

**Fact-finding Report
on the Establishment and Operation of CSIRTs in Japan 2015**

JPCERT Coordination Center

May 12, 2017

- 1. Introduction3
 - 1.1. Purpose of Study3
 - 1.2. Expected Readers4
 - 1.3. Overview of Study Method.....4
- 2. Questionnaire Results 17
 - 2.1. Structure at the time of establishment 17
 - 2.2. Structure of CSIRT.....22
 - 2.3. CSIRT members50
 - 2.4. Processes and rules58
 - 2.5. Tools69
 - 2.6. Revision of system and rules.....70
 - 2.7. Reports.....72
- 3. Results of Interviews with NCA Member CSIRTs73
 - 3.1. Interview with ASY-CSIRT73
 - 3.2. Interview with DeNA CERT77
 - 3.3. Interview with FJC-CERT.....81
 - 3.4. Interview with Fuji Xerox CERT85
 - 3.5. Interview with I-SIRT89
 - 3.6. Interview with MB-SIRT93
 - 3.7. Interview with NTT-CERT97
 - 3.8. Interview with T-SIRT101
 - 3.9. Interview with YMC-CSIRT105
- 4. Matters that Should be Defined at the time of Establishment..... 109
 - 4.1. Scope of services provided by CSIRTs 109
 - 4.2. Authority granted to CSIRTs 110
 - 4.3. Deployment and members of CSIRTs 111
 - 4.4. Point(s) of contact (PoC)..... 111
 - 4.5. Reporting structure of CSIRT activities to effectively be acknowledged by the company 112
 - 4.6. Periodic review of CSIRT activities..... 113
- 5. In Conclusion 118

1. INTRODUCTION

1.1. PURPOSE OF STUDY

Cyber attacks in recent years have become increasingly diverse in terms of their aims, targets, and methods used. While some attackers target specific organizations or industries, others target individuals to steal information or extort money. Some cyber attacks are carried out to make a political statement or simply to show off one's technical prowess. Occasionally, the impact can be large enough to shake the foundation of a business. As such, organizations are faced with the need to prepare for cyber attacks. One approach that is drawing attention is to establish a Computer Security Incident Response Team (CSIRT) that will serve as the linchpin of an organization to effectively handle security incidents. The Cybersecurity Management Guidelines*¹ published by the Ministry of Economy, Trade and Industry also refer to the need to establish CSIRTs. Under these circumstances, the number of organizations setting up their own CSIRTs is expected to increase.

CSIRTs can be established and operated in various forms, depending on the culture of the organization and the technical backgrounds of the team members. Many internal CSIRTs are members of the Nippon CSIRT Association (NCA) or other similar organizations and interact with other CSIRTs. This provides them with opportunities to compare their structures and activities with those of other CSIRTs. This association serve as a forum where CSIRTs can discuss various matters including structures and activities in search of good practices. The purpose of this study is to respond to such needs by looking at the activities of internal CSIRTs at many different organizations in Japan and documenting our findings. These efforts are intended to provide a valuable guide for organizations that are considering setting up a CSIRT, as well as for those that already operate a CSIRT and are exploring ways to take their endeavors to the next level.

This study was conducted by means of a questionnaire survey and interviews targeting NCA members. The questionnaire survey included items such as the organizational structure, composition of members, policies, and other matters that should be defined when establishing a CSIRT. The interviews were conducted with CSIRTs that are notable for their distinctive activities in each industry, and examined the status of efforts at each organization and issues they face. Interview results provide hints for improving the operation of CSIRTs in general. We hope that the information contained in this document will serve as a useful reference for those interested in establishing a CSIRT or improving its activities.

We thank all those at the CSIRTs that kindly offered their cooperation by answering the questionnaire and giving interviews for this study.

*¹ Cybersecurity Management Guidelines:<http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf>

1.2. EXPECTED READERS

We expect this study report to be read by people responsible for or charged with any of the following tasks.

- Studying the possibility of establishing a CSIRT
- Establishing a CSIRT
- Operating a CSIRT

1.3. OVERVIEW OF STUDY METHOD

1.3.1. QUESTIONNAIRE SURVEY

The following is an overview of the questionnaire survey conducted for this study. See Table 1.3.1 for the survey items.

Date	December 8, 2015
Survey Subjects	Organizations that participated in the 11th CSIRT Working Group Meeting hosted by the Nippon CSIRT Association (NCA)
Implementation Guidelines	Organizations participating in the above meeting were first given an explanation about the purpose of the study, which is to analyze and publish the questionnaire results to help raise awareness about CSIRTs and promote the activities of the CSIRT community. Then questionnaire forms were distributed to be filled out and returned at the end of the meeting. The names of respondents' were given voluntarily.
Overview of the Questionnaire Form	The questionnaire was titled "Questionnaire on the Establishment and Operation of CSIRTs" and asked about the scope of services provided and the operation status at each organization, among other matters.
No. of Respondents	66 organizations

[Table 1.3.1] Questionnaire Items

Questionnaire Items	
1. Structure at the time of establishment	
1.1	Department(s) that led the establishment
	<ul style="list-style-type: none"> (a) Information System Management Department (b) Corporate Planning Department (c) Legal Department (d) Audit Department (e) Development Department (f) General Affairs Department (g) Risk Control Department (h) Security Department (i) Quality Assurance Department (j) Other (describe) [_____]
1.2	Department(s) involved in the establishment (Mutiple answers allowed)
	<ul style="list-style-type: none"> (a) Information System Management Department (b) Corporate Planning Department (c) Legal Department (d) Audit Department (e) Development Department (f) General Affairs Department (g) Risk Control Department (h) Security Department (i) Quality Assurance Department (j) Other (describe) [_____]
1.3	Department(s) that needed coordination at the time of establishment (Mutiple answers allowed)
	<ul style="list-style-type: none"> (a) Information System Management Department (b) Corporate Planning Department (c) Legal Department (d) Audit Department (e) Development Department (f) General Affairs Department (g) Risk Control Department (h) Security Department (i) Quality Assurance Department (j) Other (describe) [_____]
1.4	Number of personnel involved in the establishment (including outsourced staff members)

	<ul style="list-style-type: none"> (a) Less than 5 (b) 5-9 (c) 10-19 (d) 20 or more
	1.5 Start of the establishment process
	MM DD, YYYY
	1.6 Completion of the establishment process (establishment date)
	MM DD, YYYY
2. Structure of CSIRT	
	2.1 Which department(s) of the organization does it belong to? (Multiple answers allowed)
	<ul style="list-style-type: none"> (a) Information System Management Department (b) Corporate Planning Department (c) Legal Department (d) Audit Department (e) Development Department (f) General Affairs Department (g) Risk Control Department (h) Security Department (i) Quality Assurance Department (j) Other (describe) [_____]
	2.2 Positioning of the CSIRT in the event of an incident (Multiple answers allowed)
	<ul style="list-style-type: none"> (a) Implement or support countermeasures on-site (b) Technical advisor (c) Coordinator (d) Other (describe) [_____]
	2.3 Recipient(s) of the CSIRT's services (Multiple answers allowed)
	<ul style="list-style-type: none"> (a) Users within the organization (b) Users at a group company (c) Customers using the company's services (d) Other (describe) [_____]
	2.4 Has the CSIRT ever received contact or queries from outside in the past? (Multiple answers allowed)
	<ul style="list-style-type: none"> (a) Regarding vulnerabilities of web services (b) Regarding vulnerabilities of products (c) Regarding incidents (d) Other (describe) [_____] (e) No query received

<p>2.4.1 Who did the CSIRT receive contact or queries from?</p> <ul style="list-style-type: none"> (a) Security vendors (b) IPA (c) General users (d) JPCERT/CC (e) Other (describe) [_____]
<p>2.5 Is the CSIRT part of any framework(s) for sharing information about cyber attacks? (Multiple answers allowed)</p> <ul style="list-style-type: none"> (a) IPA (J-CSIP) (b) Financials ISAC Japan (working groups) (c) National Police Agency (CCI) (d) JPCERT (WAISE) (e) Other (describe) [_____]
<p>2.6 What is the primary method(s) of expression used to share information? (Multiple answers allowed)</p> <ul style="list-style-type: none"> (a) Text (b) Open IOC (c) STIX/TAXII (d) Other (describe) [_____]
<p>2.7 Areas covered (Multiple answers allowed)</p> <p>[Incident response for an organization to which the CSIRT belongs]</p> <ul style="list-style-type: none"> (a) Corporate infrastructure: Respond to incidents that occur on internal networks used by employees (b) Customer service systems (network connection services, web applications, services, etc.): Respond to incidents that occur in services provided to outside users <p>[Incident response for an organization to which the CSIRT does not belong]</p> <ul style="list-style-type: none"> (c) Systems delivered to customers (SI projects, etc.) (d) Customer sites (incident response services) <p>[Other than above]</p> <ul style="list-style-type: none"> (e) Response to vulnerabilities of in-house products (hardware, software) (f) Other (describe) [_____]
<p>2.8 Authority of the CSIRT in the event of an incident</p> <ul style="list-style-type: none"> (a) Authorized to stop a system in the event of an urgent incident (Authorized to give orders and directions) (b) Can advise on the need to stop a system in the event of an urgent incident (c) Not authorized to stop a system in the event of an urgent incident

2.9 Specific services provided

[Reactive services]... Choose [in-house/outsourced/not provided] for each service

