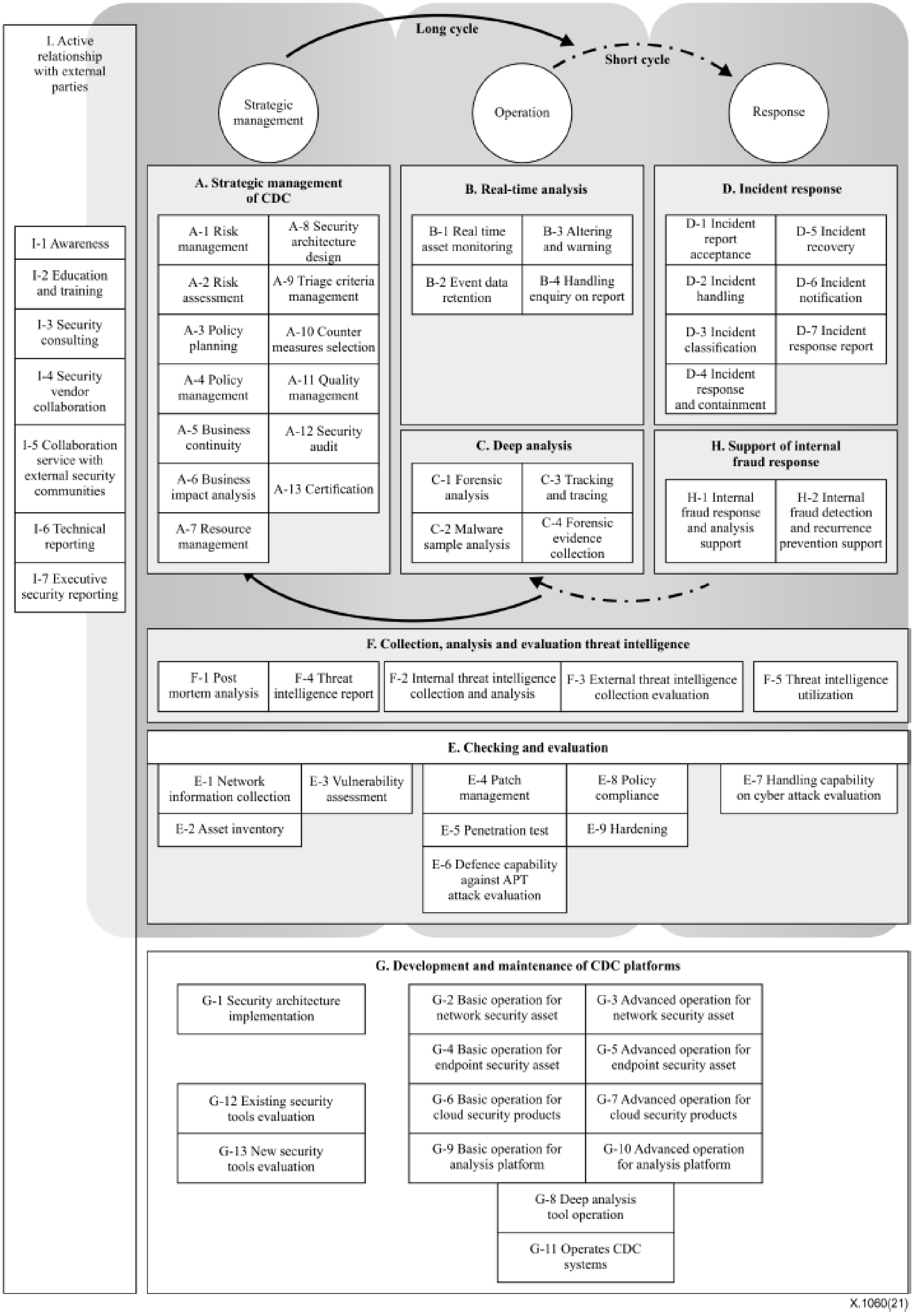

Long cycle
Short cycle
Strategic management
Operation
Response
I. Active relationship with external parties
I-1 Awareness
I-2 Education and training
I-3 Security consulting
I-4 Security vendor collaboration
I-5 Collaboration service with external security communities
I-6 Technical reporting
I-7 Executive security reporting
A. Strategic management of CDC
A-1 Risk management
A-2 Risk assessment
A-3 Policy planning
A-4 Policy management
A-5 Business continuity
A-6 Business impact analysis
A-7 Resource management
A-8 Security architecture design
A-9 Triage criteria management
A-10 Counter measures selection
A-11 Quality management
A-12 Security audit
A-13 Certification
B. Real-time analysis
B-1 Real time asset monitoring
B-2 Event data retention
B-3 Altering and warning
B-4 Handling enquiry on report
C. Deep analysis
C-1 Forensic analysis
C-2 Malware sample analysis
C-3 Tracking and tracing
C-4 Forensic evidence collection
D. Incident response
D-1 Incident report acceptance
D-2 Incident handling
D-3 Incident classification
D-4 Incident response and containment
D-5 Incident recovery
D-6 Incident notification
D-7 Incident response report
H. Support of internal fraud response
H-1 Internal fraud response and analysis support
H-2 Internal fraud detection and recurrence prevention support
F. Collection, analysis and evaluation threat intelligence
F-1 Post mortem analysis
F-4 Threat intelligence report
F-2 Internal threat intelligence collection and analysis
F-3 External threat intelligence collection evaluation
F-5 Threat intelligence utilization
E. Checking and evaluation
E-1 Network information collection
E-2 Asset inventory
E-3 Vulnerability assessment
E-4 Patch management
E-5 Penetration test
E-6 Defence capability against APT attack evaluation
E-8 Policy compliance
E-9 Hardening
E-7 Handling capability on cyber attack evaluation
G. Development and maintenance of CDC platforms
G-1 Security architecture implementation
G-12 Existing security tools evaluation
G-13 New security tools evaluation
G-2 Basic operation for network security asset
G-3 Advanced operation for network security asset
G-4 Basic operation for endpoint security asset
G-5 Advanced operation for endpoint security asset
G-6 Basic operation for cloud security products
G-7 Advanced operation for cloud security products
G-9 Basic operation for analysis platform
G-10 Advanced operation for analysis platform
G-8 Deep analysis tool operation
G-11 Operates CDC systems
X.1060(21)

Figure 14: relation between management process and each service[16]

---

[16] ITU-T recommendation X.1060 “Framework for the creation and operation of a cyber defence centre”, Figure 8
https://www.itu.int/rec/T-REC-X.1060-202106-I

© 2025 ISOG-J

The services within each category related to the management processes of Strategic Management, Operation, and Response in the diagram above can be classified as shown in the following table. This table serves as a reference for determining where in the management process each service can be utilized.

Table 8: Mapping of services to Management Processes

Category	Strategic management	Operation	Response
A	A-1～A-13	–	–
B	–	B-1～B-4	–
C	–	C-1～C-4	–
D	–	–	D-1～D-7
E	E-1～E-3	E-4, E-5, E-6, E-8, E-9	E-7
F	F-1, F-4	F-2, F-3	F-5
G	G-1, G-12, G-13	G-2～G-11	–
H	–	–	H-1, H-2
I	I-1～I-7	–	–

© 2025 ISOG-J

5.2. CDC/CSC service recommendation level

5.2.1. Consideration of Recommendation Levels in X.1060

In the initial phase of the build process, services are selected from the service list, and a service catalogue is created. At this phase, the recommendation level for each service, representing the desired level of implementation for the organisation, is defined.

In X.1060/JT-X1060, the recommendation levels for CDC/CSC services are defined five weights, as indicated by the following table: Unnecessary, Basic, Standard, Advanced, and Optional.

This document utilizes the recommendation levels defined in X.1060/JT-X1060, supplemented with the following interpretations (shown in parentheses in the table) to help organisations consider the implementation priority at each level.

Table 9 CDC/CSC service recommendation level[17] in X.1060/JT-X1060

Weight	Description
Unnecessary	Services deemed unnecessary
Basic “Essential”	Minimum services to be implemented (Essential services that should be implemented)
Standard “Standard”	Services that are generally recommended for implementation (Services that are generally required as standard)
Advanced “Recommended”	Services required to achieve a higher-level CDC cycle (Services recommended for achieving more robust security)
Optional “Arbitrary”	Services arbitrarily selected according to the expected form of CDC (Services that may be required optionally)

In the first phase of the build process, necessary services are selected from the nine categories and 64 services. If the required service is not available in the list, it can be added independently.

When selecting services for an organisation, X.1060/JT-X1060 introduces the concept of "recommendation levels."

The first step in determining the recommendation level is to decide whether a service is

---

[17] ITU-T recommendation X.1060 “Framework for the creation and operation of a cyber defence centre”, Table 1
https://www.itu.int/rec/T-REC-X.1060-202106-I

© 2025 ISOG-J

"unnecessary". If deemed unnecessary, it is crucial to document why this decision was made. Was it because there is no associated risk, or because it is currently unfeasible? This distinction is significant. In the latter case, the reason—whether it is due to budget constraints, resource limitations, or skill gaps—should be clearly identified. This information will be valuable during the evaluation process when doing the build process.

Next, for each service determined to be necessary, the recommended level—Basic, Standard, Advanced, or Optional—is decided. Basic has the highest priority, while Optional has the lowest. The recommended level for each service varies depending on the organisation's goals, industry standards, structure, and security policies. Therefore, it is challenging to define these levels universally, and X.1060/JT-X1060 does not specify which services should align with which levels.

As the adoption of X.1060/JT-X1060 progresses and more knowledge and experience are accumulated, standard patterns for recommended levels may emerge. For now, organisations must make these decisions independently. However, X.1060/JT-X1060 is designed so that subsequent processes can proceed even without determining the recommended levels, meaning it is not strictly necessary to finalize them if doing so is challenging.

5.2.2. Examples of how services are selected

In X.1060/JT-X1060, nine categories and 64 services are outlined, along with recommended levels for selecting each service.

As an ideal approach to constructing a security response organisation, organisations should conduct a risk assessment and assign recommended levels to each of the 64 services. Based on necessity, they should then determine where to start implementation. However, while conducting a risk assessment and assigning recommended levels to all 64 services is important, it is also a resource-intensive process.

As an alternative, this section presents an approach that prioritises enabling the organisation to begin daily operations within the management process. This practical approach focuses on starting operations and emphasizes that evaluations and subsequent improvement cycles of the construction process should gradually enhance the organisation over time.

© 2025 ISOG-J

Up to this point, the relationship between categories and services and the execution cycle of the management process has been demonstrated. To ensure the three phases within the management process (Strategic Management, Operation, and Response) run smoothly across two cycles, services should be selected from the mapped categories as follows:

The category related to the Strategic Management phase is Category A, "Strategic Management of the CDC/CSC."
The categories related to the Operations phase are Categories B and C. However, since Category C involves deep analysis, the priority here should be Category B, "Real-Time Analysis."
The categories related to the Response phase are Categories D and H. Since Category H pertains to internal fraud response, the priority should be Category D, "Incident Response."

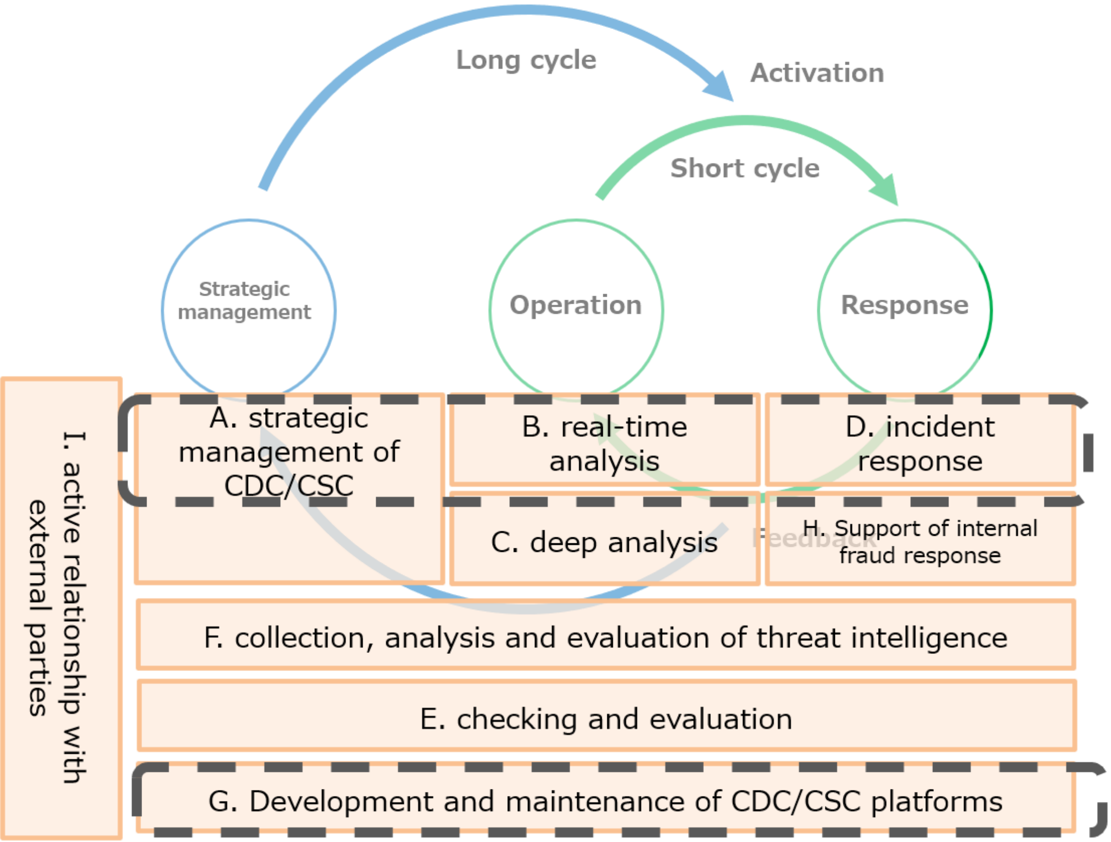

Long cycle
Activation
Short cycle
Strategic management
Operation
Response
I. active relationship with external parties
A. strategic management of CDC/CSC
B. real-time analysis
D. incident response
C. deep analysis
Feedback
H. Support of internal fraud response
F. collection, analysis and evaluation of threat intelligence
E. checking and evaluation
G. Development and maintenance of CDC/CSC platforms

Figure 15: categories for doing management process

© 2025 ISOG-J

With Categories A, B, and D in place, the management process appears ready for implementation, allowing daily operations to commence. However, it is important to note that the ability to begin monitoring operations presupposes the existence of monitoring and operational products. Thus, the use of certain security products under Category G is also essential.

Based on this understanding, the management process can begin by conducting Strategic Management under Category A, operating security products under Category G, performing daily monitoring under Category B, and responding to incidents under Category D when necessary. From these categories (A, B, D, G), organisations should select the specific services they need. Naturally, there may also be services from other categories that are already being implemented by the organisation.

For organisations starting from scratch, the priority is to identify the necessary services within Categories A, B, D, and G, including their recommendation levels, and assign them to the security team. While this approach focuses on selecting services essential for daily operations, it is also important to consider services required to comply with existing regulations, management systems, or laws, such as data protection laws. These compliance-related services should be classified as Basic "essential " and must be implemented.

At this stage, the selection process should ensure that services for daily operations and compliance are covered. Beyond this, services at the Standard “standard”, Advanced “Recommended,” or Optional “arbitrary” levels come into play. What is considered standard may vary by industry, so organisations should consult industry-specific guidelines to determine the services typically required. Additionally, if certain services are generally needed to utilize cybersecurity insurance, they should also be classified as standard.

The X.1060/JT-X1060 framework for building and operating security response organisations requires building the evaluation process regularly to facilitate ongoing improvements based on the outcomes of the management process. By leveraging the evaluation results, organisations can reassess which categories and services should be implemented. Initiating the construction process again and reallocating services allows the security response organisation to grow and improve.

Through continuous reassessment and refinement, organisations can work toward restructuring their security response systems to achieve an ideal organisational model.

© 2025 ISOG-J

6. Service assignment and structure for security response organisation

6.1. Relationship between SOC, CSIRT and services in Japan so far

Among security response organisations, the most commonly recognised are SOCs (Security Operations Centres) and CSIRTs (Computer Security Incident Response Teams). To clarify their roles, let us review the general distinctions between the two. For clarity, this section will focus on SOCs in the narrow sense (limited to Categories B and C as defined in this document).

In Japan, when the primary responsibility for incident response lies with the CSIRT, the organisation tasked with monitoring security logs to detect incidents and conducting deep analysis following incidents (often referred to as rescue or emergency response services) is typically referred to as the SOC.

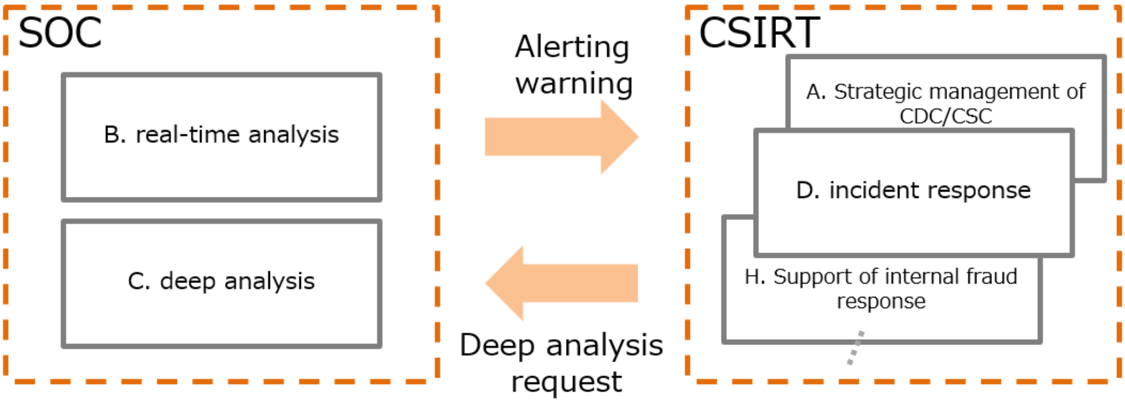

SOC
B. real-time analysis
C. deep analysis
Alerting warning
Deep analysis request
CSIRT
A. Strategic management of CDC/CSC
D. incident response
H. Support of internal fraud response

Figure 16: General classification of SOC and CSIRT

However, with the growing awareness and evolving needs of modern security, the boundaries between SOCs and CSIRTs have become increasingly blurred. SOCs are expanding their service scope to include support for incident response, while CSIRTs are enhancing their technical capabilities to perform basic analyses independently. Some organisations even maintain private SOCs within their structures. These developments have diversified the roles of SOCs and CSIRTs, depending on the scale and capabilities of the SOC provider or CSIRT.

© 2025 ISOG-J

As a result, it has become difficult to draw clear lines, such as, "This part is the responsibility of the CSIRT and handled in-house, while that part is the SOC's responsibility and outsourced to a specialized organisation." However, engaging specialized organisations often involves contractual agreements, which necessitate defining the boundaries of responsibilities.