- (a) Alerts and warnings
- (b) Incident handling (on-site or guidance)
- (c) Vulnerability handling (proprietary products or vendor products/services)
- (d) Malware analysis
- (e) Forensics
- (f) Log analysis

[Proactive services]... Choose [in-house/outsourced/not provided] for each service

- (g) Public monitoring
- (h) Security trend analysis
- (i) Intrusion detection
- (j) Technology trend monitoring
- (k) Security alerts and announcements
- (l) Provision of security-related information
- (m) Security audits or reviews
- (n) Operation of security tools, applications, infrastructure, and services
- (o) Development of security tools (including those used by CSIRTs)

[Security quality control services]... Choose [in-house/outsourced/not provided] for each service

- (p) Involvement in risk assessment of new services, systems, etc.
- (q) Involvement in business continuity and fault recovery plans
- (r) Handling consultation about security-related matters
- (s) Awareness-raising activities
- (t) Education/training
- (u) Evaluation or certification of products
- (v) Involvement in the formulation of security policies

[Other] Describe if there are any other services

- (w) Other []

2.10 Is there a service level definition?

- (a) Yes
- (b) No
- (c) Other (describe) []

2.11 Are categories of reported incidents defined?

- (a) Clearly defined, documented, and approved by the person responsible for the CSIRT

	<p>and/or the CISO, and compliance with the document is managed (supervised)</p> <p>(b) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO</p> <p>(c) Clearly defined and documented but not officially approved</p> <p>(d) Roughly defined but not documented</p> <p>(e) Not defined; considered on an ad hoc basis</p>
	<p>2.12 Are the service recipients, authority, and services of the CSIRT, and the definition of incidents, etc., documented?</p>
	<p>(a) Yes</p> <p>(b) No</p> <p>(c) Other (describe) [_____]</p>
	<p>2.13 Are security policies defined?</p>
	<p>(a) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO, and compliance with the document is managed (supervised)</p> <p>(b) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO</p> <p>(c) Clearly defined and documented but not officially approved</p> <p>(d) Roughly defined but not documented</p> <p>(e) Not defined; considered on an ad hoc basis</p>
	<p>2.14 Is a system of supervision by a SOC established and operated?</p>
	<p>(a) Yes</p> <p>(b) No</p>
	<p>2.14.1 How does the SOC exercise supervision?</p>
	<p>(a) 24-hour supervision, 365 days a year</p> <p>(b) Only during business hours on weekdays</p> <p>(c) Other (describe) [_____]</p>
	<p>2.14.2 How is the SOC operated?</p>
	<p>(a) Operated internally</p> <p>(b) Outsourced to a group company</p> <p>(c) Outsourced to another company outside the group</p>
	<p>2.14.2.1 What is the relationship between the SOC and CSIRT?</p>
	<p>(a) CSIRT has SOC functions</p> <p>(b) CSIRT is established inside the SOC</p> <p>(c) Both exist as independent units and collaborate</p>
<p>3. CSIRT members</p>	

3.1 Are guidelines and a code of conduct defined?
<ul style="list-style-type: none"> (a) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO, and compliance with the document is managed (supervised) (b) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO (c) Clearly defined and documented but not officially approved (d) Roughly defined but not documented (e) Not defined; considered on an ad hoc basis
3.2 Number of members at the time of establishment
XX members
3.2.1 Ratio between regular staff and outsourced staff
<ul style="list-style-type: none"> (a) All outsourced staff (b) Regular staff less than 20% (c) Regular staff 20-39% (d) Regular staff 40-79% (e) Regular staff more than 80% (f) All regular staff
3.3 Current number of members
XX members
3.3.1 Ratio between regular staff and outsourced staff
<ul style="list-style-type: none"> (a) All outsourced staff (b) Regular staff less than 20% (c) Regular staff 20-39% (d) Regular staff 40-79% (e) Regular staff more than 80% (f) All regular staff
3.4 Are skill sets necessary for CSIRT members defined?
<ul style="list-style-type: none"> (a) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO, and compliance with the document is managed (supervised) (b) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO (c) Clearly defined and documented but not officially approved (d) Roughly defined but not documented (e) Not defined; considered on an ad hoc basis
3.5 Are there established rules and a system for providing training to CSIRT members within the organization?

	<p>(a) Clear standards exist regarding training for CSIRT members</p> <p>(b) Rough standards exist regarding training for CSIRT members</p> <p>(c) Standards do not exist regarding training for CSIRT members and are considered on an ad hoc basis</p>
3.6	Is there an established system for CSIRT members to receive technical training outside the organization?
	<p>(a) Clear standards exist regarding training for CSIRT members</p> <p>(b) Rough standards exist regarding training for CSIRT members</p> <p>(c) Standards do not exist regarding training for CSIRT members and are considered on an ad hoc basis</p>
3.7	Is there an established system for CSIRT members to receive communication training outside the organization? (training regarding presentation and communication skills)
	<p>(a) Clear standards exist regarding training for CSIRT members</p> <p>(b) Rough standards exist regarding training for CSIRT members</p> <p>(c) Standards do not exist regarding training for CSIRT members and are considered on an ad hoc basis</p>
3.8	Is there a system (tests, qualifications, etc.) for quantitatively measuring the skills of members?
	<p>(a) Yes</p> <p>(b) No</p> <p>(c) Other (describe) [_____]</p>
4. Processes and rules	
4.1	Are rules for escalation to management (or an information security committee, etc., that includes management) defined?
	<p>(a) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO, and compliance with the document is managed (supervised)</p> <p>(b) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO</p> <p>(c) Clearly defined and documented but not officially approved</p> <p>(d) Roughly defined but not documented</p> <p>(e) Not defined; considered on an ad hoc basis</p>
4.2	Are rules for escalation to the public relations department defined?
	<p>(a) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO, and compliance with the document is managed (supervised)</p> <p>(b) Clearly defined, documented, and approved by the person responsible for the CSIRT</p>

	<p>and/or the CISO</p> <p>(c) Clearly defined and documented but not officially approved</p> <p>(d) Roughly defined but not documented</p> <p>(e) Not defined; considered on an ad hoc basis</p>
	<p>4.3 Are rules for escalation to the legal department defined?</p> <p>(a) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO, and compliance with the document is managed (supervised)</p> <p>(b) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO</p> <p>(c) Clearly defined and documented but not officially approved</p> <p>(d) Roughly defined but not documented</p> <p>(e) Not defined; considered on an ad hoc basis</p>
	<p>4.4 Are processes for preventing, detecting, and resolving incidents defined?</p> <p>(a) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO, and compliance with the document is managed (supervised)</p> <p>(b) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO</p> <p>(c) Clearly defined and documented but not officially approved</p> <p>(d) Roughly defined but not documented</p> <p>(e) Not defined; considered on an ad hoc basis</p>
	<p>4.5 Is there a defined system to have the CSIRT's activities audited through internal and/or external assessments and receive feedback?</p> <p>(a) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO, and compliance with the document is managed (supervised)</p> <p>(b) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO</p> <p>(c) Clearly defined and documented but not officially approved</p> <p>(d) Roughly defined but not documented</p> <p>(e) Not defined; considered on an ad hoc basis</p>
	<p>4.6 Is there a defined communication flow among CSIRT members and related staff in case of emergency?</p> <p>(a) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO, and compliance with the document is managed (supervised)</p> <p>(b) Clearly defined, documented, and approved by the person responsible for the CSIRT</p>

<p>and/or the CISO</p> <p>(c) Clearly defined and documented but not officially approved</p> <p>(d) Roughly defined but not documented</p> <p>(e) Not defined; considered on an ad hoc basis</p>
<p>4.7 Is there a web page explaining the aims and services of the CSIRT on the company's website?</p>
<p>(a) Yes</p> <p>(b) No</p> <p>(c) Other (describe) [_____]</p>
<p>4.8 Is there a defined method for handling incident reports and information that contain sensitive contents?</p>
<p>(a) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO, and compliance with the document is managed (supervised)</p> <p>(b) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO</p> <p>(c) Clearly defined and documented but not officially approved</p> <p>(d) Roughly defined but not documented</p> <p>(e) Not defined; considered on an ad hoc basis</p>
<p>4.9 Is there a defined system for periodically reporting CSIRT activities to management (or an information security committee, etc., that includes management)?</p>
<p>(a) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO, and compliance with the document is managed (supervised)</p> <p>(b) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO</p> <p>(c) Clearly defined and documented but not officially approved</p> <p>(d) Roughly defined but not documented</p> <p>(e) Not defined; considered on an ad hoc basis</p>
<p>4.10 Are there defined rules, etc., for statistically processing categorized incidents and disclosing relevant information to service recipients and others?</p>
<p>(a) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO, and compliance with the document is managed (supervised)</p> <p>(b) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO</p> <p>(c) Clearly defined and documented but not officially approved</p>

	<ul style="list-style-type: none"> (d) Roughly defined but not documented (e) Not defined; considered on an ad hoc basis
4.11	Is there a defined system for conducting periodic meetings in the CSIRT?
	<ul style="list-style-type: none"> (a) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO, and compliance with the document is managed (supervised) (b) Clearly defined, documented, and approved by the person responsible for the CSIRT and/or the CISO (c) Clearly defined and documented but not officially approved (d) Roughly defined but not documented (e) Not defined; considered on an ad hoc basis
5. Tools	
5.1	Are IT assets managed as an organization?
	<ul style="list-style-type: none"> (a) Yes (b) No
5.2	Are there a tracking system and workflow for tracking incident response?
	<ul style="list-style-type: none"> (a) Yes (b) No
6. Revision of system and rules	
6.1	Is the scope of service provision periodically reviewed?
	<ul style="list-style-type: none"> (a) At least once a month (b) Once a quarter (c) Once every 6 months (d) Once a year (e) Less than once a year (f) Not done
6.2	Are security policies and other documents periodically reviewed?
	<ul style="list-style-type: none"> (a) At least once a month (b) Once a quarter (c) Once every 6 months (d) Once a year (e) Less than once a year (f) Not done
6.3	Is the communication flow chart (email addresses, phone numbers, etc.) periodically reviewed?
	<ul style="list-style-type: none"> (a) At least once a month (b) Once a quarter

	<ul style="list-style-type: none"> (c) Once every 6 months (d) Once a year (e) Less than once a year (f) Not done
7. Reports	
7.1 Are reports issued periodically?	
	<ul style="list-style-type: none"> (a) At least once a month (b) Once a quarter (c) Once every 6 months (d) Once a year (e) Less than once a year (f) Not done
7.1.2 Scope of disclosure	
	<ul style="list-style-type: none"> (a) Persons in charge (b) Relevant department(s) (c) Entire company

1.3.2. INTERVIEWS

Interviews were conducted with the NCA member CSIRTs listed in Table 1.3.2 (9 teams).