The next section will discuss the considerations for defining these boundaries, specifically how services should be allocated—whether performed by the internal security team or entrusted to a specialized organisation.

© 2025 ISOG-J

6.2. Approach to role assignment in security response

In X.1060/JT-X1060, the first phase of the build process involves selecting services from the service list to create a service catalogue. In the subsequent phase, a service profile is created by determining who will execute the services listed in the catalogue.

To facilitate the creation of the service profile, X.1060/JT-X1060 defines the following four types of allocation, as shown in the table below:

Table 10: CDC/CSC service assignment in X.1060/JT-X1060[18]

Type	Description
Insourcing	Services are provided by a team within the organisation. The organisation should specify the team in charge.
Outsourcing	Services are provided by a team outside of the organisation. The organisation should specify the outsourcer.
Combination	The organisation uses insourcing and outsourcing together. A responsible team and a contractor should be specified by the organisation.
Unassigned	Although the organisation recognises a service, but there is no assignee in the organisation.

To determine which tasks should be handled in-house (insourced) and which should be entrusted to specialized organisations (outsourced), the following two criteria are introduced:

① **Nature of information handled**

Whether the information being handled pertains to internal or external aspects of the organisation. For incidents, information related to the damage or impact of an attack is considered "internal," while information related to the attack itself is considered "external."

---

[18] ITU-T recommendation X.1060 “Framework for the creation and operation of a cyber defence centre”, Table 2
https://www.itu.int/rec/T-REC-X.1060-202106-I

© 2025 ISOG-J

② **Need for specialized security skills**

The level of specialized skills in the security domain required to execute the service. "Security-specific skills" refer to security-related expertise that can be applied universally across different organisations. In contrast, the counterpart to these skills is "internal organisational skills," which are less transferable and primarily applicable within the specific organisation.

Using these criteria as axes, services can be classified into four quadrants.

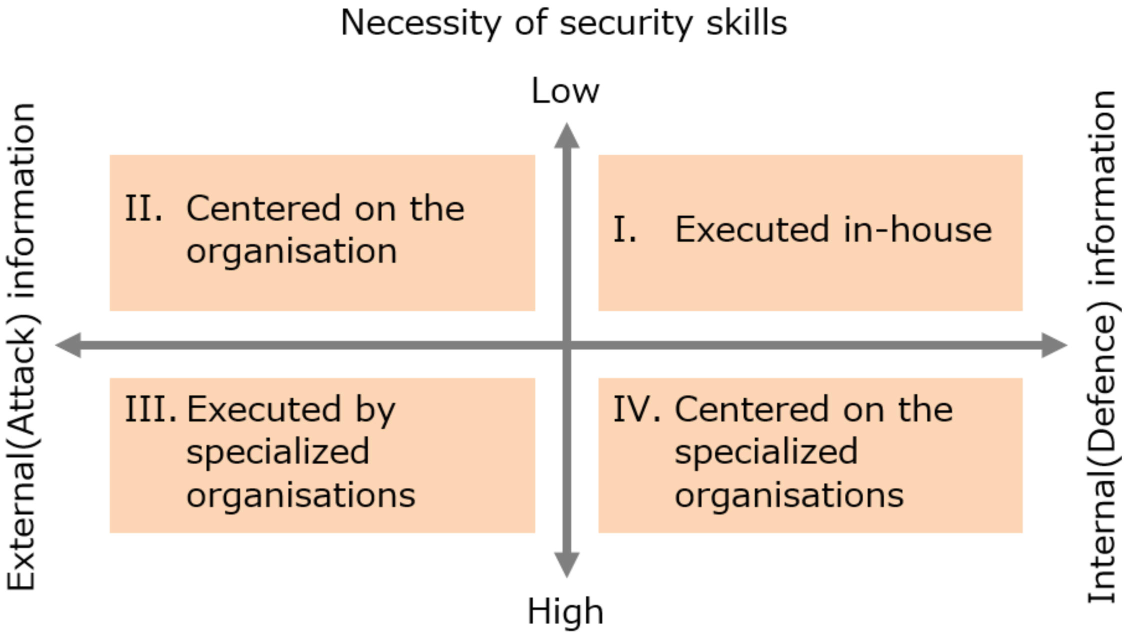

Necessity of security skills
Low
High
External(Attack) information
Internal(Defence) information
II. Centered on the organisation
I. Executed in-house
III. Executed by specialized organisations
IV. Centered on the specialized organisations

Figure 17: Sourcing quadrants

QuadrantI. Areas to Be Executed In-House (Insourcing ≫ Outsourcing)

Tasks involving internal organisational information that do not require high levels of specialization—or where such specialization is not applicable—should be executed within the organisation. This quadrant emphasizes the importance of internal organisational skills, making it difficult to rely on external organisations.

QuadrantII. Areas for Collaboration Centered on the Organisation (Insourcing ≧ Outsourcing)

While tasks involve external information, they require relatively low specialization and primarily rely on internal organisational skills. Execution and management should be

© 2025 ISOG-J

centered within the organisation, with external organisations providing support as needed.

QuadrantIII. Areas to Be Executed by Specialized Organisations (Insourcing ≪ Outsourcing)

For external information, such as data related to attacks, tasks require specialized skills and are best handled by specialized organisations. Unless the organisation has members with advanced expertise, in-house execution is challenging.

QuadrantIV. Areas for Collaboration Centred on Specialized Organisations (Insourcing ≦ Outsourcing)

Tasks involving internal organisational information but requiring high specialization should be executed primarily by specialized organisations, with the in-house team focusing on management and support.

In the service allocation phase of the build process defined in X.1060/JT-X1060, services prioritised earlier are assigned to responsible parties. Rather than having a single security department handle everything, services are divided among various teams, such as IT departments or even business units, depending on the situation. This phase focuses on how security will be implemented across the organisation as a whole.

Since not all tasks can be insourced, options such as insourcing, outsourcing, or a hybrid approach can be considered for allocation. Whereas Version 2.1 of this document only distinguished between "insourcing" and "outsourcing," X.1060/JT-X1060 introduces "hybrid" and "unallocated" as additional options.

The "unallocated" category, in particular, is useful during evaluations and reviews to identify gaps or omissions in allocations. Previously, Version 2.1 focused solely on a clear-cut distinction between "insourcing" and "outsourcing," but the addition of "hybrid" in X.1060/JT-X1060 provides a more practical and flexible approach.

As explained in the table, clarifying who will be responsible for each task and which party will execute it is crucial. These decisions should be made explicitly during this phase.

© 2025 ISOG-J

6.3. Organisational pattern for security response

The patterns of security response organisations can be broadly categorized based on how extensively an organisation's resources are used to cover the three quadrants (II, III, and IV) identified in the previous section, excluding Quadrant I, which must be executed in-house.

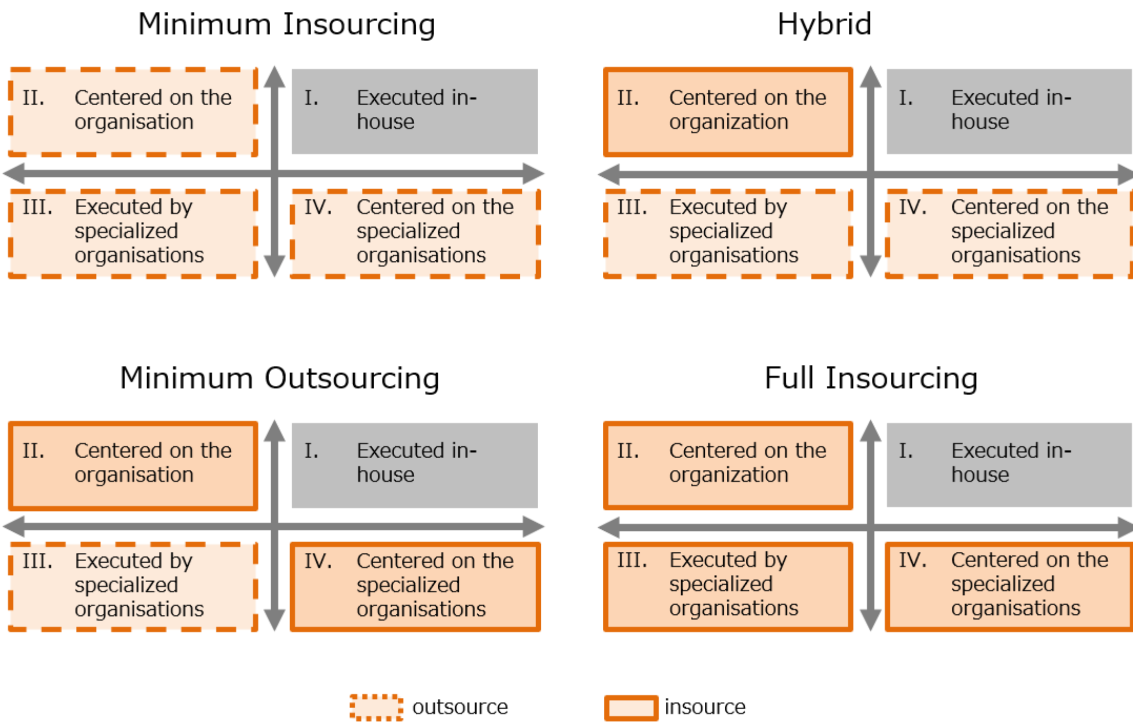

Minimum Insourcing
II. Centered on the organisation
I. Executed in-house
III. Executed by specialized organisations
IV. Centered on the specialized organisations
Hybrid
II. Centered on the organization
I. Executed in-house
III. Executed by specialized organisations
IV. Centered on the specialized organisations
Minimum Outsourcing
II. Centered on the organisation
I. Executed in-house
III. Executed by specialized organisations
IV. Centered on the specialized organisations
Full Insourcing
II. Centered on the organization
I. Executed in-house
III. Executed by specialized organisations
IV. Centered on the specialized organisations
outsource
insource

Figure 18: organisational pattern for security response

Pattern1. Minimum Insourcing

This pattern applies when the organisation has little to no specialized knowledge related to security response, and must rely heavily on external specialized organisations even in Quadrant II. For example, non-IT companies that are establishing a security organisation for the first time, led by administrative departments such as general affairs, often follow this pattern.

Pattern2. Hybrid

In this pattern, the organisation possesses at least a minimum level of expertise in security response, allowing it to take the lead in Quadrant II. This is a common form for user companies or their IT subsidiaries that establish security organisations led by

© 2025 ISOG-J

specialized IT departments. It is considered the most typical model.

Pattern3. Minimum Outsourcing

This pattern applies when the organisation has sufficient expertise in security response to take the lead in all areas except Quadrant III. IT companies that establish security organisations led by specialized information security departments often follow this pattern.

Pattern4. Full Insourcing

This pattern allows the organisation to handle all security response categories and services internally. It is typically the goal for certain IT companies, security-specialized firms, or organisations that require extremely high levels of security[19].

6.4. Service assignment for security response

When services are allocated across the four security response quadrants, the distribution can be summarised as shown in the following diagram. Organisations should consider their organisational pattern to determine which services should be outsourced and which ones must be insourced, using this as a reference for decision-making.
For example, regarding the “low” and “high” levels of need for security-specific skills, this can be viewed in terms of whether the service involves designing various security measures or focuses on implementation and operation based on those designs. For instance, Category A, "Strategic Management of the CDC/CSC," primarily involves designing strategies and setting directions, so it is mapped toward the "low" area of the need for security-specific skills axis.

For the nature of the information handled—internal organisational or victim-side information versus external or attacker-side information—services can be thought of in terms of whether they deal with confidential internal information that is difficult to obtain externally or external threat information requiring specialized skills.

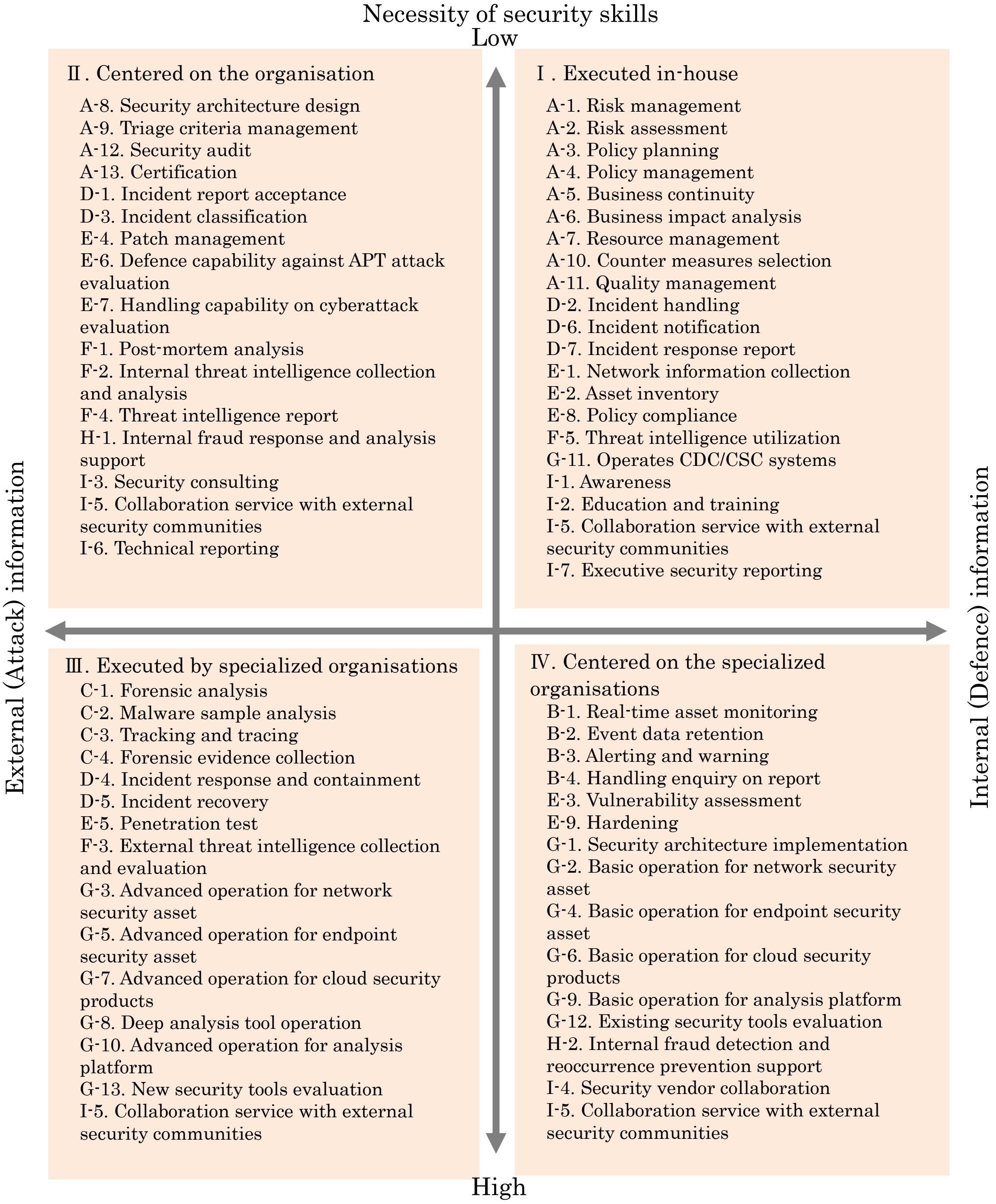
Based on these considerations, an example of how all services are allocated is shown in "Figure 19: Role Allocation in Security Response."” Figure 19: service assignment for

---

[19] It is worth noting that achieving a "full insource" model does not need to be an absolute goal. As long as the required categories and services are fulfilled and the execution cycle functions effectively in alignment with the overall strategy, there is no issue with a high ratio of outsourcing. In fact, forcing a higher insource ratio without the necessary capabilities or resources could lead to more significant problems.

© 2025 ISOG-J

security response”. However, one exception is "I-5. Collaboration with Security-Related Organisations," which is necessary across all quadrants and is therefore allocated to every area.


Necessity of security skills
Low
High
External (Attack) information
Internal (Defence) information

Ⅱ. Centered on the organisation

- A-8. Security architecture design
- A-9. Triage criteria management
- A-12. Security audit
- A-13. Certification
- D-1. Incident report acceptance
- D-3. Incident classification
- E-4. Patch management
- E-6. Defence capability against APT attack evaluation
- E-7. Handling capability on cyberattack evaluation
- F-1. Post-mortem analysis
- F-2. Internal threat intelligence collection and analysis
- F-4. Threat intelligence report
- H-1. Internal fraud response and analysis support
- I-3. Security consulting
- I-5. Collaboration service with external security communities
- I-6. Technical reporting

Ⅰ. Executed in-house

- A-1. Risk management
- A-2. Risk assessment
- A-3. Policy planning
- A-4. Policy management
- A-5. Business continuity
- A-6. Business impact analysis
- A-7. Resource management
- A-10. Counter measures selection
- A-11. Quality management
- D-2. Incident handling
- D-6. Incident notification
- D-7. Incident response report
- E-1. Network information collection
- E-2. Asset inventory
- E-8. Policy compliance
- F-5. Threat intelligence utilization
- G-11. Operates CDC/CSC systems
- I-1. Awareness
- I-2. Education and training
- I-5. Collaboration service with external security communities
- I-7. Executive security reporting

Ⅲ. Executed by specialized organisations

- C-1. Forensic analysis
- C-2. Malware sample analysis
- C-3. Tracking and tracing
- C-4. Forensic evidence collection
- D-4. Incident response and containment
- D-5. Incident recovery
- E-5. Penetration test
- F-3. External threat intelligence collection and evaluation
- G-3. Advanced operation for network security asset
- G-5. Advanced operation for endpoint security asset
- G-7. Advanced operation for cloud security products
- G-8. Deep analysis tool operation
- G-10. Advanced operation for analysis platform
- G-13. New security tools evaluation
- I-5. Collaboration service with external security communities

Ⅳ. Centered on the specialized organisations

- B-1. Real-time asset monitoring
- B-2. Event data retention
- B-3. Alerting and warning
- B-4. Handling enquiry on report
- E-3. Vulnerability assessment
- E-9. Hardening
- G-1. Security architecture implementation
- G-2. Basic operation for network security asset
- G-4. Basic operation for endpoint security asset
- G-6. Basic operation for cloud security products
- G-9. Basic operation for analysis platform
- G-12. Existing security tools evaluation
- H-2. Internal fraud detection and reoccurrence prevention support
- I-4. Security vendor collaboration
- I-5. Collaboration service with external security communities

Figure 19: service assignment for security response

© 2025 ISOG-J

6.5. Structure of security response organisation

6.5.1. Example for flat structure organisation

While it would be easier to discuss if "categories" directly equated to "organisational structure," the reality is often more complex. Therefore, this chapter organizes the concept of "organisational structure."