[Table 1.3.2] Organizations interviewed

#	Team Name (Abbr.)	Affiliation	Interview Date
1	ASY-CSIRT	ANA Systems Co., Ltd.	January 18, 2016
2	DeNA CERT	DeNA Co., Ltd.	February 12, 2016
3	FJC-CERT	Fujitsu Limited	December 14, 2015
4	Fuji Xerox CERT	Fuji Xerox Co., Ltd.	December 24, 2015
5	I-SIRT	Imperial Hotel, Ltd.	January 20, 2016
6	MB-SIRT	Mori Building Co., Ltd.	December 25, 2015
7	NTT-CERT	Nippon Telegraph and Telephone Corporation	February 10, 2016
8	T-SIRT	Taisei Corporation	December 07, 2015
9	YMC-CSIRT	Yamaha Motor Co., Ltd.	February 03, 2016

* In alphabetical order by team name

Table 1.3.3 outlines items covered in interviews with the CSIRTs. As for the "organizational model" adopted by each of these CSIRTs, an approximate model was chosen by JPCERT/CC based on the classifications listed in "Organizational Models for CSIRTs*2" published by JPCERT/CC.

[Table 1.3.3] Interview items

#	Interview Items	Description
1	Overview of the organization	Relationship with the organization to which it belongs and circumstances of establishment, with a focus on service overview
2	Structure and authority of the CSIRT	Whether CSIRT personnel are dedicated members or have other concurrent duties, the organizational model, the department(s) to which the CSIRT belongs, etc. Whether it has the authority to suspend a system in event of a security incident or in response to vulnerability information, etc.
3	Outputs of CSIRT activities	Whether activity reports submitted to management and periodic reports directed to readers inside and outside the company are issued, and whether there are assessment materials for CSIRT activities, etc.
4	Education/training of CSIRT members	Matters concerning the implementation of incident response exercises, etc., in the company, metrics for assessing technical skills of CSIRT personnel, and development of CSIRT personnel
5	Review period of structure, services and management functions of the CSIRT	Matters concerning optimization, including the review of CSIRT services and their scope, security policies and other documents, contact lists, etc.
6	Summary	General overview, characteristics of the CSIRT, etc.

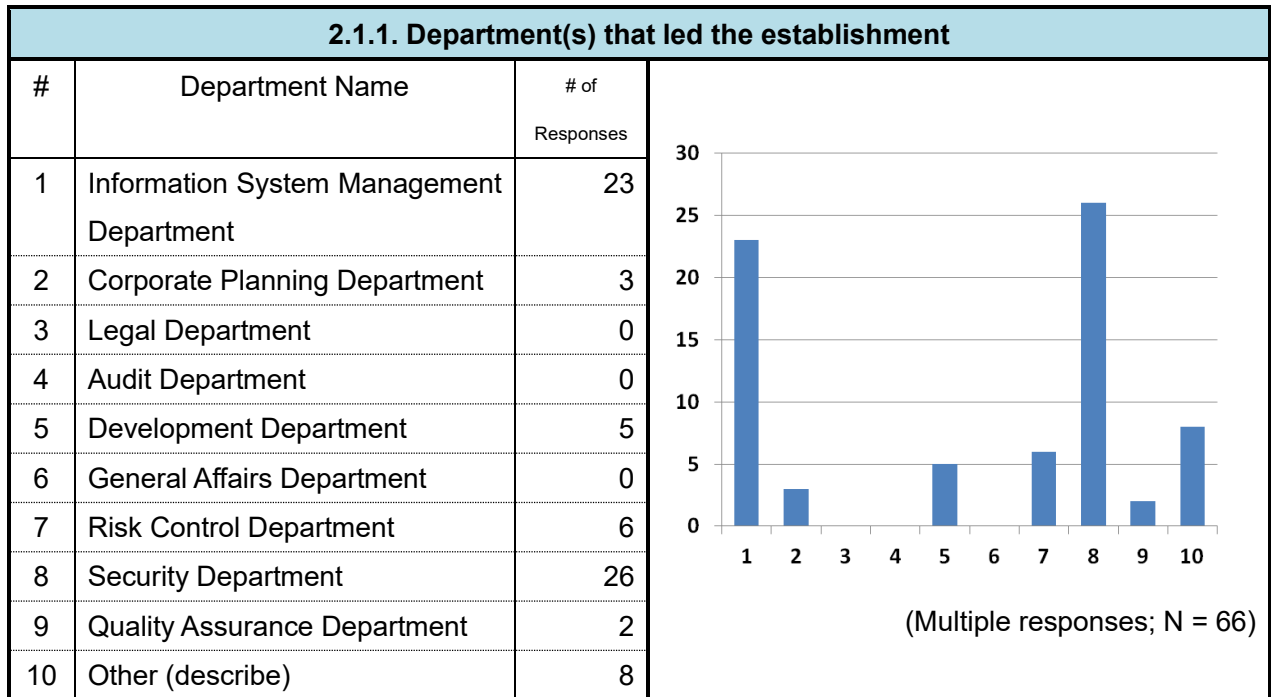
*2Organizational Models for CSIRTs:
https://www.jpccert.or.jp/csirt_material/files/05_shape_of_csirt20151126.pdf

2. QUESTIONNAIRE RESULTS

2.1. STRUCTURE AT THE TIME OF ESTABLISHMENT

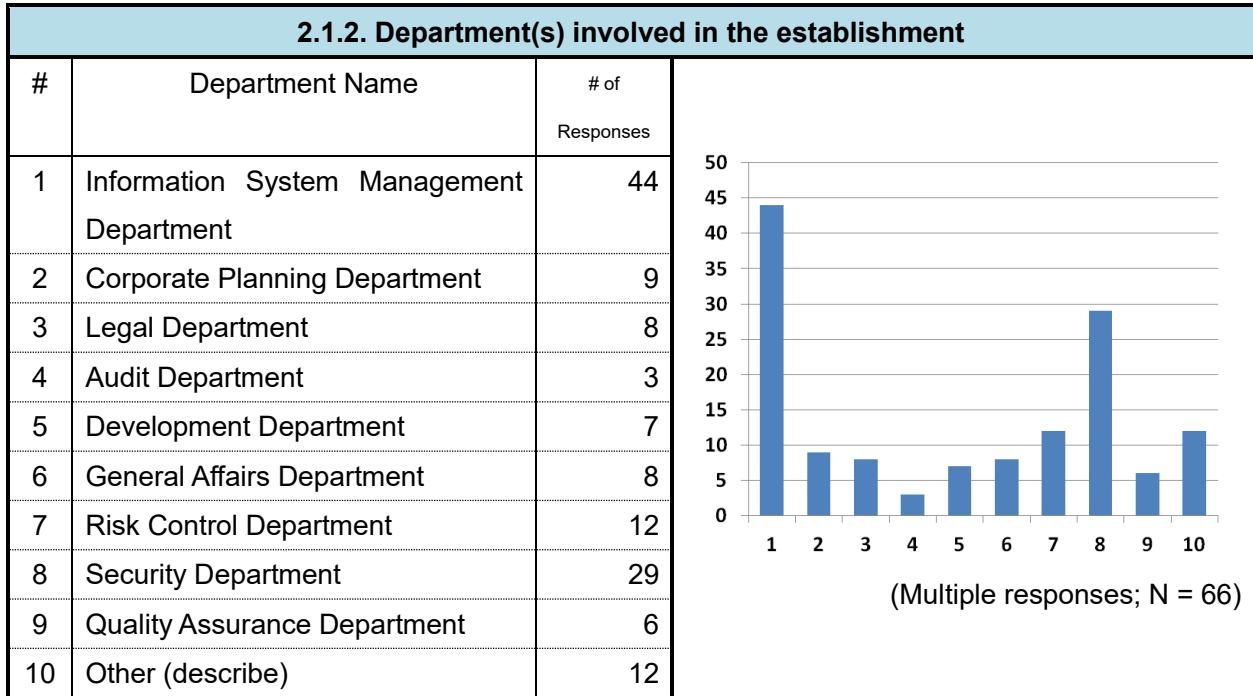
2.1.1. DEPARTMENT(S) THAT LED THE ESTABLISHMENT

A majority of the CSIRTs were established under the leadership of their companies' information system management departments and/or security departments.



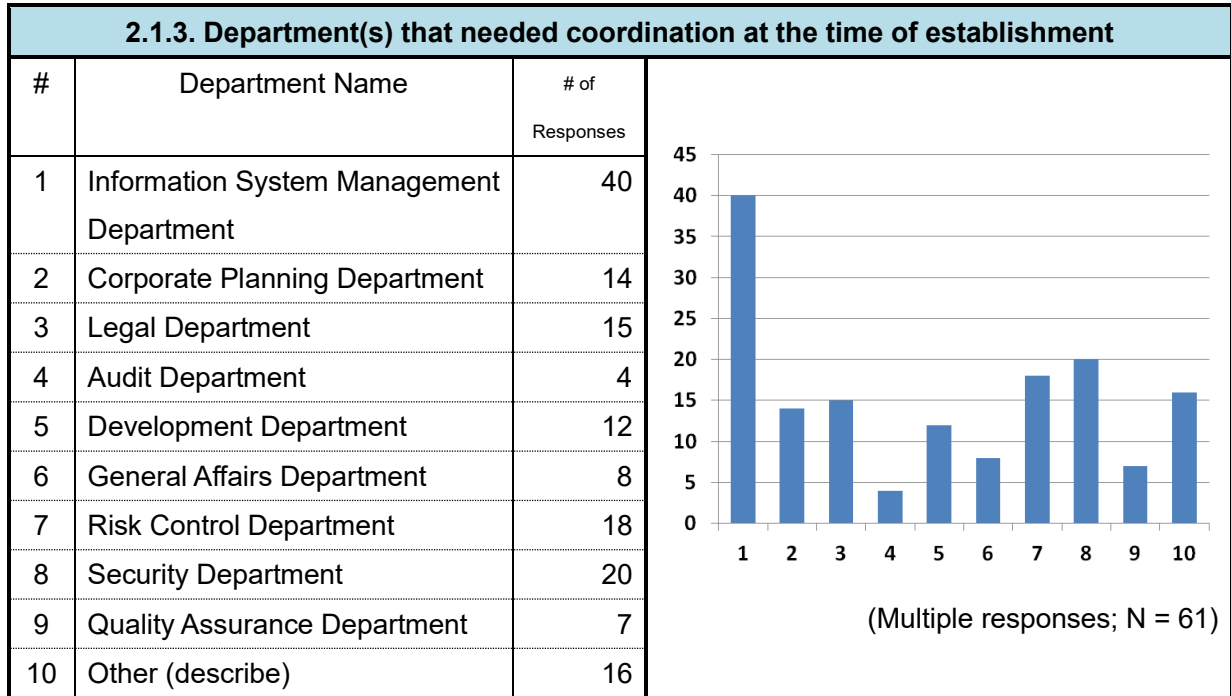
2.1.2. DEPARTMENT(S) INVOLVED IN THE ESTABLISHMENT

In addition to information system management and security departments, which led the establishment, corporate planning and general affairs departments were also involved in the establishment of the CSIRTs.



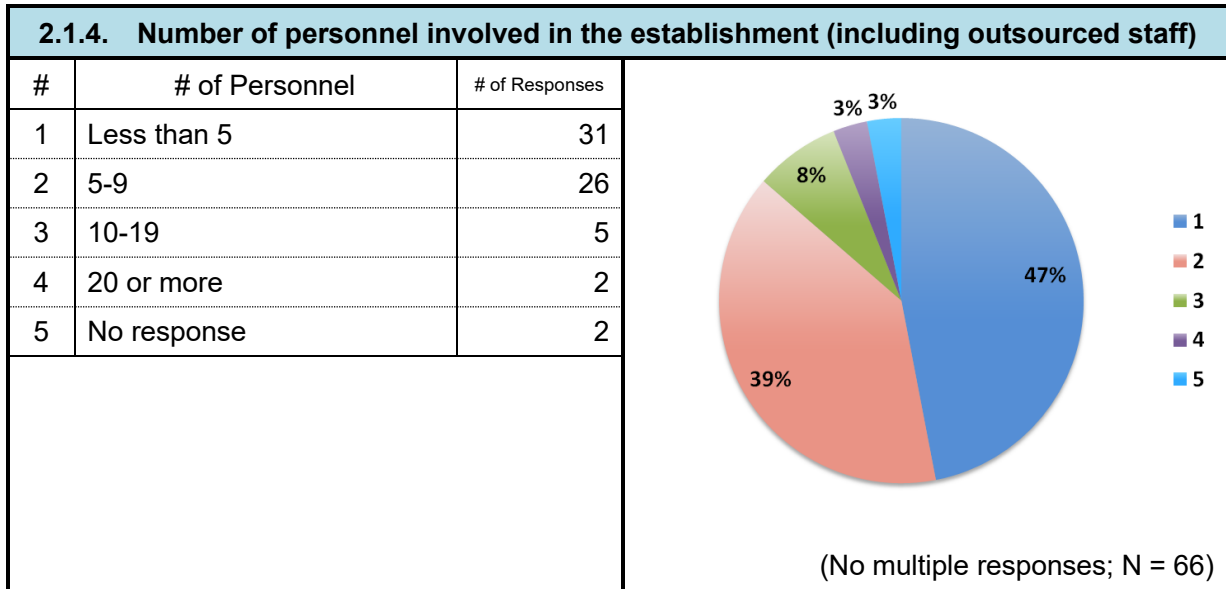
2.1.3. DEPARTMENT(S) THAT NEEDED COORDINATION AT THE TIME OF ESTABLISHMENT

Their information system management departments, which led the establishment, required coordination most for the establishment of CSIRTs, while various other departments also required coordination.



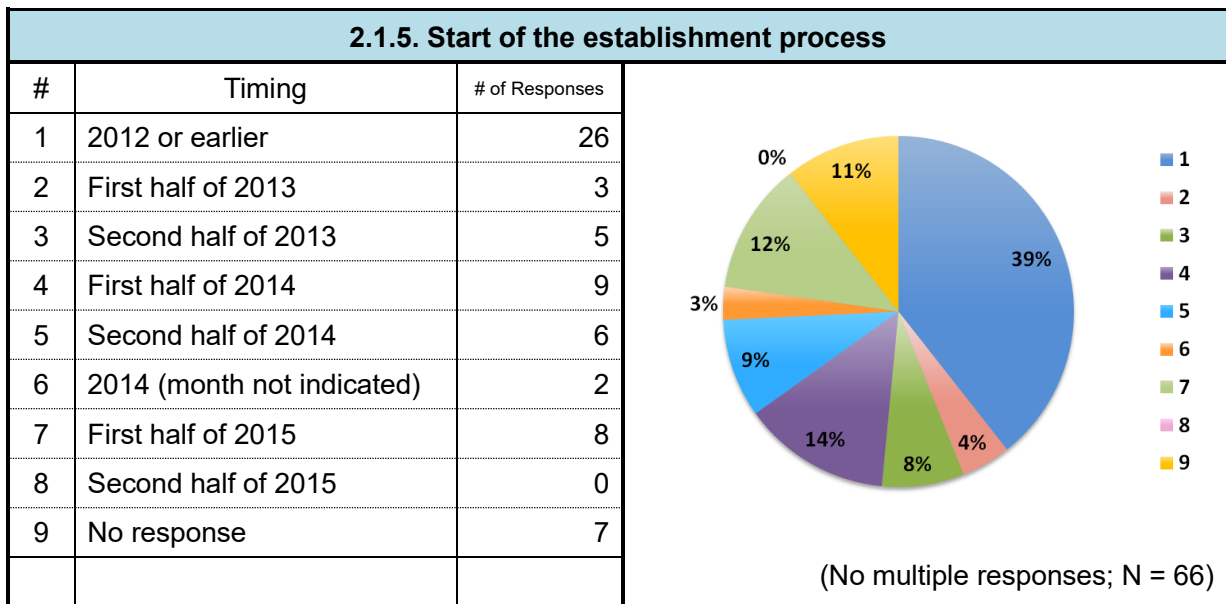
2.1.4. NUMBER OF PERSONNEL INVOLVED IN THE ESTABLISHMENT (INCLUDING OUTSOURCED STAFF)

About half of the organizations have less than 5 members. More than 80% of the CSIRTs have less than 10 members.



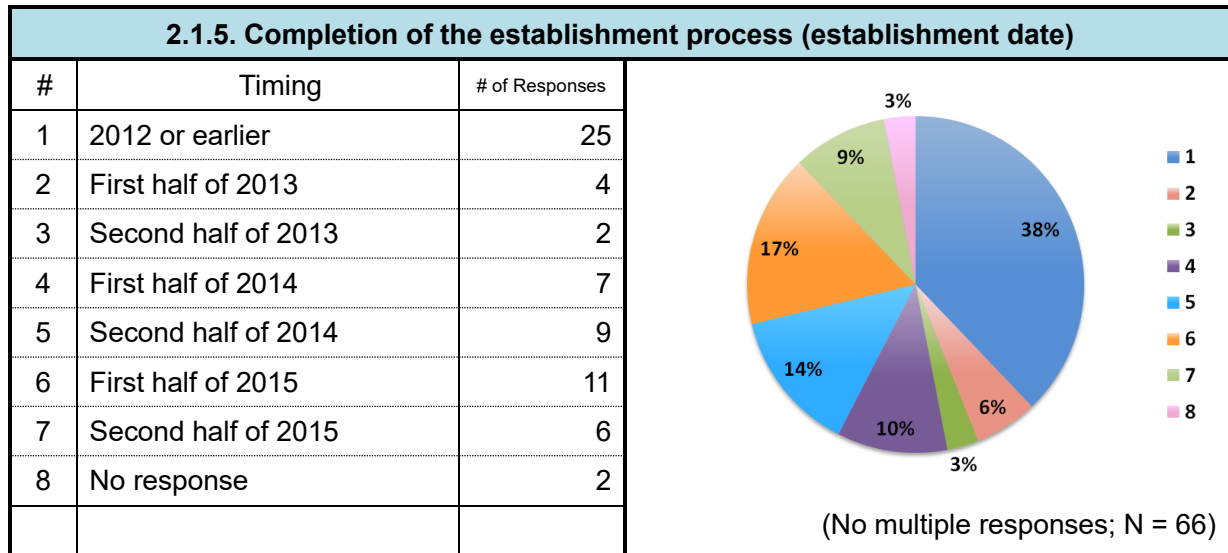
2.1.5. START OF THE ESTABLISHMENT PROCESS

About half of the organizations started the establishment of their CSIRTs in 2014 or later.