In practice, actual organisational structures vary widely between companies, making it extremely difficult to account for all these differences in discussions. To simplify, this section assumes an ideal organisational structure where all categories and services are arranged in a flat hierarchy under the CISO. Such a structure is often seen in "full insourcing" security organisations or specialized security firms.

A detailed example of such a structure is summarised in the following table[20]. It presents a matrix of "responsibilities" and "quadrants," with specific "services" listed within the matrix.

The table does not explicitly include "I-5. Collaboration with Security-Related Organisations". This is because this service is universally applicable across all quadrants. While some organisations might centralize this responsibility within a specific team, the fundamental principle is that it should be executed in all quadrants and services.

While this ideal structure may differ from your organisation's reality, the "services" themselves are clearly defined as outlined previously. You can adapt this framework to fit your organisation, thinking along the lines of, "This is handled by our ** department, and that is outsourced to ** company."

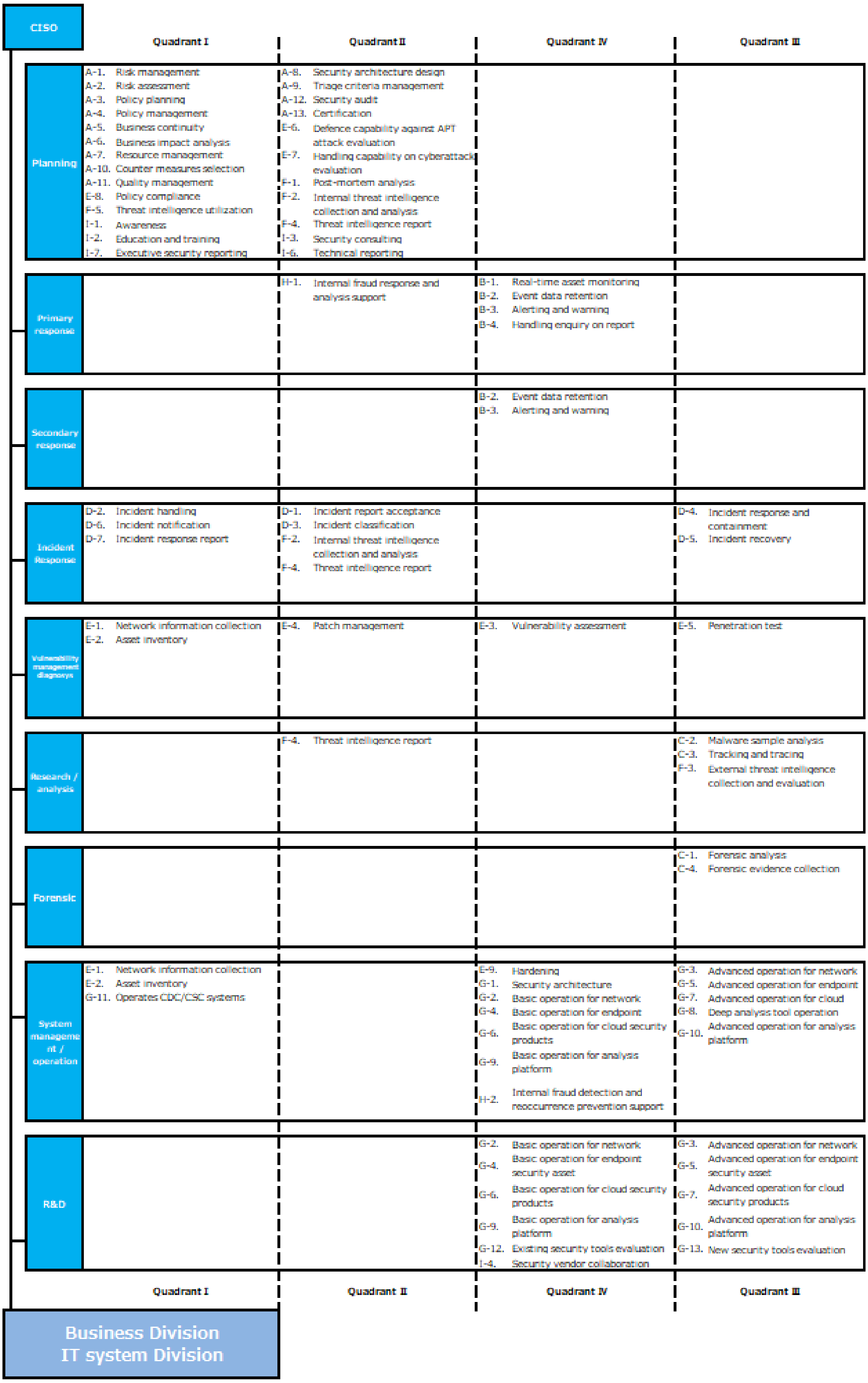
For organisations in the process of building a security response structure, this model can serve as a reference for designing and implementing an effective structure.

---

[20]

- The "quadrants" are arranged in the order I, II, IV, III. This sequence reflects a progressively increasing dependence on specialized organisations.
- For roles listed under multiple responsibilities, these are tasks likely to require joint efforts. In practice, even more responsibilities may collaborate to address security responses. The table should be viewed as representative examples. Collaboration within the same responsibility is assumed, and to avoid overcomplicating the table, the same service is not repeated across multiple quadrants.

© 2025 ISOG-J



	Quadrant I	Quadrant II	Quadrant IV	Quadrant III
Planning	A-1. Risk management A-2. Risk assessment A-3. Policy planning A-4. Policy management A-5. Business continuity A-6. Business impact analysis A-7. Resource management A-10. Counter measures selection A-11. Quality management E-8. Policy compliance F-5. Threat intelligence utilization I-1. Awareness I-2. Education and training I-7. Executive security reporting	A-8. Security architecture design A-9. Triage criteria management A-12. Security audit A-13. Certification E-6. Defence capability against APT attack evaluation E-7. Handling capability on cyberattack evaluation F-1. Post-mortem analysis F-2. Internal threat intelligence collection and analysis F-4. Threat intelligence report I-3. Security consulting I-6. Technical reporting		
Primary response		H-1. Internal fraud response and analysis support	B-1. Real-time asset monitoring B-2. Event data retention B-3. Alerting and warning B-4. Handling enquiry on report	
Secondary response			B-2. Event data retention B-3. Alerting and warning	
Incident Response	D-2. Incident handling D-6. Incident notification D-7. Incident response report	D-1. Incident report acceptance D-3. Incident classification F-2. Internal threat intelligence collection and analysis F-4. Threat intelligence report		D-4. Incident response and containment D-5. Incident recovery
Vulnerability management diagnosys	E-1. Network information collection E-2. Asset inventory	E-4. Patch management	E-3. Vulnerability assessment	E-5. Penetration test
Research / analysis		F-4. Threat intelligence report		C-2. Malware sample analysis C-3. Tracking and tracing F-3. External threat intelligence collection and evaluation
Forensic				C-1. Forensic analysis C-4. Forensic evidence collection
System management / operation	E-1. Network information collection E-2. Asset inventory G-11. Operates CDC/CSC systems		E-9. Hardening G-1. Security architecture G-2. Basic operation for network G-4. Basic operation for endpoint G-6. Basic operation for cloud security products G-9. Basic operation for analysis platform H-2. Internal fraud detection and reoccurrence prevention support	G-3. Advanced operation for network G-5. Advanced operation for endpoint G-7. Advanced operation for cloud G-8. Deep analysis tool operation G-10. Advanced operation for analysis platform
R&D			G-2. Basic operation for network G-4. Basic operation for endpoint security asset G-6. Basic operation for cloud security products G-9. Basic operation for analysis platform G-12. Existing security tools evaluation I-4. Security vendor collaboration	G-3. Advanced operation for network G-5. Advanced operation for endpoint security asset G-7. Advanced operation for cloud security products G-10. Advanced operation for analysis platform G-13. New security tools evaluation
	Quadrant I	Quadrant II	Quadrant IV	Quadrant III

Figure 20: organisational structure for security response

© 2025 ISOG-J

6.5.2. Example of general pattern for assignment on X.1060/JT-X1060

When building an organisational structure, two primary cases are considered: building a new structure from scratch or revising an existing one.

In” 5.2.2 Examples of how services are selected”, guidance was provided for creating a new structure, focusing on selecting "essential" services to enable daily operations within the management process. In that example, necessary services were identified at the level of Categories A, B, D, and G. By combining this with the "insource and outsource" allocation shown in” Figure 19: service assignment for security response”, it becomes easier to identify which services should be performed in-house and which can be outsourced.

For example, within "Quadrant I: Areas to Be Executed In-House," organisations can determine which services from Category A (e.g., A-1, A-2, A-3, A-4, A-5, A-6, A-7, A-10, A-11) are essential. This approach provides clarity on starting the management process in-house. t should be considered as a guide only, as which services are essential will vary from organisation to organisation. The same applies to Categories B, D, and G, where services within Quadrant I and Quadrant II can guide the initial selection of services that can be handled internally. The decision to insource or outsource ultimately depends on the organisation’s specific circumstances and is not necessarily confined to in-house execution.

For organisations that already have security structures such as SOCs or CSIRTs, improvements may be driven by various triggers. These could include significant changes in the environment after several years, resource shortages due to increased responsibilities, or even incidents that prompt a reassessment.

First, map existing activities onto the nine categories and 64 services. If certain services are missing, they can be added. This mapping process helps re-evaluate organisational goals and the recommended levels for services, confirming what additional services are necessary. New services should then be assigned appropriately. It is also essential to ensure that the structure enables the execution of the management process with Categories A, B, D, and G as a starting point. However, these categories alone are insufficient; it is vital to verify that no necessary services are overlooked.

For organisations starting small, perhaps with just one person, parts of the structure

© 2025 ISOG-J

can be outsourced or managed using hybrid models. The X.1060/JT-X1060 framework emphasizes flexibility during the allocation of services, allowing the organisation to function while utilizing external resources. Through the short- and long-term cycles of the management process, daily reviews, structural improvements, and skill development can enhance the organisation's capabilities over time. During the evaluation process, changes in circumstances—such as increased staff or improved skills—can inform the next construction process. Resource allocation decisions can be guided by recommended levels or assessment scores.

For example, if the focus is on prevention, services from Category F (Threat Intelligence Collection, Analysis, and Evaluation) or Category E (Diagnosis and Evaluation) can be selected to strengthen threat intelligence, diagnostics, and training.
For internal and external collaboration within and between organisations, as well as awareness-raising and training of personnel, services are to be selected from Category I (Proactive Collaboration with External Organisations). The process often begins with limited resources and expands over time, aiming for continuous improvement and better outcomes.

In recent years, security structures within organisations have become more diverse. Instead of having a single centralized security team, organisations may have teams focused on the entire company, specific business units, or individual products. X.1060/JT-X1060 provides examples of simple cases with one security team per organisation, while the Cybersecurity Management Guidelines Appendix F by Japan's Ministry of Economy, Trade, and Industry provides insights into the varied structures in Japanese organisations. These resources can help organisations adapt the elements of X.1060/JT-X1060 to their specific needs.

In cases where multiple security organisations across different companies or entities need to collaborate (e.g., in supply chain or partnership contexts), differences in security policies and approaches often exist. Here, X.1060/JT-X1060 can serve as a common language, enabling discussions on which services should be implemented to enhance overall security. If certain services must be jointly implemented, organisations could consider establishing a shared security team. They might also share information, collectively manage operations, or utilize a common outsourced provider for unified monitoring and operations.

© 2025 ISOG-J

6.6. Number of members for security response organisation

When considering the structure of a security response organisation, determining the required number of personnel is a critical factor. For Quadrants I and II, which involve tasks to be handled in-house, organisations can likely estimate staffing needs based on existing personnel, including staff from other departments, and the categories and services already aligned with their current operations.

On the other hand, Quadrants III and IV involve categories and services that may be entirely new to the organisation. Estimating the required number of personnel for these quadrants can be challenging. However, these quadrants represent the areas where significant decisions must be made regarding whether to cover the responsibilities in-house or outsource them. To make these decisions, it is essential to simulate and calculate the necessary personnel.

This section presents four model cases as simulations for staffing and operating personnel in Quadrants III and IV. These cases represent the minimum baseline and are meant to provide a starting point. Depending on the scale of operations, the number of sensors to be monitored, and compliance with organisational work regulations, additional personnel may be required. Each organisation should consider these cases in the context of their specific monitoring and operational scale.

Table 11 assignment model for security expert members

	Level 0	Level 1	Level 2	Level 3
primary response	1 for day	2 for day	1 for 24/7 (6 for team)	2 for 24/7 (12 for team)
secondary response	1 for day	1 for day	2 for day	1 for 24/7 (6 for team)
incident response	(secondary response concurrently serves)	1 for day	1 for day	2 for day
vulnerability management / diagnosis	(secondary response concurrently serves)	(incident response concurrently serves)	(incident response concurrently serves)	(incident response concurrently serves)

© 2025 ISOG-J

research / analysis	N/A	(secondary response concurrently serves)	(secondary response concurrently serves)	1 for day
forensic	N/A	N/A	(secondary response concurrently serves)	(research/analys is concurrently serves)
system operations and management	1 for day	2 for day	2 for day	3 for day
R&D	1 for day	1 for day	1 for day	2 for day
all	4 persons	7 persons	12 persons	26 persons

Level 0

This is the minimum team composition model, focusing on essential functions with no capacity for forensic investigations, research, or advanced analysis. Security response is handled with very simple response rules. It serves as a guideline for a trial team structure during the initial startup phase. In practice, a single incident can overwhelm the team, and even minor issues in security-related systems would overburden the system management team. Unless Quadrants I and II can support Quadrants III and IV, this model cannot serve as a practical structure.

Level 1

This model represents the bare minimum for a functional structure. While it does not include 24/7 coverage or forensic capabilities, it enables basic security response. If another organisation, such as a Network Operations Centre (NOC), provides 24/7 support, some easily standardized tasks, such as "primary response" and "system operations and management", can be outsourced to supplement this model effectively.

Level 2

A model with a dedicated 24/7 security team. With this scale, the organisation can achieve comprehensive security response capabilities. If the goal is to establish an in-house private SOC, this model serves as the baseline. For both Level 2 and Level 3 (described below), the primary triage function within "system operations and management" is integrated into "primary response" to improve efficiency, eliminating

© 2025 ISOG-J

the need for a separate 24/7 system operations team.

Level 3

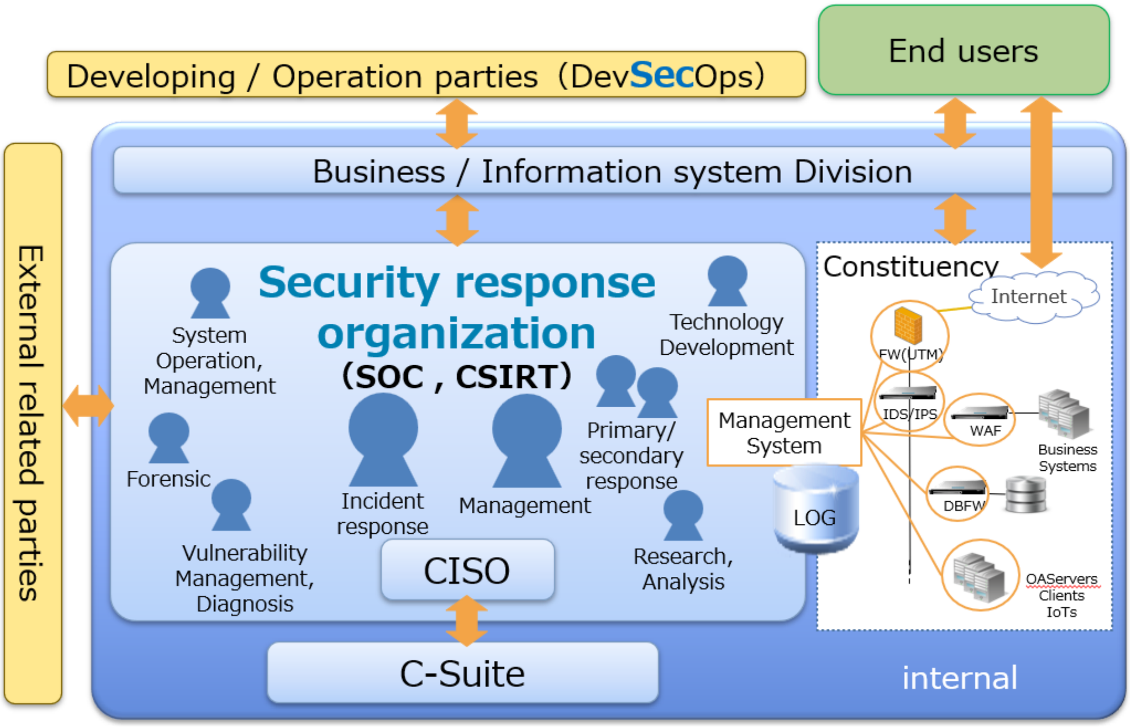
This model goes beyond supporting a single organisation, covering multiple related entities such as branches, subsidiaries, or group companies nationwide. For global enterprises, Level 3 can be scaled up and centralized at a single location or distributed based on the size of operations in each region. Smaller regional operations may adopt Level 1 or Level 2 models as branches, while the largest regional operation houses a Level 3 structure to oversee and manage the entire hierarchy.

© 2025 ISOG-J

7. Relations between categories and services

The categories and services organized thus far operate in collaboration with external organisations, as illustrated in” Figure 21: the environment surrounding security organisations”. This section explains how the categories and services within the security response organisation interact using relationship diagrams and workflows.

The explanation is structured around two scenarios: "when an incident occurs" and "during normal operations without incidents." For each scenario, the operational dynamics of the categories and services are outlined, demonstrating how they function in their respective contexts.



Developing / Operation parties（DevSecOps)
End users
External related parties
Business / Information system Division
Security response organization
(SOC , CSIRT)
System Operation, Management
Technology Development
Forensic
Incident response
Management
Primary/ secondary response
Vulnerability Management, Diagnosis
CISO
Research, Analysis
Management System
LOG
Constituency
Internet
FW(UTM)
IDS/IPS
WAF
Business Systems
DBFW
OAServers Clients IoTs
C-Suite
internal

Figure 21: the environment surrounding security organisations

© 2025 ISOG-J

7.1. Flow in incident response

The overall flow during an incident response remains largely consistent across different cases. First, the relationship between the baseline incident response categories and services is illustrated as an example. These relationships are aligned with the categories and services described in" 6.5 Structure of security response organisation" and are shown in " Figure 22: relationships during incident response".