2.1.6. COMPLETION OF THE ESTABLISHMENT PROCESS (ESTABLISHMENT DATE)

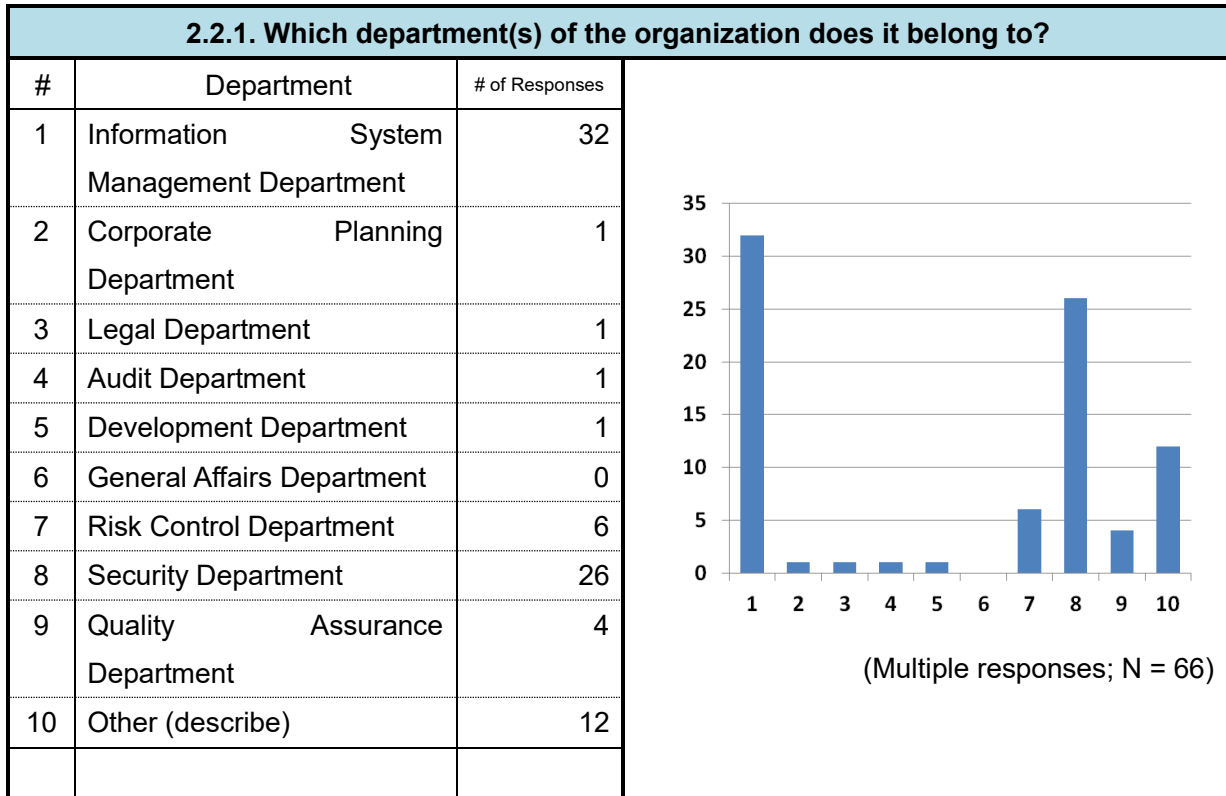
More than half of the organizations completed the establishment of their CSIRTs in 2014 or later. Time taken for establishment will be stated in Appendix 1 (p. 114).



2.2. STRUCTURE OF CSIRT

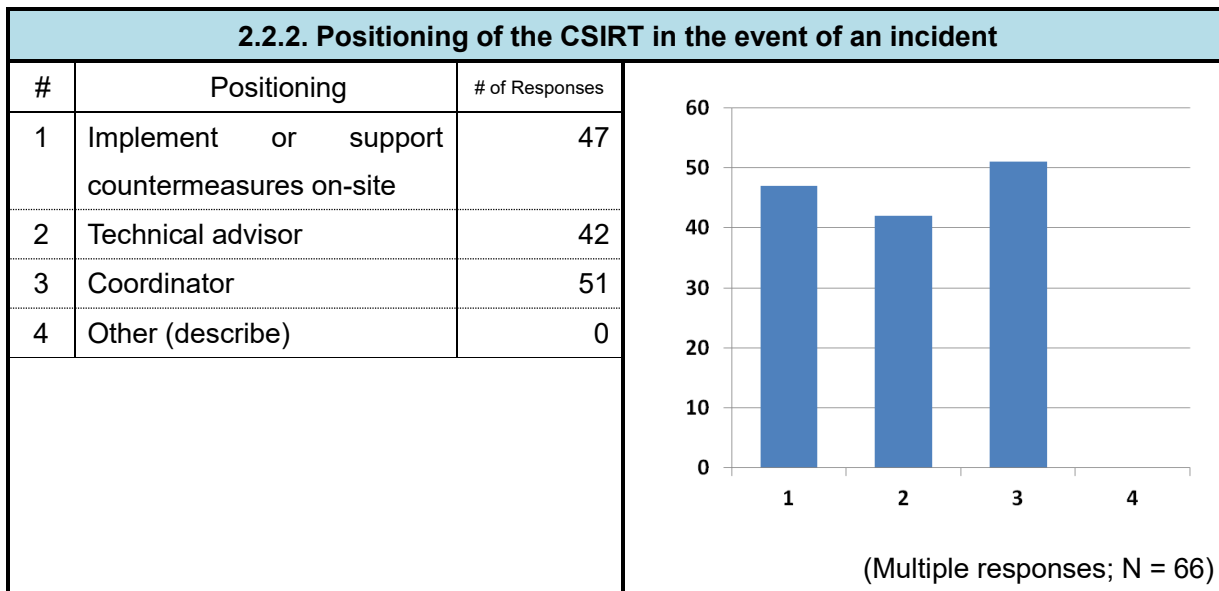
2.2.1. WHICH DEPARTMENT(S) OF THE ORGANIZATION DOES IT BELONG TO?

Many of the organizations set up their CSIRTs in information system management or security departments, which led the establishment. Three respondents stated "Research Department" in "Other."



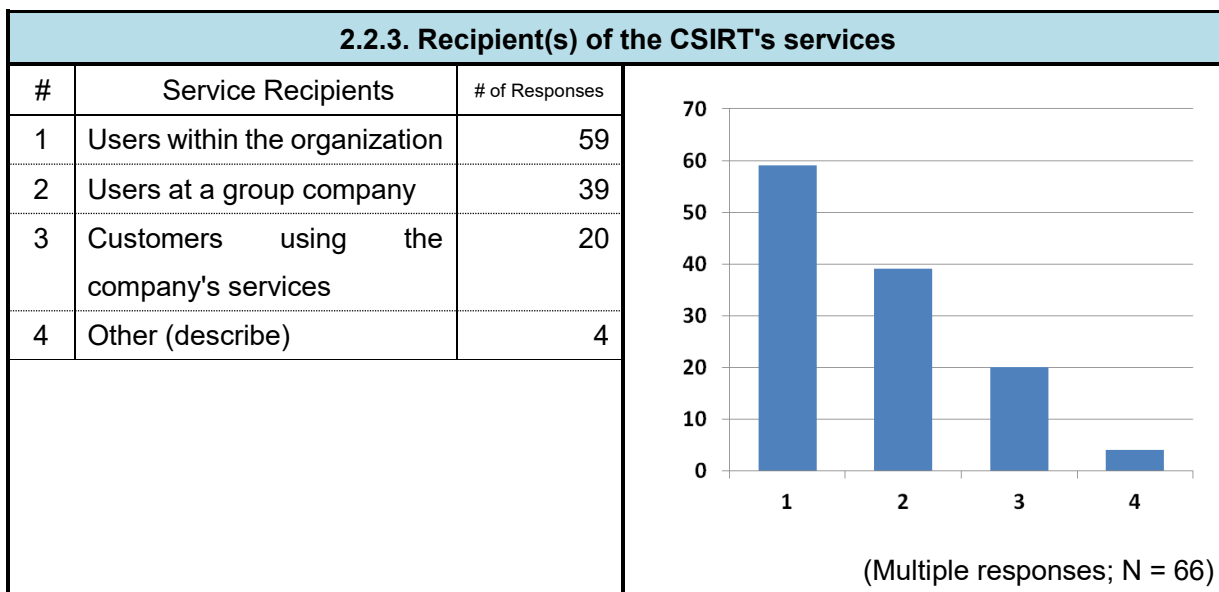
2.2.2. POSITIONING OF THE CSIRT IN THE EVENT OF AN INCIDENT

In the event of an incident, CSIRTs are expected to play a wide range of roles, from responding on-site to providing support and coordination.