1 The monitoring state must be maintained continuously.
2 Incident response begins when an event is triggered.
    - Triggers may include external reports, alerts from monitoring systems, or vulnerability notifications requiring confirmation by the CISO.
3 Determine if the Event Requires Incident Response.
    - Assessing whether the event qualifies as an incident is handled within Quadrant II (D-1, D-3, D-4). Based on the collected information, determine if the event qualifies as an incident.
4 Conduct Detailed Investigation of Incident Information
    - Gather information and assess the impact to manage the situation effectively. This involves directing specialized data collection efforts, including primary responses in Quadrant IV, advanced secondary responses in Quadrants III and IV, and forensic investigations in Quadrant III for confirmed damages. If countermeasures need to be derived based on the attack background, utilize research and analysis from Quadrant III.
5 Evaluate the Incident's Impact and Priority
    - Assess the impact and priority of the incident using the collected information within Quadrant II (D-3).
6 Take Measures to Resolve the Incident
    - Manage the incident within Quadrant I (D-2) and implement response measures in Quadrant II (D-4). After resolving the incident, compile reports within Quadrant I (D-6, D-7).
7 Declare the Conclusion of Incident Response
    - Once the impacts, damages, and necessary actions have been fully addressed, declare the conclusion of the incident response. If the incident is unresolved, continue information gathering and responses until

© 2025 ISOG-J

resolution.

8 Reports summarizing the incident and response are prepared and made public as necessary.

Note: For details on Quadrants I/II/III/IV, refer to" Figure 22: relationships during incident response".

© 2025 ISOG-J

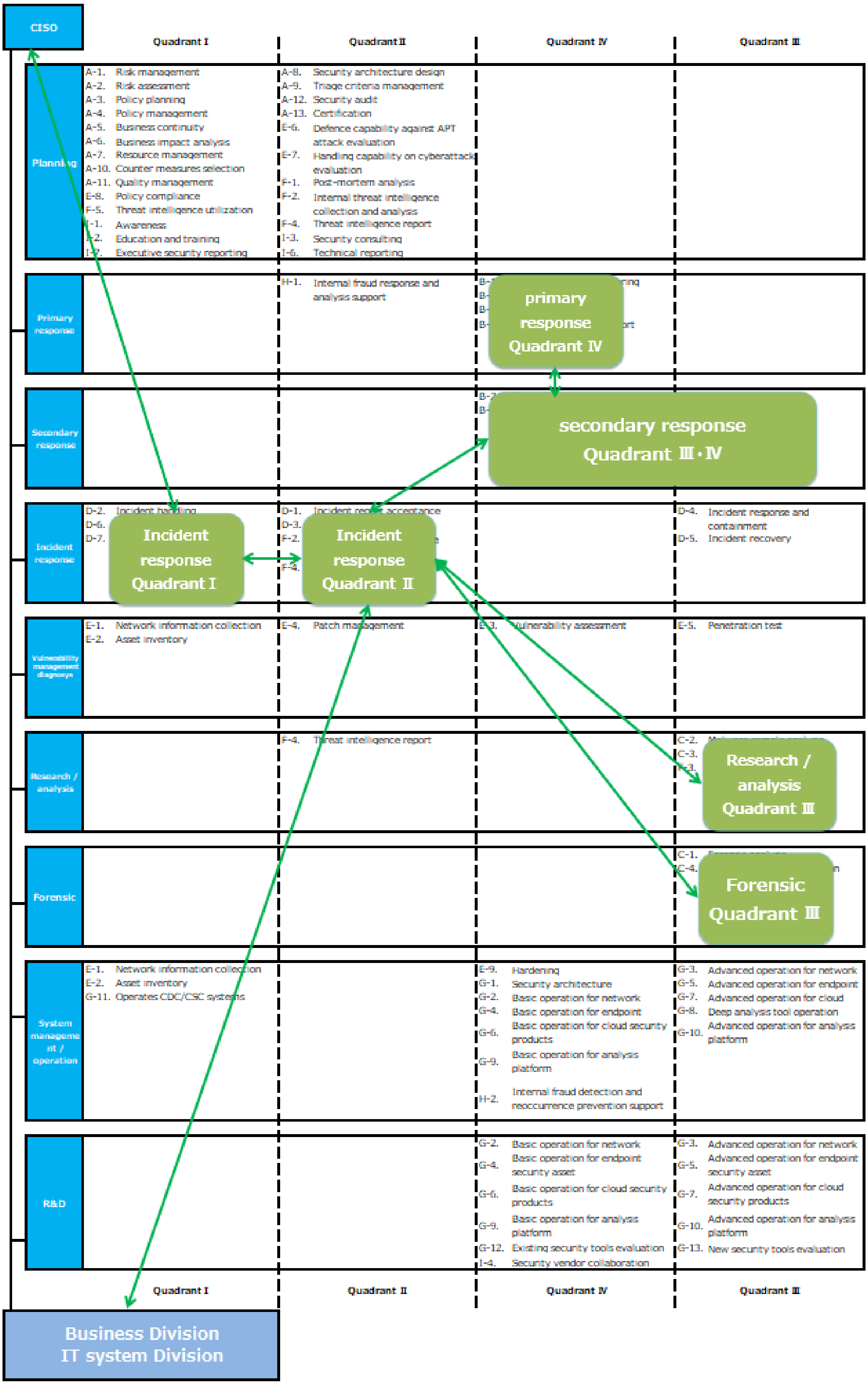

CISO
Quadrant I
Quadrant II
Quadrant IV
Quadrant III
Planning
A-1. Risk management
A-2. Risk assessment
A-3. Policy planning
A-4. Policy management
A-5. Business continuity
A-6. Business impact analysis
A-7. Resource management
A-10. Counter measures selection
A-11. Quality management
E-8. Policy compliance
F-5. Threat intelligence utilization
I-1. Awareness
I-2. Education and training
I-7. Executive security reporting
A-8. Security architecture design
A-9. Triage criteria management
A-12. Security audit
A-13. Certification
E-6. Defence capability against APT attack evaluation
E-7. Handling capability on cyberattack evaluation
F-1. Post-mortem analysis
F-2. Internal threat intelligence collection and analysis
F-4. Threat intelligence report
I-3. Security consulting
I-6. Technical reporting
Primary response
H-1. Internal fraud response and analysis support
primary response Quadrant IV
Secondary response
secondary response Quadrant III・IV
Incident response
D-2. Incident handling
D-6.
D-7.
Incident response Quadrant I
D-1. Incident report acceptance
D-3.
F-2.
F-4.
Incident response Quadrant II
D-4. Incident response and containment
D-5. Incident recovery
Vulnerability management diagnosys
E-1. Network information collection
E-2. Asset inventory
E-4. Patch management
E-3. Vulnerability assessment
E-5. Penetration test
Research / analysis
F-4. Threat intelligence report
C-2.
C-3.
F-3.
Research / analysis Quadrant III
Forensic
C-1.
C-4.
Forensic Quadrant III
System management / operation
E-1. Network information collection
E-2. Asset inventory
G-11. Operates CDC/CSC systems
E-9. Hardening
G-1. Security architecture
G-2. Basic operation for network
G-4. Basic operation for endpoint
G-6. Basic operation for cloud security products
G-9. Basic operation for analysis platform
H-2. Internal fraud detection and reoccurrence prevention support
G-3. Advanced operation for network
G-5. Advanced operation for endpoint
G-7. Advanced operation for cloud
G-8. Deep analysis tool operation
G-10. Advanced operation for analysis platform
R&D
G-2. Basic operation for network
G-4. Basic operation for endpoint security asset
G-6. Basic operation for cloud security products
G-9. Basic operation for analysis platform
G-12. Existing security tools evaluation
I-4. Security vendor collaboration
G-3. Advanced operation for network
G-5. Advanced operation for endpoint security asset
G-7. Advanced operation for cloud security products
G-10. Advanced operation for analysis platform
G-13. New security tools evaluation
Quadrant I
Quadrant II
Quadrant IV
Quadrant III
Business Division
IT system Division

Figure 22: relationships during incident response

© 2025 ISOG-J

In” Figure 22: relationships during incident response”, the relationships between categories and services were illustrated. When summarised as an incident response flow, it can be represented as shown in” Figure 23: flow in incident response”.

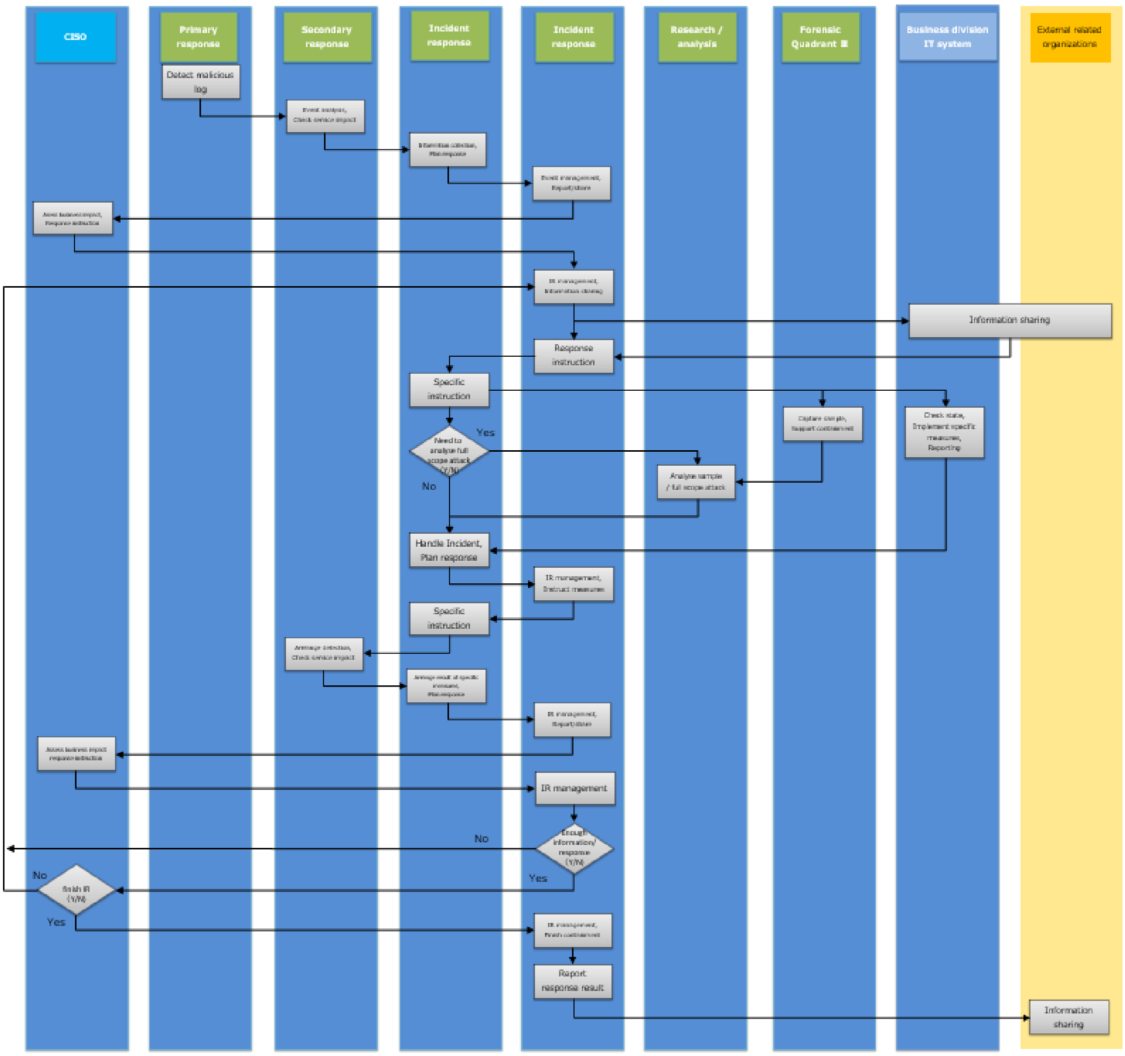

CISO
Primary response
Secondary response
Incident response
Incident response
Research / analysis
Forensic Quadrant Ⅲ
Business division IT system
External related organizations
Detect malicious log
Event analysis, Check service impact
Information collection, Plan response
Event management, Report/share
Assess business impact, Response instruction
IR management, Information sharing
Information sharing
Response instruction
Specific instruction
Need to analyse full scope attack (Y/N)
Yes
No
Capture sample, Support containment
Check state, Implement specific measures, Reporting
Analyse sample / full scope attack
Handle Incident, Plan response
IR management, Instruct measures
Specific instruction
IR management, Report/share
IR management
Enough information/ response (Y/N)
No
Yes
finish IR (Y/N)
No
Yes
IR management, Finish containment
Report response result
Information sharing

Figure 23: flow in incident response

The relationships between categories and services during incident response, as depicted in ” Figure 22: relationships during incident response” and” Figure 23: flow in incident response”, may vary depending on the specific incident. This section explains these differences using the following two examples.

The examples are based on the annual "Top 10 Threats" for organisations published by

© 2025 ISOG-J

the Information-Technology Promotion Agency (IPA, Japan) and focus on the following two threats:

- A client device is attacked: "Damage caused by ransomware"
- A server is attacked: "Theft of personal information from web services"

7.1.1. Example: “Damage caused by ransomware”

Recently, attacks involving "ransomware" - where an end user's files are encrypted, rendering them inaccessible until a ransom is paid - have been on the rise. This section uses an example where a user's device is infected with ransomware and files are encrypted, demonstrating the associated relationships and flow.

Common ransomware often infiltrates systems via email attachments, infecting devices when users mistakenly click on them. For example, the infamous ransomware WannaCry spread as a worm via network connections, primarily targeting Windows devices that lacked proper patch updates. This type of incident could have been prevented through proactive measures during normal operations, such as applying patches and maintaining effective asset management within the organisation.
Prevention through regular proactive measures is crucial. Organisations are strongly encouraged to implement such measures during normal operations. Details on responses during normal operations will be discussed later.

- Features of this scenario

When infected with ransomware, it is often discovered on devices such as employee terminals or servers within the organisation, leading to inquiries or reports from within the organisation. Incident response typically progresses from these internal communications. In this case, the steps for event reception, assessment, and management align with the baseline response process.

In this scenario, the key difference from the baseline response is that the user's device is encrypted, and decryption (i.e., unlocking the encryption) is not possible. However, there is no information leakage, which distinguishes this case from other incidents.

- Features of “category and service relationships” and ”flow during incident response”

Based on the baseline response, the distinguishing aspects of this incident involve the

© 2025 ISOG-J

implementation of "Research and Analysis" and "Forensic Investigation." In the case of ransomware, the following three points need to be considered:

- route of infection
- behaviour of ransomware
- availability of decryption

If it is determined that ransomware has caused an information leak, responses to address the leak must also be considered.

The flow from Figure 23: does not change due to the nature of the malware (e.g., ransomware). However, in this case, the following categories and services are notable for their roles in the response:

- route of infection
  Check with Quadrants III for primary response and Quadrants III/IV for secondary response.
- behaviour of ransomware
  Check with Quadrants III for research and analysis and forensic investigations
- availability of decryption
  same as above

Note: For details on Quadrants I/II/III/IV, refer to" Figure 22: relationships during incident response".

In cases where there is no information leakage, forensic investigations and evidence preservation are not prioritised.

On the other hand, there are cases of double extortion, where sensitive information is exfiltrated before being encrypted and later used to demand ransom. This scenario differs from cases where data becomes inaccessible due to encryption. The next example will address cases involving information leakage.

7.1.2. Example: "Theft of personal information from web services"

Regarding attacks on servers, there is a growing trend of shorter timeframes between the disclosure of a vulnerability and the start of attacks exploiting it. It is not uncommon for personal information to be leaked in cases where systems are targeted and attacked shortly after a vulnerability is disclosed.

This case considers a scenario where a vulnerability is disclosed, but an attack occurs before countermeasures can be implemented, resulting in the leakage of personal information. The associated relationships and flow for this situation are illustrated as

© 2025 ISOG-J

follows.

- Features of this incident case

As an example, consider a case like Apache Struts, where a vulnerability is disclosed, and attacks begin shortly thereafter, leading to the leakage of personal information.

The initial trigger in such a scenario might be news or information about the vulnerability, or a report indicating that the website has already been compromised. In some cases, monitoring systems may detect exploit code, revealing that an attack is underway. It is also possible for various types of information to be received simultaneously, leading to the identification of the incident.

Regardless of the trigger, the process of receiving this information, determining it to be an incident, and initiating management follows the same flow as the baseline response.

- Features of "category and service relationships" and "flow during Incident response"

In this case, the analysis assumes that an attack has already occurred. The discussion highlights the following three key points:

- Where the attack originated and how it was executed
- What information was leaked
- What measures should be taken to minimize the damage

It may be necessary to decide to temporarily shut down the website until the countermeasures are implemented and the extent of the damage is determined. Early reporting and decision-making by the CISO are essential for prompt responses.

Since the attack is ongoing, the damage assessment and countermeasures must be conducted simultaneously. The following categories and services are notable for addressing this scenario:

- Where the attack originated and how it was executed
  Information is verified in primary response (Quadrant IV) and secondary response (Quadrants III and IV).
- What information was leaked
  The extent of the damage is determined through research and analysis, as well as forensic investigation (Quadrant III).
- What measures should be taken to minimize the damage
  Research and analysis or forensic investigation (Quadrant III) are used to determine the full scope of the attack.
  Vulnerability information from" E. checking and evaluation" is referenced to

© 2025 ISOG-J

decide on countermeasures.
Note: Refer to" Figure 22: relationships during incident response" for details on Quadrants I/II/III/IV.

If traces of the attack reveal that the attack failed and defences held, it may be possible to take countermeasures and decide to continue operating the site. As the impact and damage are assessed, incident management and response will continue until the incident is resolved.

7.1.3. Example: "Incident in the supply chain"

Recently, incidents affecting related organisations, companies, or business partners have increasingly resulted in damage to one's own organisation. The incident response for each related entity follows the same basic flow as previously described.
When the scope of incident response in your organisation extends beyond its boundaries and impacts other organisations, it is essential to coordinate with them. Afterward, through review and evaluation, confirm what measures could have been taken by each organisation and across organisations to improve the response.

In the case of a parent-subsidiary or group company relationship, the structure of the security response organisation tends to be hierarchical. If the incident response extends beyond your organisation, you respond within the scope of authority delegated by the higher-level organisation. When the response exceeds your authority, escalate the issue to the higher-level organisation for resolution. If it falls within your authority, you expand the scope of response by notifying the relevant companies or organisations.

In contrast, relationships with business partners or subcontractors differ from those within a parent-subsidiary or group structure. In such cases, incident response is based not on authority but on the terms and scope defined by mutual agreements or contracts. Effective incident response requires close sharing of information and status between parties.
As part of preparation, within the scope of normal operations (discussed later), organisations should conduct training and exercises for incident response regularly. Additionally, each organisation must ensure it is ready to respond effectively in case an incident occurs.

© 2025 ISOG-J

7.2. Activities during normal operations

The preceding sections have outlined the categories and services relevant to the response flow during incidents. Conversely, during normal operations, there are crucial activities aimed at preventing incidents or enabling a swift response when incidents occur. These routine activities are summarised under "A. strategic management of CDC/CSC"(A-12) and "I. active relationship with external parties" (I-7), with their outcomes reported to management and other relevant stakeholders.

According to JPCERT/CC[21], the activities performed during normal operations and those during incidents are organized as shown in "Figure24: Activities of CSIRT"

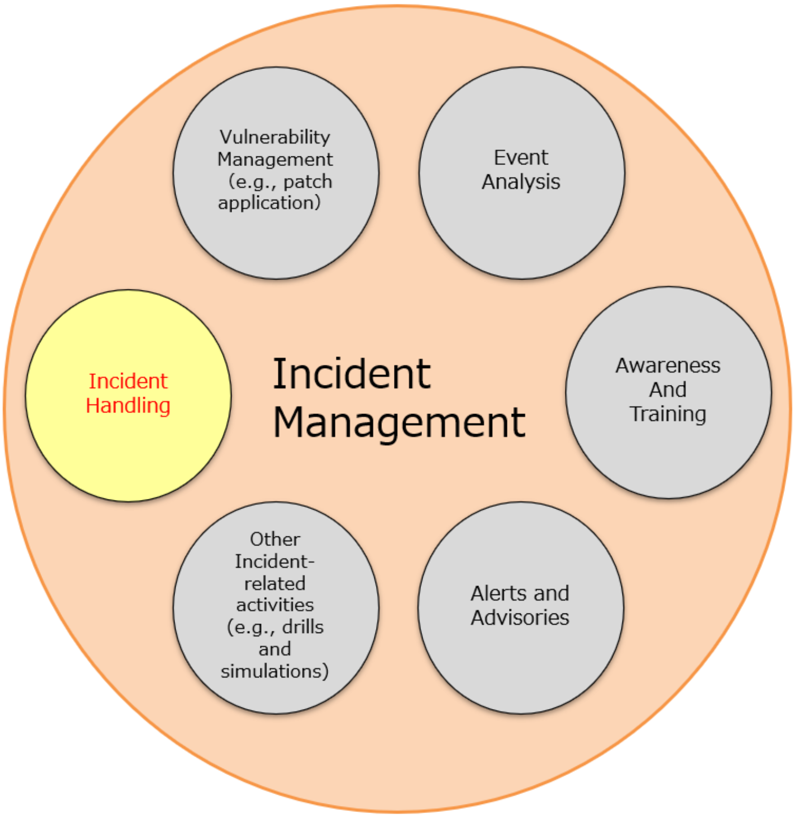

Vulnerability Management (e.g., patch application)
Event Analysis
Incident Handling
Incident Management
Awareness And Training
Other Incident-related activities (e.g., drills and simulations)
Alerts and Advisories

Figure24: Activities of CSIRT

This figure lists six types of activities, showing that while the central activity during an incident is singular, there are as many as five activities conducted during normal operations.

---

[21] Modified the figure in this reference.
http://www.jpcert.or.jp/m/csirt_material/files/manual_ver1.0_20151126.pdf

© 2025 ISOG-J

1. Vulnerability Management (e.g., patch application)
2. Event Analysis
3. Awareness and Training
4. Alerts and Advisories
5. Other Incident-Related Activities (e.g., drills and simulations)

The following outlines the implementation details for these activities during normal operations and examples of the expected deliverables:

7.2.1. Vulnerability management (e.g., patch application)

Regularly collect vulnerability information and, if necessary, prompt administrators to apply patches. It is essential to maintain an ongoing understanding of what servers exist within the organisation, what versions of software are in use, and their configurations.

On the user-side devices, regularly monitor operating systems, browsers, plugin software, and office-related products used on client devices to ensure vulnerabilities are addressed, issuing alerts and advisories as necessary.

In vulnerability management, it is crucial to maintain a clear understanding of the current state of systems. Preparing in advance is essential to avoid scrambling to investigate the configuration of servers or user devices when vulnerability information is released.

This activity primarily falls under the “E. checking and evaluation” category.

- Output

  Examples of audit results include the following:

  - The latest system configuration status
  - The latest system patch application status
  - The number of vulnerability advisories issued in the past month
  - The number of systems with unpatched vulnerabilities

  And more.

By quantifying how well the current state is understood, how promptly vulnerability advisories were issued, and to what extent systems were updated as a result, it becomes possible to evaluate the effectiveness of routine measures during normal operations.

7.2.2. Event analysis

In daily information gathering, analyse current prevalent attack types, techniques being employed, and even the background of attackers to understand the present threats.

By consistently collecting and accumulating information in preparation for potential

© 2025 ISOG-J

incidents, insights and countermeasures can be derived from past similar cases. Regarding the background of attackers, it is necessary to gather a wide range of information, as various factors such as anniversaries of international events, incidents, or political statements could be relevant triggers. Without regular accumulation of information, it becomes challenging to consider the connections behind an attack, highlighting the need for continuous collection efforts.

Analyzing security events that occurred within your organisation - even those that did not escalate into incidents - can help identify prevalent attack trends and measure the effectiveness of security measures based on event tendencies.

This task primarily falls under the “F. collection, analysis and evaluation of threat intelligence” category.

- Output

Examples include regular threat trend reports:

- The number and details of detected attacks and security events within your organisation or company.
- The methods, trends, and details of socially observed attacks

Analyze current prevalent attacks, what is being targeted, and commonly implemented countermeasures. These insights also contribute to awareness and training initiatives discussed later.

7.2.3. Awareness and training

Promote awareness and education regularly to ensure appropriate measures are taken for applying patches after vulnerabilities are disclosed and to counter various types of attacks.

In recent years, incidents have not been limited to cyberattacks but also include human errors by employees, such as the loss of USB drives or laptops, and misconfigurations in cloud services, leading to massive personal information leaks. To address such incidents, continuous improvement in literacy and awareness is essential.

For companies that have obtained certifications such as ISMS or Privacy Mark, regular employee training sessions and educational opportunities for personnel are often taken place. However, companies without such certifications should utilize publicly available resources, such as those from IPA, to enhance employee awareness and foster a security-conscious culture.

This task is primarily carried out under the “I. active relationship with external parties” category, specifically the I-1, I-2, and I-3 services.

© 2025 ISOG-J

- Output

The performance of awareness and educational activities can be demonstrated by using indicators such as the frequency, content, target employees or personnel, and whether the necessary information was provided to the appropriate audience.

For example, the content of awareness efforts should differ for roles that require opening emails, such as managerial or executive positions, compared to employees or personnel in general roles where email usage is limited. Similarly, for those managing systems, it is essential to provide information on patch management, trends in system attacks, and the corresponding countermeasures.

7.2.4. Alerts and advisories

Based on the vulnerability management and event analysis described above, organisations can issue alerts on what requires immediate attention and how to respond, enabling proactive measures to be taken before incidents occur.

For server and system administrators, it is effective to provide guidance on addressing vulnerabilities in publicly accessible servers or countering globally prevalent attacks. Similarly, for end-users, sharing information about software updates and issuing warnings about mass phishing or targeted attack emails can be highly beneficial.

Alerts can be based on notifications from organisations such as JPCERT/CC, IPA, or the National Police Agency. However, it is crucial to regularly gather information so that, when issuing alerts, the content can be quickly understood and disseminated.

This task primarily leverages the information collected in the categories of “E. checking and evaluation” and “F. collection, analysis and evaluation of threat intelligence”, with the services in “I. active relationship with external parties” (I-1, 2, 3) playing a central role.

- Output

The following examples can be cited:

- Number of alerts issued this month
- Number of systems or users addressed through the alerts

The extent to which the alerts contributed to defence, and whether incidents could be prevented as a result.

The key point lies in determining how effectively the alerts supported defensive measures and whether they successfully prevented incidents from occurring.

© 2025 ISOG-J

7.2.5. Other incident-related activities (e.g., drills and simulations)

This sub-section covers other related tasks that do not fall into the previous categories are allocated, such as rehearsals, resource management, and personnel training.

For rehearsals, a common example is purchasing services that simulate targeted phishing attacks by sending mock emails to train end users. However, to comprehensively train for security responses, it is essential to simulate an incident and verify response procedures, including workflows and decision-making by management.

Exercises tailored for CSIRTs, such as practical cyber defence training (Cyber Defence Exercise with Recurrence: CYDER by NICT, Japan) or competitions like the Hardening Project, offer methods to evaluate overall preparedness for incident responses.

This work is primarily carried out under the services “E. checking and evaluation” (E-6, E-7) and “I. active relationship with external parties”(I-5).

Additionally, managing resources, ensuring quality in security responses, and maintaining overarching policies are crucial. It is during regular operations that "A. CDC Strategic Management" should be planned and executed systematically.

- Output

Taking rehearsals as an example, performance can be measured based on the participants involved and the scope and content of the exercises or training conducted.

If the scope of rehearsals and training is insufficient, it is essential to systematically plan who should be included, what content should be covered, and progressively implement these activities.

© 2025 ISOG-J

8. Security response organisation assessment

This section provides an overview of the assessments used to objectively evaluate security response organisations.

8.1. Purpose of assessment

The goal of assessing a security response organisation is to clarify the following:

- Identifying the "Strengths" and "Weaknesses" of the current security response organisation
    - By evaluating the current state of the organisation, the assessment aims to highlight:
        - Strengths: The categories and services that are adequately fulfilled, which can serve as points of pride or evidence of successful past initiatives.
        - Weaknesses: Areas that are insufficiently addressed, allowing the identification of improvement opportunities for short-term cycles.

- Determining the key points needed to achieve the desired future model
    - By setting medium- to long-term goals, the assessment aims to identify structural or fundamental issues that require long-term cycle adjustments, which cannot be resolved through short-term improvements alone.

These assessments are conducted under “A-12 Security audit” and play a critical role in the “A-1 Risk management” process to support the operation of the security response organisation.

In X.1060/JT-X1060, at the final phase of the build process, the assessment is used to confirm the current "As-Is" score and the target "To-Be" score for each selected service, and to create a service portfolio.

This assessment is not only used during the build process but also applied in the evaluation process. The target "To-Be" scores are defined during the build process, and in the evaluation process, the current status of the service portfolio is compared against them to identify improvements for the next build process.

© 2025 ISOG-J

8.2. Assessment workflow

Conducting an assessment systematically involves the following steps:

1. Refer to Section “6.3 Organisational pattern for security response” to determine which organisational pattern closely matches your current structure. Ensure alignment and consensus within the organisation on this determination.
2. Using Section “6.3 Organisational pattern for security response”, decide which organisational pattern serves as the aspirational model for medium- to long-term goals. Align this vision across all relevant organisational stakeholders.
3. Assess the implementation levels (as detailed in later sections) for each service within the current organisational pattern identified in Step 1. Collaborate with the individuals or teams primarily responsible for each category and service to ensure accurate evaluations.
4. Based on the evaluations in Step 3, highlight categories with high scores as "Strengths", identify categories with low scores as "Weaknesses."
5. Compare the evaluations in Step 3 with the target model identified in Step 2. Extract areas with significant gaps as key improvement points for medium- to long-term organisational development.

8.3. Service scores

To establish objective criteria for assessment, it is necessary to define the service scores of each service. In X.1060/JT-X1060, the criteria are defined as follows:

- Services are provided by a team within the organisation. (insource)
  - Documented operation is authorized by CISO or other organisational director who has appropriate responsibilities. (+5 points)
  - Operation is documented and others can play the role of existing operator .(+4 points)
  - Operation is not documented, and others can play the partial role of existing operator temporarily. (+3 points)
  - Operation is not documented, and the existing operator can play role. (+2 points)
  - Operation is not working. (+1 point)
  - Decided not to implement by insourcing. (N/A)

© 2025 ISOG-J

- Services are provided by a team outside of the organisation. (outsource)
    - Content of service and expected output are understood and their outputs are as expected. (+5 points)
    - Content of service and expected output are understood but their outputs are not as expected. (+4 points)
    - Either content of service or expected output is not understood. (+3 points)
    - Both content of service and expected output are not understood. (+2 points)
    - Nether output nor report is not reviewed. (+1 point)
    - Decided not to implement by outsourcing. (N/A)

The assessment conducted here aims to clarify the current state and goals of the organisation and enable continuous improvement to build a sustainable organisation. The evaluation approach considers two key aspects: insourcing, where services are handled internally, and outsourcing, where services are entrusted to external entities.

For insourced services, the focus is on evaluating whether responses are handled organisationally rather than relying on specific individuals. Many organisations face limitations in security personnel, and reliance on individual expertise poses a risk. If a key individual is absent or leaves the organisation, security responses could collapse entirely. Therefore, it is critical to ensure that tasks are performed at an organisational level.

The target scores for insourced activities should align with the organisation's current state and aspirations. For instance, if an organisation is constrained by budget or human resources and accepts a degree of reliance on individuals, a score of 2 or 3 may not be problematic. Conversely, if the goal is to move away from dependence on individuals, maintaining a score below 3 without improvement indicates an issue. Instead of indiscriminately striving for a score of 5 across all categories, it is more important to set realistic goals, evaluate the current situation appropriately, and address gaps systematically.

For outsourced services, the key evaluation point is whether the organisation understands and effectively utilizes the services provided. This approach ensures the organisation avoids a "set-it-and-forget-it" mentality. While organisations may carefully review service details when signing a contract, over time, awareness can fade, or the original team members involved in the contract discussions may leave, leading to a lack

© 2025 ISOG-J

of understanding of the service's specifics. As long as the organisation can operationalize the results from outsourced services, this is not a significant problem. However, failure to do so diminishes the value of outsourcing, potentially turning it into a costly yet ineffective endeavour.

A shared principle between insourcing and outsourcing is that categories intentionally marked as "not implemented" based on organisational decisions are excluded from maturity evaluations. If risks can be transferred or avoided through means other than security measures, this is acceptable. For instance, it is realistic to weigh business risks against security costs and decide to accept certain risks. However, it is essential to maintain records of the rationale and evidence supporting such decisions, ensuring flexibility to reassess as situations evolve.

8.4. Service portfolio sheet for security response organisation

In this book, a service portfolio is created as part of the build process. A template sheet for the service portfolio is provided in the appendix.

To make effective use of this template, avoid assigning responsibilities or scoring assessments based solely on subjective judgments. Conducting interviews with the relevant personnel can result in a more accurate and effective portfolio.

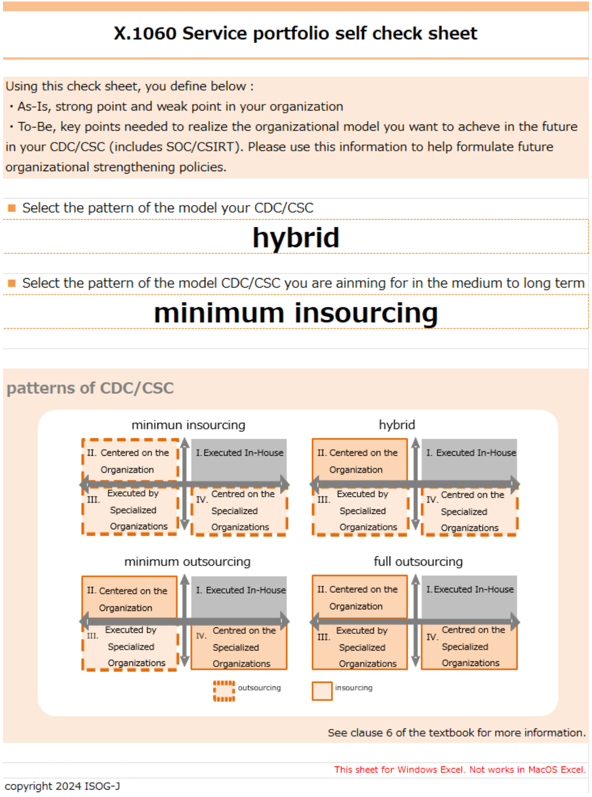
When assigning each service, it is advisable not only to list department or team names but also to include the names of responsible managers and individual staff members. Doing so clarifies accountability and helps identify any imbalances or areas requiring additional support.

8.5. Service portfolio self-check sheet for security response organisation

A self-check sheet has been prepared as an appendix to this book to facilitate the implementation of the self-check process summarised so far. This sheet allows users to easily perform self-assessments. Below, the usage of the sheet is explained.

© 2025 ISOG-J

■ sheet for starting



X.1060 Service portfolio self check sheet

Using this check sheet, you define below :
・As-Is, strong point and weak point in your organization
・To-Be, key points needed to realize the organizational model you want to acheve in the future in your CDC/CSC (includes SOC/CSIRT). Please use this information to help formulate future organizational strengthening policies.

■ Select the pattern of the model your CDC/CSC

hybrid

■ Select the pattern of the model CDC/CSC you are ainming for in the medium to long term

minimum insourcing

patterns of CDC/CSC

minimun insourcing
hybrid
minimum outsourcing
full outsourcing
II. Centered on the Organization
I. Executed In-House
III. Executed by Specialized Organizations
IV. Centred on the Specialized Organizations
outsourcing
insourcing

See clause 6 of the textbook for more information.

This sheet for Windows Excel. Not works in MacOS Excel.

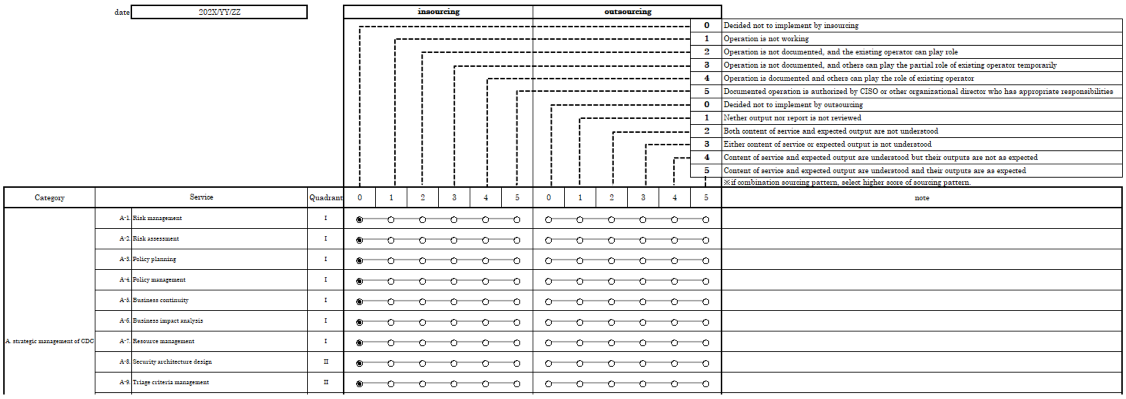
copyright 2024 ISOG-J

1. Select the current pattern of security response organisation

2. Select the future model pattern of security response organisation

Scores can be defined based on these choices.

■ self-check sheet



date 202X/YY/ZZ

0	Decided not to implement by insourcing
1	Operation is not working
2	Operation is not documented, and the existing operator can play role
3	Operation is not documented, and others can play the partial role of existing operator temporarily
4	Operation is documented and others can play the role of existing operator
5	Documented operation is authorized by CISO or other organizational director who has appropriate responsibilities
0	Decided not to implement by outsourcing
1	Nether output nor report is not reviewed
2	Both content of service and expected output are not understood
3	Either content of service or expected output is not understood
4	Content of service and expected output are understood but their outputs are not as expected
5	Content of service and expected output are understood and their outputs are as expected

※if combination sourcing pattern, select higher score of sourcing pattern.