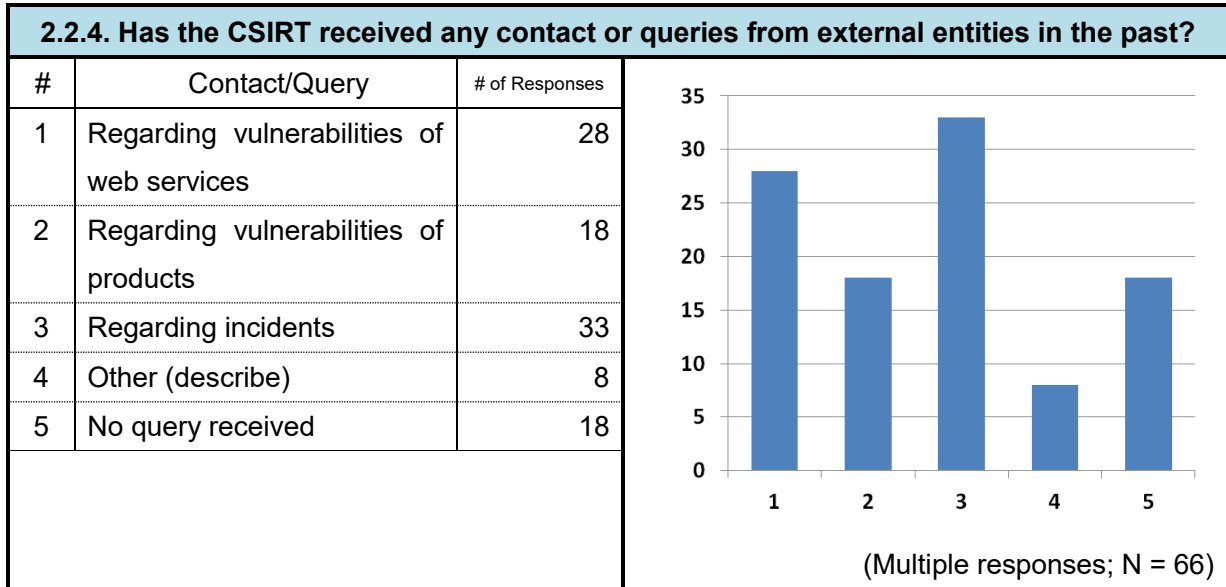
2.2.3. RECIPIENT(S) OF THE CSIRT'S SERVICES

Many of the CSIRTs provide services within their organization or to their group companies. Approximately 30% of the organizations provide services to customers of their organizations.



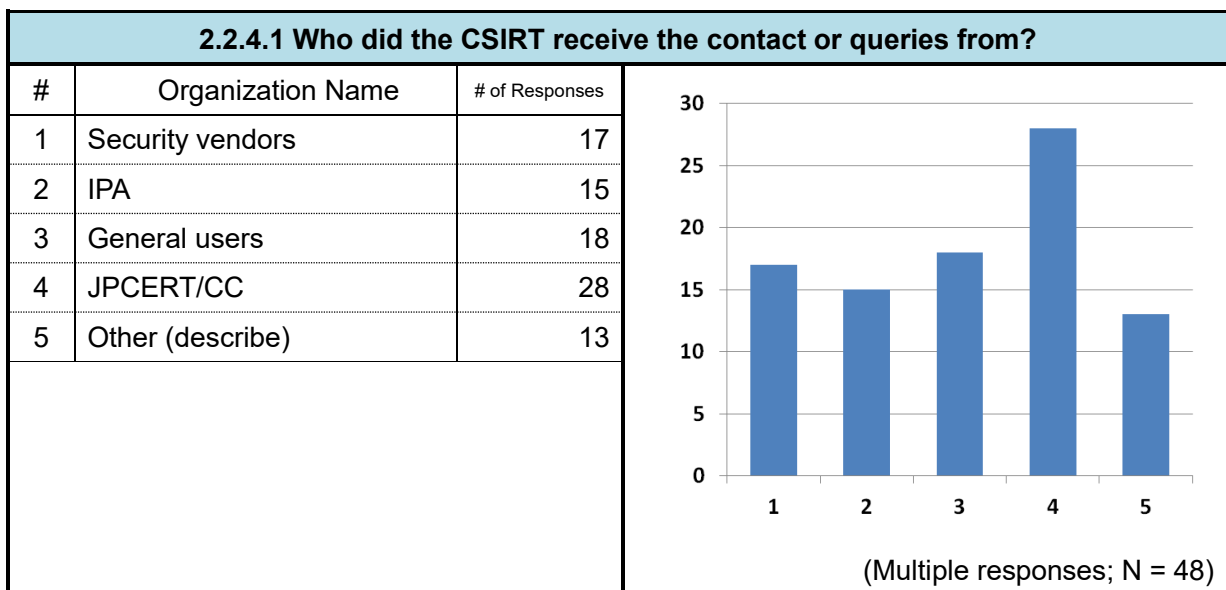
2.2.4. HAS THE CSIRT RECEIVED ANY CONTACT OR QUERIES FROM EXTERNAL ENTITIES IN THE PAST?

Many CSIRTs have received contact or queries from external entities.



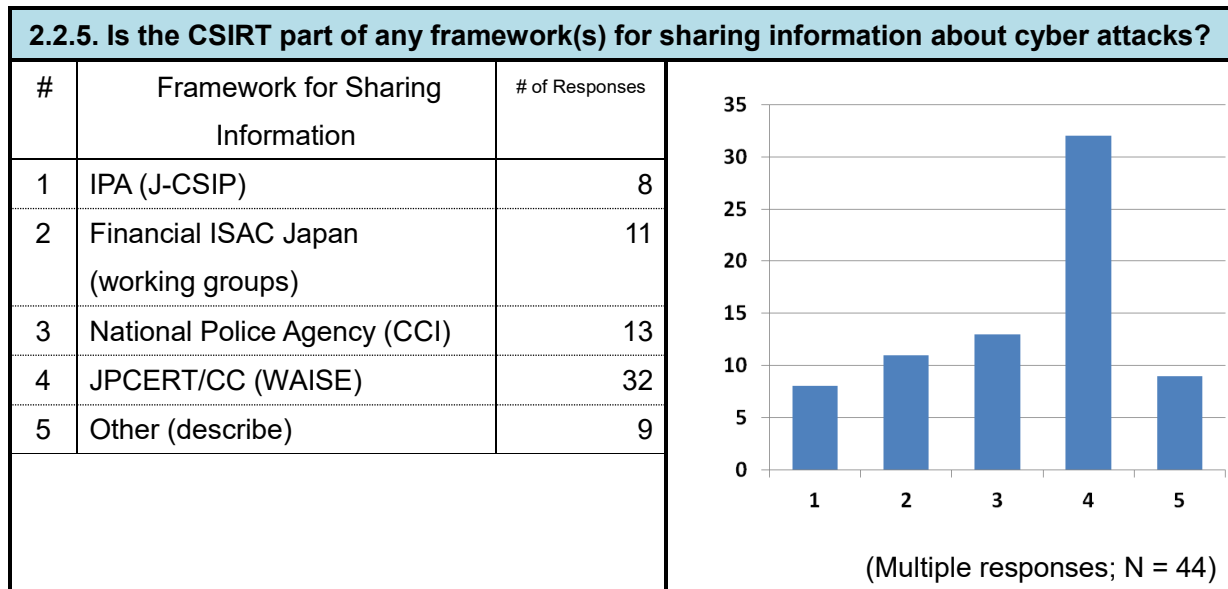
2.2.4.1. WHO DID THE CSIRT RECEIVE THE CONTACT OR QUERIES FROM?

Many organizations have contacted the CSIRTs, but contact and queries from JPCERT/CC make up the majority.



2.2.5. IS THE CSIRT PART OF ANY FRAMEWORK(S) FOR SHARING INFORMATION ABOUT CYBER ATTACKS?

The framework operated by JPCERT/CC is used as a framework*³ for sharing information about cyber attacks. Five respondents stated "other CSIRTs" in "Other."