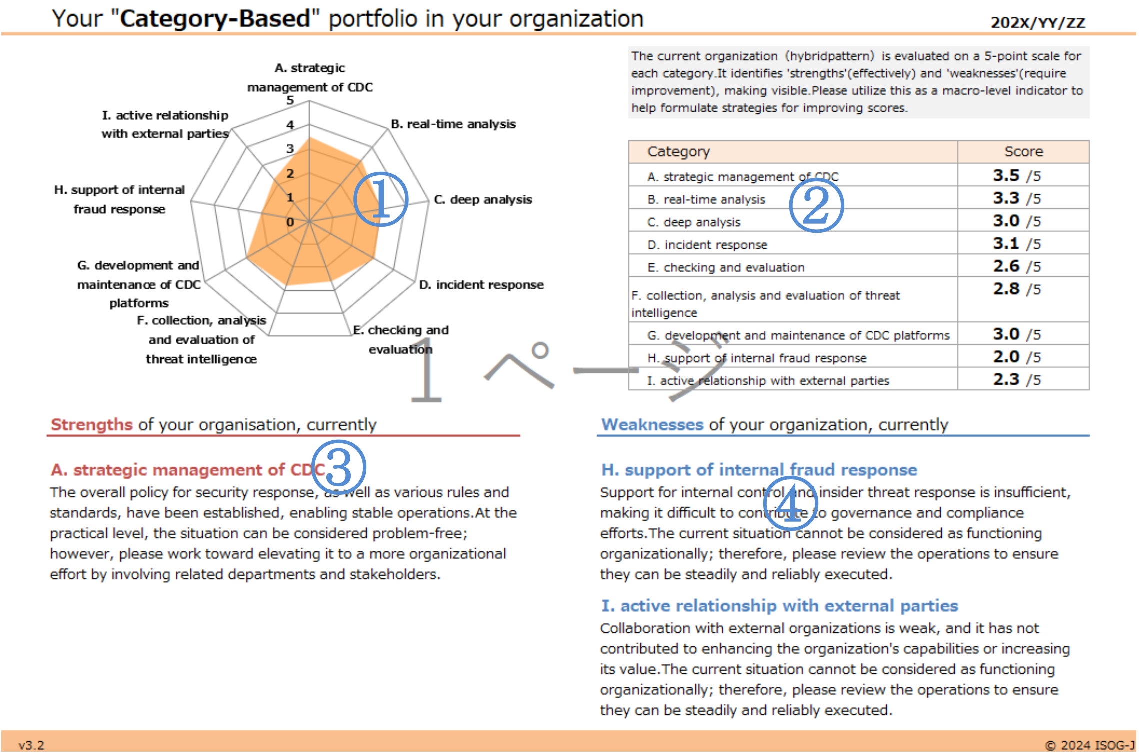
Category	Service		Quadrant	**insourcing**						**outsourcing**						note
				0	1	2	3	4	5	0	1	2	3	4	5	
A. strategic management of CDC	A-1.	Risk management	I	●	○	○	○	○	○	○	○	○	○	○	○	
	A-2.	Risk assessment	I	●	○	○	○	○	○	○	○	○	○	○	○	
	A-3.	Policy planning	I	●	○	○	○	○	○	○	○	○	○	○	○	
	A-4.	Policy management	I	●	○	○	○	○	○	○	○	○	○	○	○	
	A-5.	Business continuity	I	●	○	○	○	○	○	○	○	○	○	○	○	
	A-6.	Business impact analysis	I	●	○	○	○	○	○	○	○	○	○	○	○	
	A-7.	Resource management	I	●	○	○	○	○	○	○	○	○	○	○	○	
	A-8.	Security architecture design	II	●	○	○	○	○	○	○	○	○	○	○	○	
	A-9.	Triage criteria management	II	●	○	○	○	○	○	○	○	○	○	○	○	

For each role, it is possible to select the indicators defined in “8.3 Service scores”. The checkboxes on the sheet should be completed for the organisation through interviews or other means. As noted, if both insource and outsource options are utilized, you may choose and record the higher score.

If it is unclear which level is applicable, it is reasonable to select "1" for either insource or outsource. Additionally, a remarks column is provided for any special notes you wish to include. This section can be used this section for memos or additional observations; however, it will not affect the scoring.

■ result sheet

Once the "Preparation Sheet" and the "Input Sheet" are completed, the results are automatically reflected in the "Result Sheet." In the "Result Sheet," you can visualize the "Category Scores" and "Service Scores". The details of each score visualization are as follows:


①
②
③
④
5
4
3
2
1
0
A. strategic management of CDC
B. real-time analysis
C. deep analysis
D. incident response
E. checking and evaluation
F. collection, analysis and evaluation of threat intelligence
G. development and maintenance of CDC platforms
H. support of internal fraud response
I. active relationship with external parties
1ページ

Your "**Category-Based**" portfolio in your organization **202X/YY/ZZ**

The current organization (hybridpattern) is evaluated on a 5-point scale for each category.It identifies 'strengths'(effectively) and 'weaknesses'(require improvement), making visible.Please utilize this as a macro-level indicator to help formulate strategies for improving scores.

Category	Score
A. strategic management of CDC	**3.5** /5
B. real-time analysis	**3.3** /5
C. deep analysis	**3.0** /5
D. incident response	**3.1** /5
E. checking and evaluation	**2.6** /5
F. collection, analysis and evaluation of threat intelligence	**2.8** /5
G. development and maintenance of CDC platforms	**3.0** /5
H. support of internal fraud response	**2.0** /5
I. active relationship with external parties	**2.3** /5

Strengths of your organisation, currently

A. strategic management of CDC

The overall policy for security response, as well as various rules and standards, have been established, enabling stable operations.At the practical level, the situation can be considered problem-free; however, please work toward elevating it to a more organizational effort by involving related departments and stakeholders.

Weaknesses of your organization, currently

H. support of internal fraud response

Support for internal control and insider threat response is insufficient, making it difficult to contribute to governance and compliance efforts.The current situation cannot be considered as functioning organizationally; therefore, please review the operations to ensure they can be steadily and reliably executed.

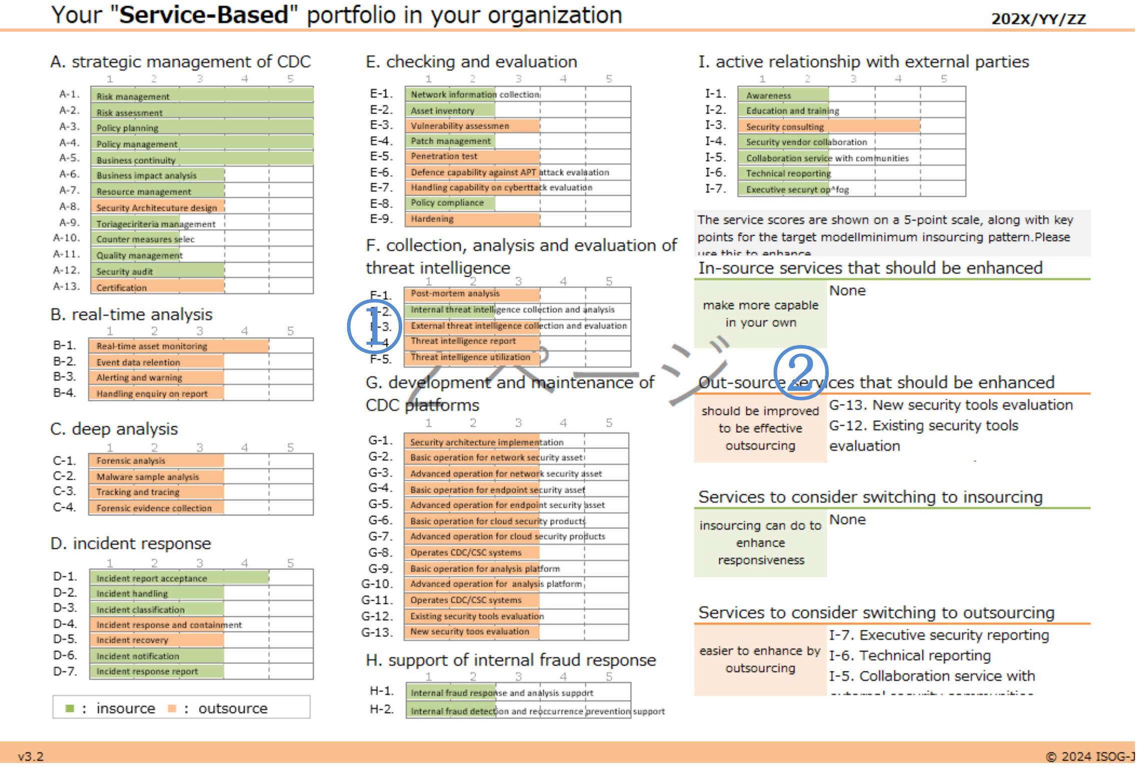
I. active relationship with external parties

Collaboration with external organizations is weak, and it has not contributed to enhancing the organization's capabilities or increasing its value.The current situation cannot be considered as functioning organizationally; therefore, please review the operations to ensure they can be steadily and reliably executed.

v3.2 © 2024 ISOG-J

1. A radar chart of scores by "category" in the current security response organisation, based on the results of the "Input Sheet."
2. A numerical summary of the content in point 1 presented in a list format.
3. Categories with high scores are identified as the "strengths" of the security response organisation.
4. Categories with low scores are identified as the "weaknesses" of the security response organisation.

The "Category-Specific Scores" make it possible to visualize the "strengths" and "weaknesses" of each category within the security response organisation, allowing a focus on categories that require prioritised review. This can be a useful tool for understanding the current state of the security response organisation from a macro perspective.



Your "**Service-Based**" portfolio in your organization

202X/YY/ZZ

A. strategic management of CDC

A-1. Risk management
A-2. Risk assessment
A-3. Policy planning
A-4. Policy management
A-5. Business continuity
A-6. Business impact analysis
A-7. Resource management
A-8. Security Architecuture design
A-9. Toriageciriteria management
A-10. Counter measures selec
A-11. Quality management
A-12. Security audit
A-13. Certification

B. real-time analysis

B-1. Real-time asset monitoring
B-2. Event data relention
B-3. Alerting and warning
B-4. Handling enquiry on report

C. deep analysis

C-1. Forensic analysis
C-2. Malware sample analysis
C-3. Tracking and tracing
C-4. Forensic evidence collection

D. incident response

D-1. Incident report acceptance
D-2. Incident handling
D-3. Incident classification
D-4. Incident response and containment
D-5. Incident recovery
D-6. Incident notification
D-7. Incident response report

🟩 : insource 🟧 : outsource

E. checking and evaluation

E-1. Network information collection
E-2. Asset inventory
E-3. Vulnerability assessmen
E-4. Patch management
E-5. Penetration test
E-6. Defence capability against APT attack evaluation
E-7. Handling capability on cyberttack evaluation
E-8. Policy compliance
E-9. Hardening

F. collection, analysis and evaluation of threat intelligence

F-1. Post-mortem analysis
F-2. Internal threat intelligence collection and analysis
F-3. External threat intelligence collection and evaluation
F-4. Threat intelligence report
F-5. Threat intelligence utilization

G. development and maintenance of CDC platforms

G-1. Security architecture implementation
G-2. Basic operation for network security asset
G-3. Advanced operation for network security asset
G-4. Basic operation for endpoint security asset
G-5. Advanced operation for endpoint security asset
G-6. Basic operation for cloud security products
G-7. Advanced operation for cloud security products
G-8. Operates CDC/CSC systems
G-9. Basic operation for analysis platform
G-10. Advanced operation for analysis platform
G-11. Operates CDC/CSC systems
G-12. Existing security tools evaluation
G-13. New security toos evaluation

H. support of internal fraud response

H-1. Internal fraud response and analysis support
H-2. Internal fraud detection and reoccurrence prevention support

I. active relationship with external parties

I-1. Awareness
I-2. Education and training
I-3. Security consulting
I-4. Security vendor collaboration
I-5. Collaboration service with communities
I-6. Technical reoporting
I-7. Executive securyt op^fog

The service scores are shown on a 5-point scale, along with key points for the target modellminimum insourcing pattern.Please use this to enhance

In-source services that should be enhanced

make more capable in your own	None

Out-source services that should be enhanced

should be improved to be effective outsourcing	G-13. New security tools evaluation G-12. Existing security tools evaluation

Services to consider switching to insourcing

insourcing can do to enhance responsiveness	None

Services to consider switching to outsourcing

easier to enhance by outsourcing	I-7. Executive security reporting I-6. Technical reporting I-5. Collaboration service with

v3.2

© 2024 ISOG-J

1. Based on the results of the "Input Sheet," create a graph to illustrate the assessment of each service within the current security response organisation.
2. Extract services requiring improvement toward realising the future model security response organisation pattern selected in the "Preparation Sheet," based on the following four perspectives:

- ➢ Services to Strengthen Through Insource Efforts
    - Services currently handled insource that need further score enhancement.
- ➢ Services to Strengthen Through Outsourcing
    - Services currently outsourced that require further score enhancement.
- ➢ Services to Consider Transitioning to Insource
    - Services currently outsourced but should prioritise reducing external dependency and transitioning to insource to achieve the future model.
- ➢ Services to Consider Transitioning to Outsourcing
    - Services currently handled insource but may benefit from outsourcing to specialized organisations to achieve higher score.

© 2025 ISOG-J

The "Service-Specific Scores" make it clear which services within the security response organisation need improvement. Including future enhancement points, this can be utilized to formulate specific improvement strategies.

© 2025 ISOG-J

9. at the end

This textbook summarises the categories, services, and assessments required for security response organisations. Creating an organisation that satisfies all these categories and services is exceedingly challenging. Realistically, such organisations are built gradually, step by step. It is hoped that this textbook will help you understand what your organisation is currently capable of, what it lacks, and what steps need to be taken next. Recognizing your organisation's "achievements and shortcomings" or its "current level of capability" is essential for enhancing its security response abilities. It is recommended that organisations use this book to gain an objective understanding of your organisation's status. Furthermore, as the security landscape will undoubtedly continue to evolve, this book will be updated this book regularly to address these changes.
The Information Security Operation providers Group Japan (ISOG-J) will continue to widely share the knowledge and expertise generated through the collaboration of security operation providers.

References

- Recommendation X.1060 "Framework for the creation and operation of a cyber defence centre" (ITU-T)
  - https://www.itu.int/rec/T-REC-X.1060-202106-I
- JT-X1060 "Framework for the creation and operation of a cyber defence centre" (Japanese) (The Telecommunication Technology Committee (TTC))
- https://www.ttc.or.jp/document_db/information/view_express_entity/1423
  - https://www.ttc.or.jp/document_db/information/view_express_entity/1423
- "Cybersecurity Management Guidelines Ver.3.0 Annex F Guidance for establishing a cybersecurity system and securing human resources Ver 2.0" (Ministry of Economy, Trade and Industry)
  - https://www.meti.go.jp/policy/netsecurity/mng_guide.html
- SOC services and skills for people v1.0 (ISOG-J) (origin of this book. Revised version is this book.)
  - http://isog-j.org/output/2016/SOC_skill_v1.0.pdf
- Ten Strategies of a World-Class Cybersecurity Operations Center (MITRE)
  - https://www.mitre.org/publications/all/ten-strategies-of-a-world-class-cybersecurity-operations-center

© 2025 ISOG-J

Appendix 1 Categories and service list

Category

The management process of security response organisation is based on nine categories below:

A. strategic management of CDC/CSC

This category manages the overall policy for security response, including the events to be handled, response scope, triage (response priority) criteria, and resource planning required. The purpose of this category is to ensure the stable operation of security response.

B. real-time analysis

This category constantly monitors and analyses logs and data from various systems, such as network devices, servers and security products. The goal is to discover threats in real time, which can lead to a rapid and appropriate incident response.

C. deep analysis

This is a category related to the incident, such as investigating the affected systems, reviewing the compromised data, and analysing the tools and methods used in the attack.

The aim is to elucidate the full scope of the incident and identify the impact.

D. incident response

This category takes specific actions based on the results of real-time analysis and threat information to deter and eliminate threats.

It aims to minimize the impact on the system and the business, including coordination and reporting with stakeholders.

E. checking and evaluation

This category is for vulnerability assessment of systems to be protected, and incident response training and its evaluation. The purpose of this category is to improve the level of security and reduce the burden of analysis and incident response, as well as to improve the level of incident prevention and incident response skills.

F. collection, analysis and evaluation of threat intelligence

This category collects threat information on vulnerabilities and attacks (external intelligence) that is available on the Internet and handles information on real-time

© 2025 ISOG-J

analysis and incident response (internal intelligence).
The objective is to improve the accuracy of real-time analysis and incident response, and to improve security assets.

G. development and maintenance of CDC/CSC platforms

This category manages, improves or develops new systems (e.g., security products, log collection databases and operational systems) that are necessary for security response. The aim is to achieve a smooth and sustainable security activities in other categories.

H. support of internal fraud response

This category collects audit data to support responses to internal fraud. While internal control itself and internal fraud investigations are generally handled by the internal control and legal departments, the objective is to provide logs and analysis to assist in the handling and resolution of such investigations.

I. active relationship with external parties

This category includes coordination and collaboration with internal stakeholders and external organisations.
The objective is to improve the security level of the organisation, increase the value of the security to the organisation, thus further developing and strengthening the organisation.

© 2025 ISOG-J

service list

Here is an explanation of each of the nine categories of services.

A. Strategic management of CDC/CSC

A-1. Risk management

The risk management service is to achieve coordinated activities including A-2 to A-13 to direct and control an organisation with regard to risk. "X.1060/JT-X1060"

A-2. Risk assessment

The risk assessment service provides a snapshot of the risk level of an organisation in terms of assets, threats and security measures. "X.1060/JT-X1060"

A-3. Policy planning

The policy planning service is supporting all the activities of defining specific security policies, compiling the guidelines. "X.1060/JT-X1060"

Policies are set by the CISO; planning is a supporting role for this service in CDC/CSC and security supervision.

A-4. Policy management

The policy management service is to achieve periodic reviews for evaluation of policy and organisation rules, to comply with new or external requirements (e.g., regulations and guidelines). "X.1060/JT-X1060"

When reviewing the service portfolio during the evaluation process, it is essential to also consider updating outdated regulations and policies. Insights from the analysis and organisation of threat information obtained through Category F: Collection, analysis and evaluation threat intelligence can be used to reassess these regulations and policies. The results of this reassessment can then be applied in the next build process, allowing for improved policies to be effectively utilized.

A-5. Business continuity

The business continuity service supports the operational functions necessary to ensure correct implementation and execution of the business continuity plan of an organisation. "X.1060/JT-X1060"

© 2025 ISOG-J

A-6. Business impact analysis

The business impact analysis service is to achieve a systematic assessment of the possible impacts resulting from various events or scenarios. This service helps organisations understand the scale of loss that could occur. It may cover not only direct financial loss, but also other impacts, such as loss of stakeholder confidence and reputational damage. "X.1060/JT-X1060"

A-7. Resource management

The resource management service plans resources (personnel, budget, systems, etc.) to support security activities and allocates them appropriately to each service. "X.1060/JT-X1060"

To effectively implement security measures, plan the allocation of necessary resources (personnel, budget, systems, etc.) and distribute them appropriately across each category. Collaborate with the HR organisation to secure security talent. Consider establishing recruitment systems to attract top talent, designing career paths to retain personnel, and revising or creating new curricula to enhance skill development. Additionally, explore interdepartmental personnel exchanges to elevate the overall security level across the organisation.

A-8. Security architecture design

The security architecture design service is to establish an architecture to secure the business. Development and maintenance of CDC platforms (category G) can be achieved by compiling various security measurements that consider system design and constraints of business processes (e.g., supply chain). "X.1060/JT-X1060"

A-9. Triage criteria management

The triage criteria management service is to set specific triage (response priority) criteria for events (e.g., incidents, vulnerabilities found, threat information discovered) under the agreed scope in the overall policy. "X.1060/JT-X1060"

Establish specific triage criteria for handling events within the response scope determined by overall policy. These criteria should focus on prioritization and must include three primary categories:

© 2025 ISOG-J

- Triage Criteria for Incident Response
  Classify incidents based on the type of attack, its progression and severity[22], and the importance of the affected asset.
- Triage Criteria for Vulnerability Discovery
  Categorize vulnerabilities based on the potential damage if exploited, ease of exploitation, and the criticality of the affected asset.
- Triage Criteria for Threat Intelligence Discovery
  Evaluate threat information collected internally or reported externally, considering factors such as the progression of the attack, potential damage, and asset importance.

In all cases, explicitly defining "non-incident criteria" will help reduce judgment discrepancies and ensure consistent decision-making.

A-10. Counter measures selection

The counter measures selection service is to support all activities of countermeasure selection for triage criteria (A-9) and of the best technologies with respect to all dispositions of security. "X.1060/JT-X1060"

For "A-9.Triage criteria management", establish specific response actions for each classification category. These actions should align with the triage criteria and must address the following three primary policies:

- Actions for Incident Response
- Actions for Vulnerability Discovery
- Actions for defining threat intelligence

The actions determined here must be established as a shared understanding with system administrators and other relevant stakeholders responsible for actual responses. It is essential to ensure that, when the triage criteria are met, these stakeholders can promptly take the necessary actions without delay.

A-11. Quality management

The quality management service is to check problems in the quality of security activities, whether or not they have a negative impact for business (e.g., usability, productivity) over a period of time (e.g., one week or one month). "X.1060/JT-X1060"

---

[22] Since there is no uniquely fixed definition of the naming of types of attacks or the level of danger, and each security product or service is different, organisation is necessary when implementing multiple products and services.

© 2025 ISOG-J

Over a set period, such as one week or one month, an inventory of various analyses and responses should be taken to confirm whether the quality of responses was satisfactory. Feedback from the recipient organisations, including inquiries and opinions, should be actively incorporated. If issues are identified, corrective measures should be implemented to ensure higher-quality responses in the future.

It is essential to evaluate not only the quality of responses at the individual service level but also the overall impact of the security response organisation on business operations. This includes assessing whether the organisation's activities negatively affect productivity or whether practical security activities are being compromised to prioritise business operations.

If multiple security response organisations exist within a company or if security response organisations are structured hierarchically, such as in a group of companies, it is crucial to consider the overall state of activities across the entire organisation.

This service includes receiving feedback through "I-3.Security consulting" where organisational decisions and areas requiring improvement are identified based on established criteria and integrated into the organisation's continuous improvement efforts.

A-12. Security audit

The security audit service systematically and measurably audits how an organisation implements security policies and controls at a specific site or time. CDC staff are indirectly involved in audit activities in order to provide necessary information and evidence of implemented state of controls. "X.1060/JT-X1060"

In relation to audits, the effectiveness of security responses should also be measured. Outputs from various categories should be collected and compiled as results, including: The number of incidents responded to, The number of attacks blocked by security devices, The outcomes of vulnerability management.

A-13. Certification

The certification service supports activities necessary for an organisation to conform to various standards and certification schemes. "X.1060/JT-X1060"

Regarding "certifications" within an organisation, the scope of certifications, the specific types to be obtained, and whether to focus solely on security-related certifications or to include other types of certifications are decisions that depend on

© 2025 ISOG-J

the organisation's policies and strategic objectives. These considerations should align with the organisation's unique needs and goals.

B. Real-time analysis

B-1. Real time asset monitoring

The real-time asset monitoring service is to supervise and analyse systems status or suspicious activities from logs and network flows, and supporting triage as incident or event for gathering information needed. "X.1060/JT-X1060"

The following types of logs are primarily monitored and analyzed in real time:

- Network-related logs: Logs from firewalls, network devices, network flows, and NDR (Network Detection and Response) solutions.
- Security device logs: Logs from IPS/IDS, WAF (Web Application Firewall), DBFW (Database Firewall), CASB (Cloud Access Security Broker), and similar security devices.
- Access logs: Logs from web servers and related applications.
- System logs: Logs from AD (Active Directory), DNS, and other critical systems.
- Endpoint-related logs: Logs from EDR (Endpoint Detection and Response), antivirus software, and asset management tools on user endpoints.
- Activity-related logs: Logs from XDR (Extended Detection and Response), UEBA (User and Entity Behaviour Analytics), and other tools monitoring complex behaviours.
- Cloud platform logs: Logs obtained from external cloud infrastructure and platforms

Given the variety of logs handled, normalization of log data and storage in a unified database or SIEM (Security Information and Event Management) system is essential for efficient analysis. Additionally, network flow information should be incorporated whenever feasible.

If basic log and network flow analysis cannot adequately determine the impact or details of an incident, further detailed analysis is conducted. This may involve: Utilizing specialized network capture devices or packet capture functions in security appliances to obtain relevant packet captures. Immediately retrieving necessary data from endpoints or servers to gather more evidence and enable precise situational assessments and impact determinations

For internal controls and audit requirements, the logs to be collected should be defined in advance and systematically gathered. These logs may be formatted into

© 2025 ISOG-J

standardized templates and shared as periodic reports to relevant organisations.
Internal controls and audits cover not only the organisation's operations but also the activities of security organisations like CDCs /CSCs(Cyber Defence Centres/Cyber Security Centres), security leadership teams, SOCs (Security Operations Centres), and CSIRTs (Computer Security Incident Response Teams). These groups' actions and processes are included in the audit scope to ensure comprehensive governance.

B-2. Event data retention

The event data retention service collects and centrally stores events gathered in the process of security monitoring and analysis.　"X.1060/JT-X1060"

There are cases where triage decisions cannot be made solely based on real-time analysis or packet capture data. In such situations, information from "E. Checking and evaluation" can be referenced, or additional data may be collected from log sources that are not typically handled.
If access to such log sources is not available within the organisation and coordination with external entities is required, this process may fall under the incident response services of Category D.

B-3. Alerting and warning

The alerting and warning service notifies the internal function involved of events that highlight potential risks to information assets (e.g., security devices alert, security bulletins, vulnerabilities and spreading threats).　"X.1060/JT-X1060"

Information revealed through real-time analysis, such as details of affected devices, attack methods, attack vectors, the presence or absence of data breaches, impact assessments, and immediate short-term countermeasures, should be compiled and documented.
Since this serves as the trigger report for incident response, it is crucial to include the minimum necessary information required for response. To ensure consistency and completeness, it is recommended to predetermine the items to be included in the report. However, it should be noted that not all details will be clarified at this stage of analysis. Any unclear points should be explicitly marked as "unknown," with plans to address them through supplementary efforts from other categories. This approach ensures thorough and structured incident handling while maintaining transparency.

© 2025 ISOG-J

B-4. Handling enquiry on report

The handling enquiry on report service is to respond to enquiries about data and reports regarding analysis. "X.1060/JT-X1060"

Inquiries regarding analysis data and provided reports should be addressed promptly. Communication can take place through various channels, including phone calls, emails, websites, chat tools, or web conferencing systems.

To ensure proper documentation of interactions, it is recommended to maintain comprehensive records. For voice-based communications, such as phone calls and web conferences, recording or utilizing transcription systems is advised. Additionally, the content of such interactions should be summarised and documented via emails or on the organisation's website for future reference and traceability.

C. Deep analysis

C-1. Forensic analysis

The forensic analysis service analyses digital evidence that is gathered from security assets and relates to an event to assist in determining what happened. "X.1060/JT-X1060"

Real-time analysis demands immediacy, and as a result, not all network logs or packet captures may be thoroughly analyzed during the initial phase. A follow-up analysis is conducted to review these elements comprehensively. Additionally, logs and packet captures that were not included in the real-time analysis are also examined to uncover behaviours observed on the network.

Where necessary, the scope of analysis extends beyond the network. This includes examining digital data stored on compromised endpoints, servers, HDDs/SSDs, memory, and external storage devices. Such analysis helps identify information targeted by attackers and determines whether data exfiltration attempts were successful, especially in cases where network-based observations alone cannot provide clear answers.

C-2. Malware sample analysis

The malware sample analysis service is to analyse malware, programs or scripts deployed by attackers that are found during each forensic process. "X.1060/JT-X1060"

In each stage of forensic analysis, if malware or programs/scripts deployed by

© 2025 ISOG-J

attackers are discovered, their functionality is analyzed. This involves a combination of techniques such as dynamic analysis, where the malware is executed to observe its behaviour, and static analysis through reverse engineering to understand its code structure and functionality without executing it.

C-3. Tracking and tracing

The service is the capability of an organisation to track and trace the source of any attacks on its infrastructures, which is a critical success factor to reduce further occurrences and prevent security incidents. An acknowledged ability to track and trace both internal and external attackers (e.g., cyber attribution) can pre-empt future attacks. "X.1060/JT-X1060"

Based on the results of forensic analysis and sample examination, the complete picture of the attack activities is uncovered. If analysis materials are insufficient, publicly available threat intelligence or information gathered through "F-3.External threat intelligence collection and evaluation" can be utilized to supplement the data. Hypotheses can be incorporated to reinforce the available information. When sufficient evidence is collected, efforts may also be made to profile the attacker, including assumptions about their affiliated organisation and the organisation's objectives.

C-4. Forensic evidence collection

The forensic evidence collection service collects and conserves digital electronic evidence related to an assessed incident, and develops and maintains validity of evidence ("evidence chain of custody"). "X.1060/JT-X1060"

When there is a possibility of conducting cybercrime investigations or taking legal action, digital evidence preservation must be carried out at each stage of the analysis process.

D. Incident response

D-1. Incident report acceptance

The incident report acceptance service is to receive analytical reports of operations. However, it may receive reports from another organisation within the company or from an outside organisation. "X.1060/JT-X1060"

Primarily, analysis reports from operations are received. However, there is also the

© 2025 ISOG-J

potential for reports from other internal departments or notifications from external organisations.

For internal submissions, establish multiple communication channels such as email, chat tools, and web conferencing systems, and ensure these options are well-publicized. For external reports, a dedicated email address should be set up and widely shared both internally and externally. If resources are limited, leveraging "B-4. Handling enquiry on report" can be a viable option.

Additionally, external incident reports may use contact information registered in the WHOIS database. Therefore, it is crucial to regularly update registration details and ensure that communications reach the appropriate security response team. If another department manages these communications, a process for sharing the contents with the security response organisation should be established.

D-2. Incident handling

The incident handling service is to deal with accepted incidents and coordinates activities including D-3 to D-7. "X.1060/JT-X1060"

For incidents determined to require action through triage, manage the response progress and ensure alignment with the policies established under "A-9. Triage criteria management". This includes monitoring whether responses are being conducted in accordance with the set guidelines and tracking the status of incident analysis. This management continues until the incident response is fully completed.

D-3. Incident classification

The incident classification service is to classify an incident to contribute to a common understanding of the types of incident that occur and what causes them. "X.1060/JT-X1060"

Incident information received should be assessed for actionability and priority based on the "A-9. Triage criteria management" guidelines. If there is insufficient data to make a decision, coordinate with "B-2. Event data retention". If decisions are made that fall outside the scope of the triage criteria, provide feedback to "A-9. Triage criteria management".

After making the determination, identify the incident's overall impact, including direct business implications (such as losses from service downtime and costs associated with recovery and mitigation) and indirect effects (such as reputational damage and

© 2025 ISOG-J

decreased operational efficiency). Develop provisional countermeasures and long-term preventive strategies.

If the analysis is inadequate due to missing information, closely coordinate with “C. Deep analysis” to ensure comprehensive evaluation and resolution.

D-4. Incident response and containment

The incident response and containment service is to contain an incident before it spreads through all resources and increases the damage to or impact on them. “X.1060/JT-X1060”

For actual incident response, low-priority incidents can be addressed via phone, email, chat tools, or web conferencing systems. If strict evidence preservation is not required, remote access (such as remote desktop or SSH) can be used to resolve the issue. The results of the response must be shared with “B. Real-time analysis” to prevent unnecessary analysis or escalation of the incident.

If remote response is insufficient to resolve the issue or if strict evidence preservation is required, specialists should physically visit the site housing the affected system to conduct the necessary interventions. The results of such responses must also be shared with “B. Real-time analysis” to ensure that unnecessary analysis or escalation of the incident does not occur.

D-5. Incident recovery

The incident recovery service is to support the restoration of the functionality of a target to its normal system operability. “X.1060/JT-X1060”

D-6. Incident notification

The incident notification service is to communicate the occurrence of an incident to incident response teams and other concerned groups. “X.1060/JT-X1060”

Coordinate and collaborate with internal stakeholders. Internal stakeholders include executives, relevant internal departments (such as IT and legal), and external partner organisations (such as development vendors and service providers). These stakeholders are primarily "those who should be involved in jointly investigating the full scope of the incident." Tasks include reporting on the incident, sharing information, and coordinating the sharing of data necessary for analysis.

Coordinate and collaborate with external stakeholders. External stakeholders include

© 2025 ISOG-J

regulatory authorities, external business partners, and end users, primarily defined as "those impacted by the incident." Tasks include providing explanations regarding the incident, verifying the extent of the damage, and collecting specific details about the impact.

D-7. Incident response report

The incident response report service is to achieve the completion and distribution of the report of a closed incident response (if countermeasure efforts are protracted, it will be handed over to the strategic management of CDC (category A)). If CDC staff need a report of current status during handling of an incident, this service distributes an interim report. "X.1060/JT-X1060"

Summarise and document the impact, root causes, implemented responses, and fundamental countermeasure policies identified during the incident response. If the mitigation efforts become prolonged, hand over the management to "A-1. Risk management".
Prepare separate reports for internal[23] and external stakeholders, as the level of detail will differ for each audience. The completion and distribution of these reports mark the closure of the incident response. Once the reporting is finalized, if there is a need to revise or improve organisational procedures or tools, address this through "F-1. Post-mortem analysis".

E. Checking and evaluation

E-1. Network information collection

The network information collection service is to receive an overview of the network configuration that is to be protected. "X.1060/JT-X1060"

Gain an overview of the network configuration of the assets to be protected. This does not mean understanding every detail perfectly but being able to quickly identify the relationships and types of various network and security devices, such as whether security devices are deployed inline or not. To achieve this, collaboration with other departments, such as the IT or systems department, is essential. This information is

---

[23] One often overlooked aspect is providing feedback to the real-time analysis team. If they are not informed about whether their analysis was accurate, what actions were taken, and whether those actions successfully resolved the issue, it becomes challenging to improve the accuracy of subsequent real-time analysis results.

© 2025 ISOG-J

crucial not only for vulnerability management but also as a reference for analysis and incident response.

E-2. Asset inventory

The asset inventory service is to achieve information management relevant to the census of systems, assets and applications that constitute the overall business infrastructure within the scope of CDC support.　"X.1060/JT-X1060"

Collect information about the assets to be protected, such as servers, endpoints, and network devices. While using asset management data from frameworks like ISMS as a foundation, it is desirable to gather more detailed information, such as firmware versions and the versions of installed applications. When procuring physical assets or software, it may also be necessary to check and manage which external libraries or modules are used internally. Similarly, for the business operations, services, or products managed by your organisation, it is essential to track the external libraries or modules used as components of your products or services.

However, collecting this information is highly challenging. Collaboration with ISMS-related departments is crucial to establish rules that mandate registering such information in internal processes. Leveraging information collected during vulnerability assessments, as discussed later, can also be an effective strategy. This collected data serves not only for vulnerability management but also as a critical reference for analysis and incident response.

E-3. Vulnerability assessment

The vulnerability assessment service is to examine networks, systems and applications to identify vulnerabilities, determines how they can be exploited and recommends how the risks can be mitigated.　"X.1060/JT-X1060"

Use tools to check for vulnerabilities in the systems, networks, and applications that need protection. Select the type of diagnostic that matches the purpose, such as platform diagnostics, web application diagnostics, web API diagnostics, or smartphone application diagnostics. While tool-based diagnostics may have precision limitations, they are cost-effective and can be performed within a short timeframe, making it feasible to conduct regular diagnostics on a larger number of systems.

© 2025 ISOG-J

E-4. Patch management

The patch management service is to support the installation of any security patches required, while the availability of information technology (IT) service is maintained. "X.1060/JT-X1060"

Cross-reference vulnerability information with the previously mentioned network mapping and asset information to identify systems requiring action. Notify the responsible system management entities and monitor the progress of the mitigation efforts. New threat information is obtained from "F-3. External threat intelligence collection and evaluation", while vulnerability information for key software and products should be gathered regularly from the respective providers' websites and other official sources.

E-5. Penetration test

The penetration test service is to reveal security vulnerabilities that could be exploited by attackers and highlights possible methods of compromise (e.g., threat-led penetration test). "X.1060/JT-X1060"

This process is carried out "manually" by specialized personnel rather than "automated" tools. While it requires more time and cost compared to tools, it delivers more accurate results. It is essential to perform such assessments for high-priority systems. Additionally, diagnostics should be conducted at critical milestones, such as the launch of new systems or major system overhauls.

In a Threat-Led Penetration Test[24] (TLPT), red teams (attackers) and blue teams (defenders) conduct the tests. In such cases, this service is coordinated with other services, including "E-6. Defence capability against ATP attack evaluation" and "E-7. Handling capability on cyberattack evaluation".

E-6. Defence capability against ATP attack evaluation

The defence capability against advanced persistent threat (ATP) attack evaluation service is to measure the resistance of an organisation to targeted attacks while conducting targeted email training and social engineering tests. "X.1060/JT-X1060"

---

[24] "about Penetration Test", skill map project for vulnerability assessment specialist. https://github.com/ueno1000/about_PenetrationTest

© 2025 ISOG-J

To measure the organisation's resilience against targeted attacks, exercises such as targeted email training and social engineering tests are conducted. The results of these activities can be used to enhance employee education and provide a basis for advocating the necessity of security measures to the company.