*³ J-CSIP(Initiative for Cyber Security Information sharing Partnership of Japan):

<https://www.ipa.go.jp/security/J-CSIP/>

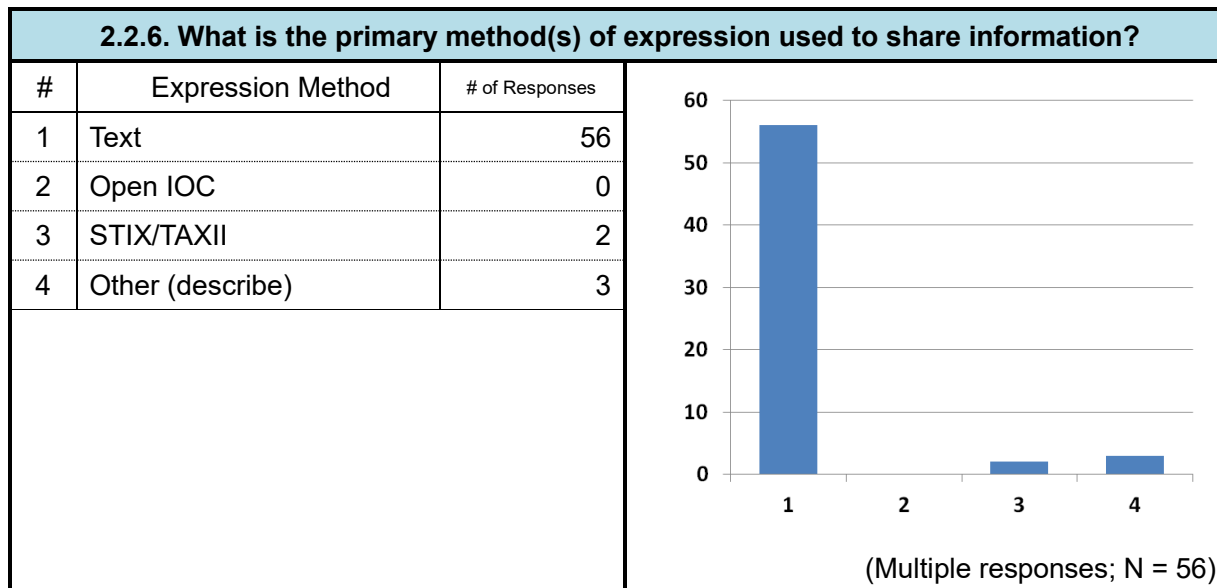
Financial ISAC Japan: http://www.f-isac.jp/working_group/

CCI (Counter Cyber Intelligence)

WAISE(Watch and Warning Analysis Information for Security Experts): <https://www.jpcert.or.jp/wwinfo/>

2.2.6. WHAT IS THE PRIMARY METHOD(S) OF EXPRESSION USED TO SHARE INFORMATION?

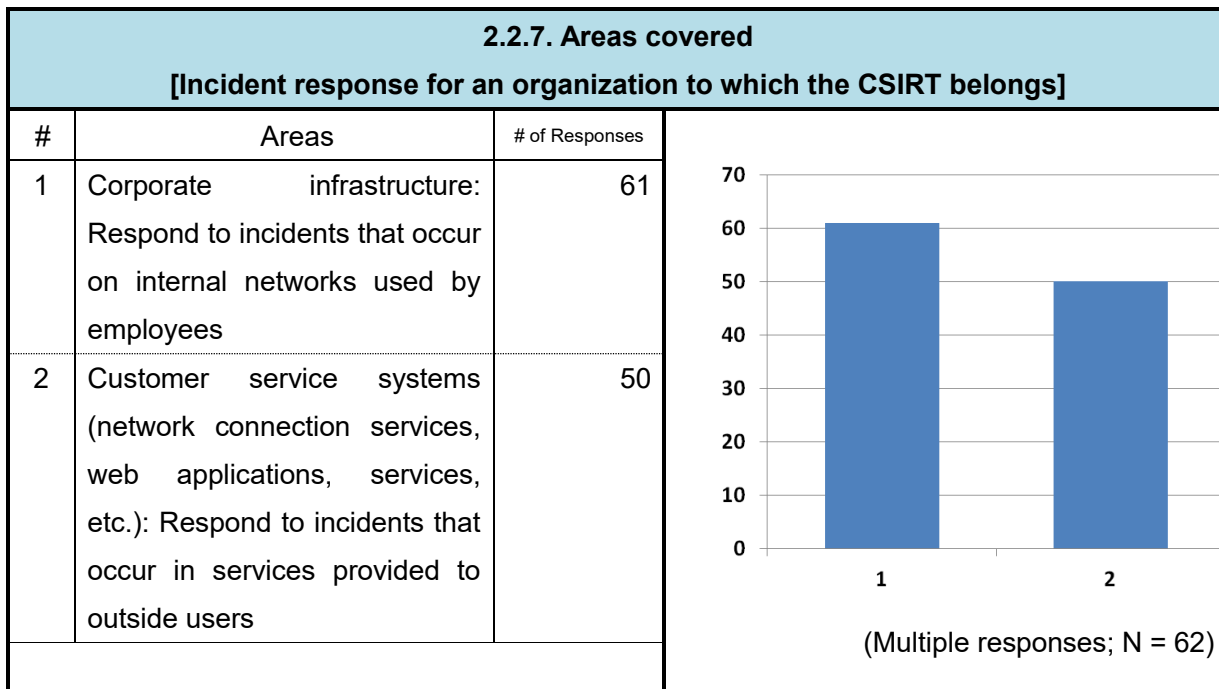
The primary method of expression*⁴ used to share information is almost entirely text.



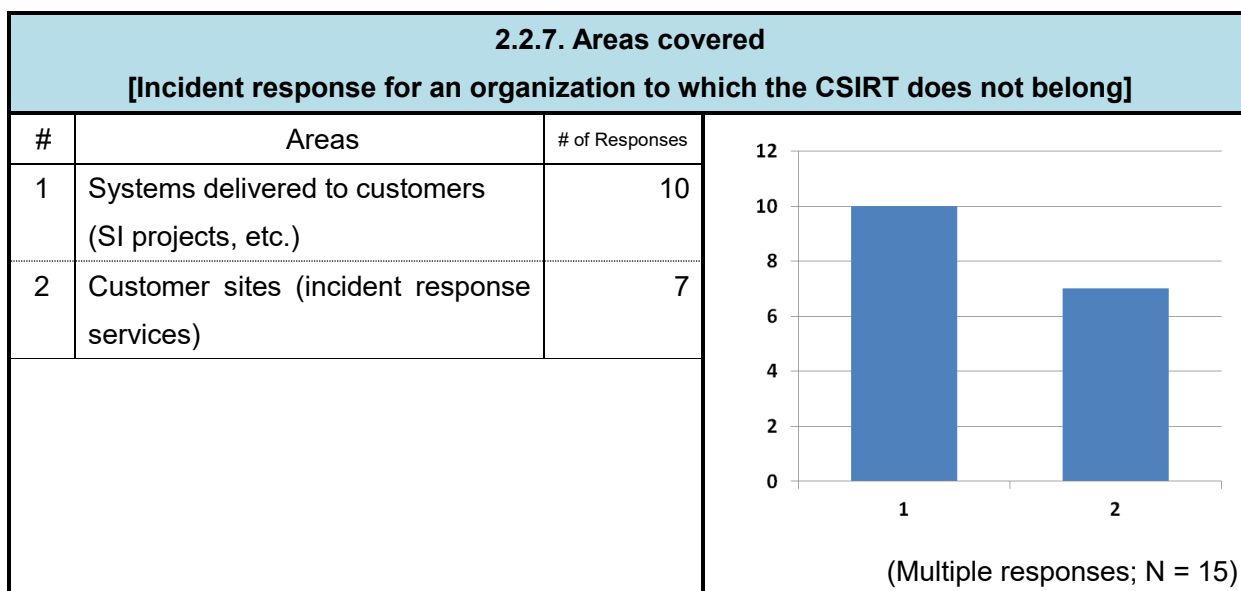
*⁴ Open IOC: <http://www.openioc.org/>
 STIX: <https://stixproject.github.io/about/>
 TAXII: <https://taxiiproject.github.io/about/>

2.2.7. AREAS COVERED

As for areas covered by services provided by the CSIRTs, almost all CSIRTs responded that they handle incidents that occurs in networks used by their own company or systems for services provided to customers.

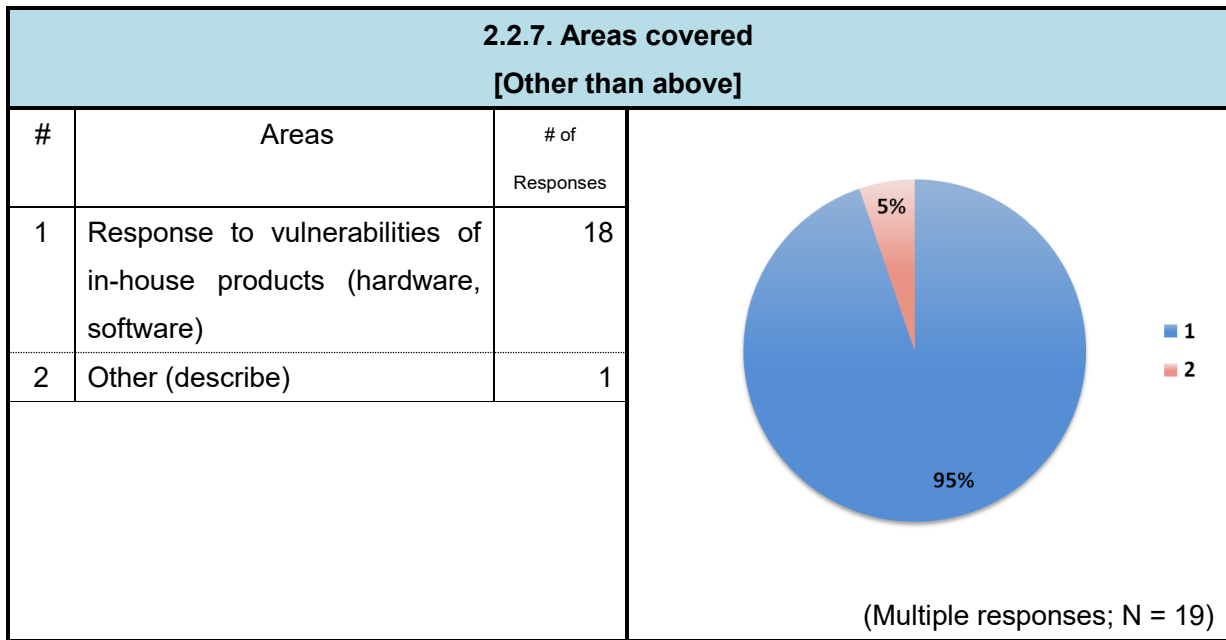


Only about 20% of the CSIRTs provide incident response services to customers, etc., outside their organizations.