In the case of penetration tests or Threat-Led Penetration Tests (TLPT), coordination with "E-5. Penetration test" is required.

E-7. Handling capability on cyberattack evaluation

The handling capability on cyber-attack evaluation service is to confirm whether actual security response activities based on a scenario that assumes an attack has occurred can be activated and whether the incident can be brought to an end without delay (called a cyber-attack response exercise). "X.1060/JT-X1060"

Based on a scenario assuming an attack has occurred, real-world security response activities are initiated to confirm whether the incident can be smoothly resolved to completion (commonly referred to as a cyberattack response exercise). If issues arise, the causes are analyzed and used to enhance response capabilities.

In addition to tabletop exercises, if the defensive Blue Team is involved in penetration testing or Threat-Led Penetration Tests (TLPT), coordination with "E-5. Penetration test" is necessary. The results from these exercises are utilized to evaluate the organisation's response capabilities.

E-8. Policy compliance

The policy compliance service is to support the verification of conformity to and compliance with predefined security policies. "X.1060/JT-X1060"

E-9. Hardening

The hardening service is to optimize IT component configuration to identify, evaluate and apply systems security configurations, and to mitigate or eliminate the risk of attacks. "X.1060/JT-X1060"

F. Collection, analysis and evaluation threat intelligence

F-1. Post-mortem analysis

The post-mortem analysis service describes resolution of an incident to ensure review and improvement of the processes and tools for CDC staff. "X.1060/JT-X1060"

© 2025 ISOG-J

When incident response is completed under “D-7. Incident response report”, the security response organisation undertakes improvements to overall procedures and tools. For areas requiring organisational-level improvements, actions are carried out under Category “A. Strategic management of CDC/CSC”.

F-2. Internal threat intelligence collection and analysis

The internal threat intelligence collection and analysis service is to gather information (internal intelligence) on real-time analysis and incident response. “X.1060/JT-X1060”

Collect information related to real-time analysis and incident response (internal intelligence). Analyze the root causes of incidents that need to be managed and understood within the organisation, including the supply chain, considering not only system perspectives but also internal rules and processes. Organize the findings to develop mid- to long-term countermeasures. Additionally, identify and document challenges in real-time analysis and incident response processes themselves to drive improvements across the entire security response framework.

F-3. External threat intelligence collection and evaluation

The external threat intelligence collection and evaluation service is to gather information (external intelligence), such as new vulnerabilities, attack trends, malware behaviour and malignant Internet protocol addresses or domain information. “X.1060/JT-X1060”

Collect newly published vulnerability information, attack trends, malware behaviour details, and information on malicious IP addresses and domains (external intelligence). Evaluate the credibility of the obtained information, its potential impact on the organisation, and prioritise vulnerabilities for action. Threat intelligence is utilized through “F-5. Threat intelligence utilization” , and if necessary, external threat information can also be employed for analysis under “C-3. Tracking and tracing”.
Regularly review information sources to ensure the collection of the most up-to-date intelligence. Additionally, if issues that should have been discovered through analysis emerge or if certain countermeasures prove challenging at the time, revise operational practices as needed.

F-4. Threat intelligence report

The threat intelligence report service is to compile internal and external threat

© 2025 ISOG-J

information and document it, including all details.　“X.1060/JT-X1060”

Consolidate collected internal and external threat intelligence into a comprehensive document, including detailed information. It is desirable to generate this report regularly, such as monthly or quarterly, to provide consistent observation points. However, the rapidly changing nature of the security landscape requires frequent content reviews to prevent the report from becoming obsolete or ineffective. It is essential not to fear making adjustments to the format or content as needed.
For threat intelligence with potentially significant impacts, prepare and issue alerts or special reports promptly to address urgent needs.

F-5. Threat intelligence utilization

The threat intelligence utilization service is to achieve compilation and dissemination of threat information for all categories of security response.　“X.1060/JT-X1060”

Consolidated threat intelligence must be disseminated across all security response categories. While each category may focus on different aspects of the information, ensuring no gaps in understanding fosters seamless collaboration between categories. To facilitate this, it is crucial to establish processes and rules within security response policy management that encourage both actionable guidance to each category and feedback from them.
When designing these processes, particular attention should be paid to integrating insights into “G. development and maintenance of CDC/CSC platforms” to enhance the platform's capabilities effectively. For information related to vulnerabilities and patches, proper utilization is expected within “E-4. Patch management” to ensure timely and effective handling of security risks.

G. Development and maintenance of CDC platforms

G-1. Security architecture implementation

The security architecture implementation service is to implement the security architecture designed by strategic management of CDC (category A) by using assets.
“X.1060/JT-X1060”

G-2. Basic operation for network security asset

The basic operation for network security asset service is to operate network devices, such as firewalls, intrusion detection system/intrusion prevention system (IDS/IPS),

© 2025 ISOG-J

web application firewall (WAF) and proxies.　"X.1060/JT-X1060"

Manage the operation of network devices such as firewalls, IDS/IPS, WAF, proxies, and NDR. This includes understanding the network architecture and managing the details of network security products, such as types, placement, installation configurations (e.g., inline or tap), hardware/firmware versions, and configuration settings.

Ensure that all devices are functioning properly through health monitoring and regular updates to detection signatures. Given that configuration or settings changes can significantly impact the network, it is essential to establish clear procedures and processes for these operations. This ensures the stability and security of the network while minimizing risks associated with changes.

G-3. Advanced operation for network security asset

The advanced operation for network security asset service is to create custom signatures of an organisation for products with attack detection capabilities, such as IDS/IPS and WAF, and applies them if the signature provided by the vendor is insufficient.　"X.1060/JT-X1060"

For products with attack detection capabilities, such as IDS/IPS and WAF, create and apply custom signatures when the detection signatures provided by the product vendor are insufficient.

Additionally, to mitigate the risks of excessive or false detections that can lead to log flooding or erroneous blocking, establish and implement a master signature policy. This policy should be based on a thorough understanding of the characteristics of each signature to ensure effective detection while minimizing unnecessary disruptions.

G-4. Basic operation for endpoint security asset

The basic operation for endpoint security asset service is to operate countermeasure products, such as anti-virus software, at endpoints.　"X.1060/JT-X1060"

Manage endpoint protection products such as antivirus software and EDR (Endpoint Detection and Response). In recent years, these solutions often include features to detect or log malware behaviour and attacks exploiting vulnerabilities at the endpoint level. Ensure comprehensive oversight by monitoring for installation gaps, verifying timely pattern updates, and confirming the activation of scanning functionalities.

© 2025 ISOG-J

For endpoint management, asset management or dedicated asset tracking software may also be utilized. Maintain detailed operational oversight of which endpoint protection products are deployed, what software is installed on endpoints, and ensure consistent and thorough management of these assets.

G-5. Advanced operation for endpoint security asset

The advanced operation for endpoint security asset service is to detect suspicious program activity within the endpoint using its protection product, and collects and analyses registry status, process execution, etc. If needed, the service establishes customised indicators of compromise to enable endpoint detection. "X.1060/JT-X1060"

In endpoint protection products, detect suspicious program activities within the endpoint by collecting and analyzing data such as registry states and process execution statuses. If necessary, independently define custom Indicators of Compromise (IOCs) and configure the endpoint protection system to detect threats based on these custom IOCs.

G-6. Basic operation for cloud security products

The basic operation for cloud security products service is to operate security services in a cloud. "X.1060/JT-X1060"

G-7. Advanced operation for cloud security products

The advanced operation for cloud security products service is to create custom signatures of an organisation for security services in a cloud with attack detection capabilities. If the signature provided by a vendor is insufficient, the service applies custom signatures. "X.1060/JT-X1060"

When utilizing cloud services, information leaks may occur due to configuration errors on the user side. To address this, leverage services that identify misconfigurations in the cloud and services that help modify settings when such issues are detected.

G-8. Deep analysis tool operation

The deep analysis tool operation service is to operate tools used in deep analysis, such as digital forensics and malware analysis. "X.1060/JT-X1060"

Operate tools used for digital forensics and malware analysis. In-depth analysis often

© 2025 ISOG-J

involves handling data that contains sensitive or personal information, as well as highly dangerous programs like malware. Therefore, strict management is required, including proper usage of tools, detailed procedures, and well-defined approval processes for carrying out tasks.

G-9. Basic operation for analysis platform

The basic operation for analysis platform service is to operate analytical infrastructure that stores the log data required and enables the analysis to be performed routinely, mainly in real-time analysis, such as security information and event management (SIEM). "X.1060/JT-X1060"

An analysis platform primarily refers to a system that stores log data required for real-time analysis and enables regular analysis activities. This includes tools like SIEM (Security Information and Event Management). The platform involves determining what types of data to retain and for how long, updating or adding analysis rules, and monitoring to ensure data is being stored and analysis processes are continuously operational.

G-10. Advanced operation for analysis platform

The advanced operation for analysis platform service is to achieve more detailed and accurate analysis using the organisation's own systems to retain system logs and packet capture data that commercial SIEMs cannot capture, and develops customized analysis algorithms and logic for these data, as well as the system. "X.1060/JT-X1060"

Logs and packet capture data from systems that commercial SIEM solutions cannot ingest are stored using a custom system. Additionally, analysis algorithms and logic tailored for these data, as well as the systems that run them, are independently developed. This approach enables more detailed and accurate analysis.

G-11. Operates CDC/CSC systems

The operates CDC/CSC systems service is to operate systems that perform the tasks required for security response operations, such as the various security response tools previously described, the production of various reports, the response to enquiries, and the vulnerability management system. "X.1060/JT-X1060"

The CDC/CSC system encompasses the various tools and systems necessary for

© 2025 ISOG-J

security operations, such as security response tool management, report generation, inquiry handling, and vulnerability management systems. It is designed based on the required workflows, processes, and procedures to fill gaps in functionality in other systems, prevent operational errors, enhance efficiency, and enable automation of tasks.

G-12. Existing security tools evaluation

The existing security tools evaluation service is to verify the impact on other systems and operations, mainly in terms of availability, when upgrading or changing the settings of existing security-enabled tools. "X.1060/JT-X1060"

When performing version upgrades or configuration changes to existing security response tools, the impact on other systems and operations, particularly regarding availability, must be thoroughly evaluated.

G-13. New security tools evaluation

The new security tools evaluation service is to design and install new security assets, if new measures are needed in security activities. "X.1060/JT-X1060"

When new measures are required as part of a series of security responses, the introduction of new tools to address those needs should be considered. This involves researching commercial products, conducting trial usage to assess whether the expected effects can be achieved, and evaluating the impact on current operations. If no commercial product meets the requirements, custom development should be undertaken.

New security measures in security response may involve the following three scenarios:

- Solutions or products for analyzing attacks used within the security response organisation: Tools dedicated to internal analysis and investigation.
- Business solutions or products used outside the security response organisation: Tools implemented for broader organisational purposes.
- Attack countermeasure solutions or products provided as services by the security response organisation: Products or services offered to clients or external organisations.

Solutions or products for use within the security response organisation to analyze

© 2025 ISOG-J

attacks require evaluation based on whether their specifications and architecture meet established standards.

Business solutions or products used outside the security response organisation must not only meet these standards but also ensure a robust support system for addressing discovered vulnerabilities.

For attack countermeasure solutions or products offered as services by the security response organisation, it is essential to evaluate their ability to handle current and emerging attack trends. Additionally, there must be a system in place to receive adequate support if vulnerabilities are discovered.

These considerations necessitate a comprehensive risk assessment of services or products intended for use within the organisation's security architecture. This includes analyzing potential risks, determining whether the solution can be effectively implemented, and evaluating whether it requires approval or decision-making at higher levels of the organisation.

H. Support of internal fraud response

H-1. Internal fraud response and analysis support

The internal fraud response and analysis support service is to support the organisation responding to internal fraud when it is discovered, by organizing its activities from the logs collected by the security activities. "X.1060/JT-X1060"

In cases where internal fraud is discovered, the security response organisation assists by organizing and analyzing activity details based on the logs it collects. The scope of internal fraud includes the entire organisation, encompassing the security response organisation such as CDC/CSC, security management, SOC, and CSIRT as potential subjects of investigation.

H-2. Internal fraud detection and reoccurrence prevention support

The internal fraud detection and reoccurrence prevention support service is to analyse the details of internal fraudulent activities that have been discovered, and considers whether it is possible to detect them from the logs, and if so, implements the detection logic. "X.1060/JT-X1060"

Analyze the activities associated with discovered internal fraud and explore whether they can be detected through logs. If detection is feasible, implement detection logic accordingly. Utilize tools like UEBA (User and Entity Behavior Analytics) to

© 2025 ISOG-J

incorporate detection logic capable of identifying suspicious user behavior. When fraud is detected, notify the organisation responsible for addressing internal fraud, contributing to its prevention. The scope of internal fraud includes the entire organisation, encompassing the security response organisation such as CDC/CSC, security management, SOC, and CSIRT as subjects of potential scrutiny.

I. Active relationship with external parties

I-1. Awareness

The awareness service is to precisely create awareness for the relevant staff across and in relation to the CDC, promotes the utilization of the correct tools, best practice, policies and resources to ensure protection of the business assets. "X.1060/JT-X1060"

Compile real-world security response cases and statistical data, collaborating with relevant departments to raise awareness among employees by presenting these issues as relatable concerns. Conduct awareness activities through initiatives such as creating a dedicated portal site, producing videos, distributing posters, or developing educational materials.

I-2. Education and training

The education and training service is to support specialized training activities in the areas of security for staff in the organisations that the CDC supports. "X.1060/JT-X1060"

Conduct internal training sessions and workshops on security-related topics to share the specialized knowledge gained through security response efforts. These initiatives aim to enhance the understanding and awareness of security concepts in departments outside the security response organisation.

I-3. Security consulting

The security consulting service provides consultancy services to the various business functions with regards to security. "X.1060/JT-X1060"

Receive security-related inquiries from departments responsible for internal system development or customer-facing service operations. Provide advice based on the policies and decision-making criteria outlined in category "A. Strategic management of CDC/CSC". If any recommendations or items requiring improvement exceed existing

© 2025 ISOG-J

standards, collaborate with “A-11. Quality management”. to implement enhancements or necessary actions. Through this activity, contribute to the promotion and integration of Security By Design principles.

I-4. Security vendor collaboration

The security vendor collaboration service is to build a direct line of communication with the provider of a security product or service purchased, requests a response to any deficiencies found in the security response and exchanges positive feedback on areas for improvement X.1060/JT-X1060”

Establish a direct communication channel with the providers of purchased security products or services. Build a collaborative relationship to address any issues identified during security operations by requesting fixes or improvements. Engage in constructive discussions to share feedback and suggest enhancements to improve the products or services.

I-5. Collaboration service with external security communities

The collaboration service with external security communities is to exchange information proactively by participating in external communities. Such information can reflect on the security activities. “X.1060/JT-X1060”

Participate in gatherings of organisations involved in security operations (such as NCA(Nippon CSIRT Association) or various ISACs). Actively engage in information exchange within the scope of permissible disclosures to expand the network of information sharing and utilization.

I-6. Technical reporting

The technical reporting service is to provide reports of the results of monitoring and management activities. These activities help to show the security level of systems and IT infrastructure. “X.1060/JT-X1060”

I-7. Executive security reporting

The executive security reporting service is to produce periodic reports and statistical analysis to top management to highlight the security level and indicators of operational performance of an organisation. “X.1060/JT-X1060”

© 2025 ISOG-J

Appendix 2 handbook for self-assessment

The handbook for self-assessment and the list of services have been added to this document.
The handbook was created in response to the need for easy reference to the list of services when using the self-assessment sheet, as it is difficult to review the entire document.
The handbook is 16 pages in length, so please print it as a booklet by printing on both sides of the paper, etc., and use it as needed.

© 2025 ISOG-J

Appendix 3 mapping to FIRST CSIRT Services Framework ver.2.1.0

We have examined the mapping of how each service in this document or X.1060 corresponds to the CSIRT Services Framework Ver. 2.1.0, which is provided by FIRST and is related to CSIRT operations.

Please refer to “Mapping to FIRST CSRT Services Framework” as an annex to this document as well as to each other when reviewing CSIRT services.

Since the concept of CDC/CSC in this document or X.1060 encompasses the entire picture of security activities, the mapping results confirmed that all services in the FIRST CSIRT Services Framework are covered. Mapping on the other side also confirmed that the FIRST CSIRT Services Framework is more granular than the CDC/CSC in defining the services to be performed by CSIRTs, but it does not cover all the services in the CDC/CSC.

This means that the services of the FIRST CSIRT Services Framework can be linked to the services of the FIRST CSIRT Services Framework and used as a reference when first defining the overall image of security response in this document or in X.1060, and then considering the business area called CSIRT in a more granular manner. The FIRST CSIRT Services Framework services can be used as a reference.

© 2025 ISOG-J

Authors

Information Security Operations providers Group Japan（ISOG-J）

Security Operations Chaos WG (SOC-WG, WG6)

Shigenori TAKEI	SCSK Security Corp. / leader of ISOG-J WG6
Kanon YOSHIDA	NEC Solution Innovators, Ltd.
Kimitomo KAWASHIMA	NTT DATA INTELLILINK Corp.
Takahiro HIKOSAKA	NTT TechnoCross Corp.
Yasuhiro NOJIRI	NTT Docomo Business Corp.
Shinji ABE	GMO Cybersecurity by Ierae, Inc. / leader of ISOG-J WG4
Atsushi HAYAKAWA	GMO Cybersecurity by Ierae, Inc. / leader of ISOG-J operational support
Hirohumi INOUE	Deloitte Thomatsu Cyber LLC.
Motoshi KAKUDA	Net One Systems Co., Ltd.
Sho AOKI	Hitachi, Ltd.

Supporters

Makoto TAMAKI	SCSK Security Corp.
Takanori KAWADA	NTT Security (Japan) KK.
Kosuke MOTOHASHI	NTT Security (Japan) KK.
Toshiya FUJIWARA	NTT DATA INTELILINK Corp.
Hideto GOTO	NTT DATA INTELILINK Corp.
Yuta NAKAMURA	NTT TechnoCross Corp.
Yoshiya MAKI	NTT Docomo Business Corp.
Keita GOTO	Orix Computer Systems Corp.
Akifumi ISHIKAWA	Cisco Systems G.K.
Itaru URIKURA	Cisco Systems G.K.
Takumi ISHIBASHI	Cisco Systems G.K.
Yohei INAGAKI	The Japan Research Institute, Limited
Kazuaki TAKENOUCHI	PERSOL CROSS TECHNOLOGY Co., LTD.
Fumiyasu UNO	Hitachi Systems, Ltd.
Kei INOUE	LAC Co., Ltd.

（Writing parties, in alphabetical order of company name）

© 2025 ISOG-J