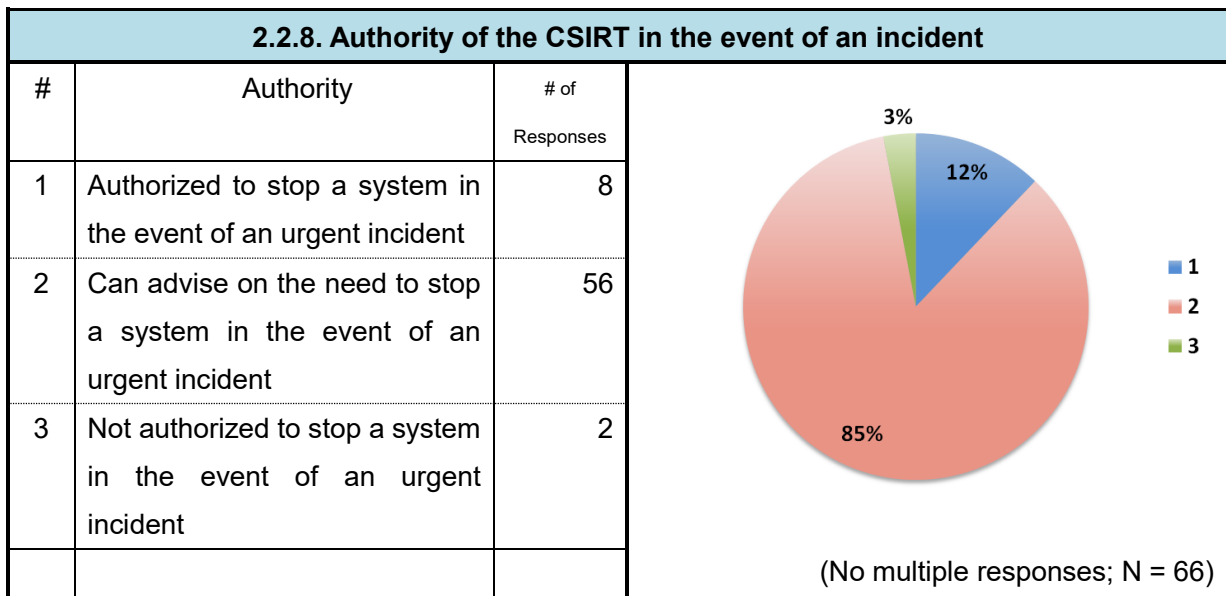
Some of the CSIRTs provide services that respond to vulnerabilities of their own products (hardware,

software) as a PSIRT*⁵ in addition to incident response.



2.2.8. AUTHORITY OF THE CSIRT IN THE EVENT OF AN INCIDENT

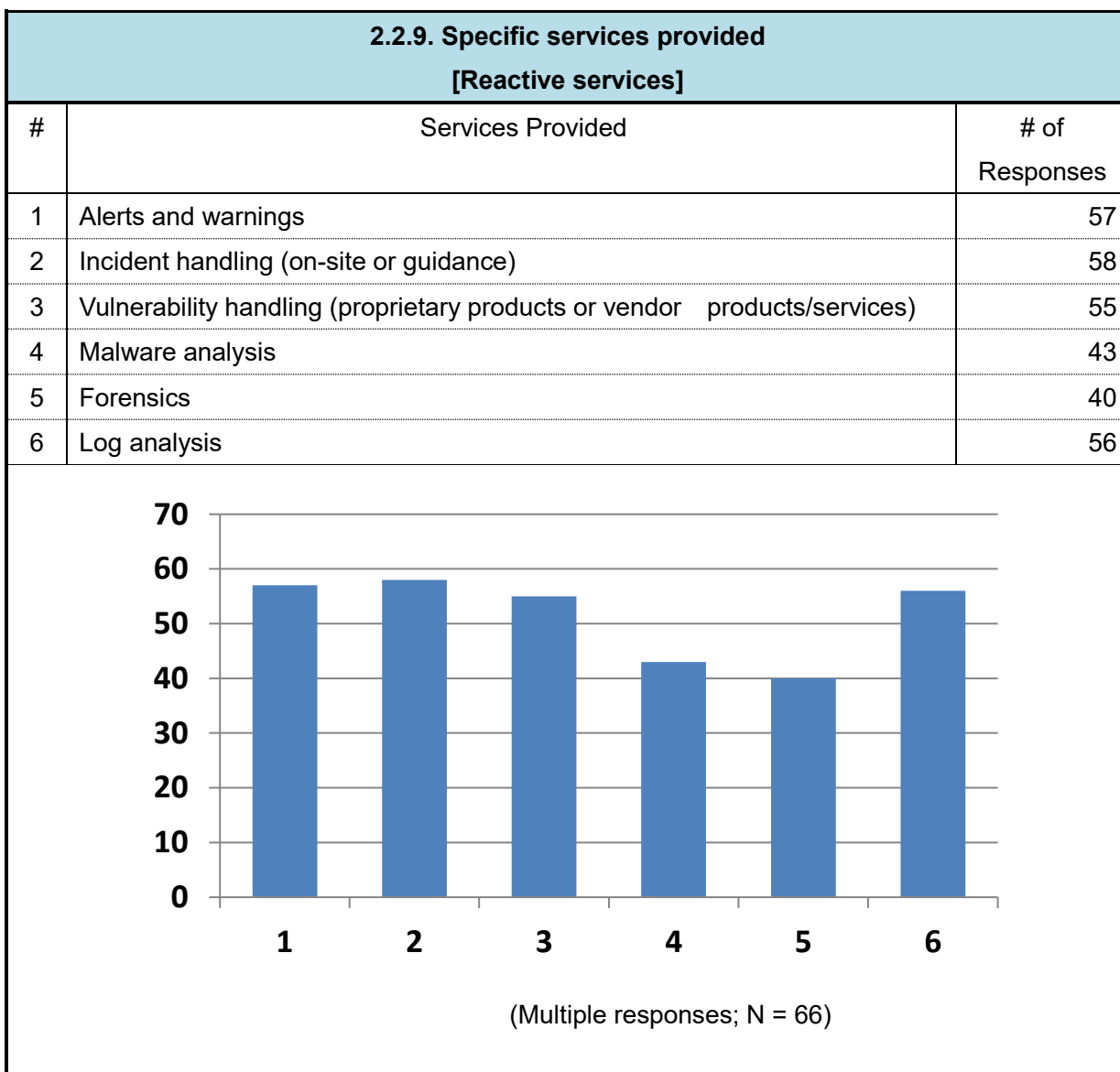
In the event of an urgent incident, about 90% of the CSIRTs are in a position that allows them to advise on the need to stop the systems concerned. About 10% of the CSIRTs also have the authority to order that the systems be be stopped.



*⁵ PSIRT: Stands for Product Security Incident Response Team. A PSIRT is responsible for receiving information related to vulnerabilities of software and software products, coordinating efforts within its own company to fix the vulnerabilities, and publishing relevant information.

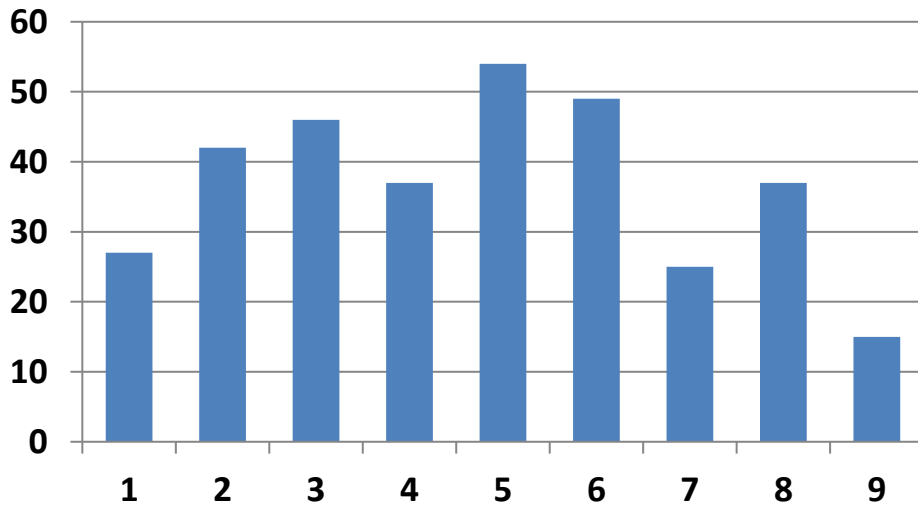
2.2.9. SPECIFIC SERVICES PROVIDED

The CSIRTs were asked about details of the reactive services, proactive services, and security quality control services they provide. The most common type of reactive services the CSIRTs provide is "incident handling." As for proactive services, many of the CSIRTs provide "security alerts and announcements," which shows that they emphasize their role of disseminating information to help prevent incidents. In the area of security quality control services, many of the CSIRTs provide services such as "awareness-raising activities" and "education/training," showing that they focus on raising awareness about security within their own organizations.



**2.2.9. Specific services provided
[Proactive services]**

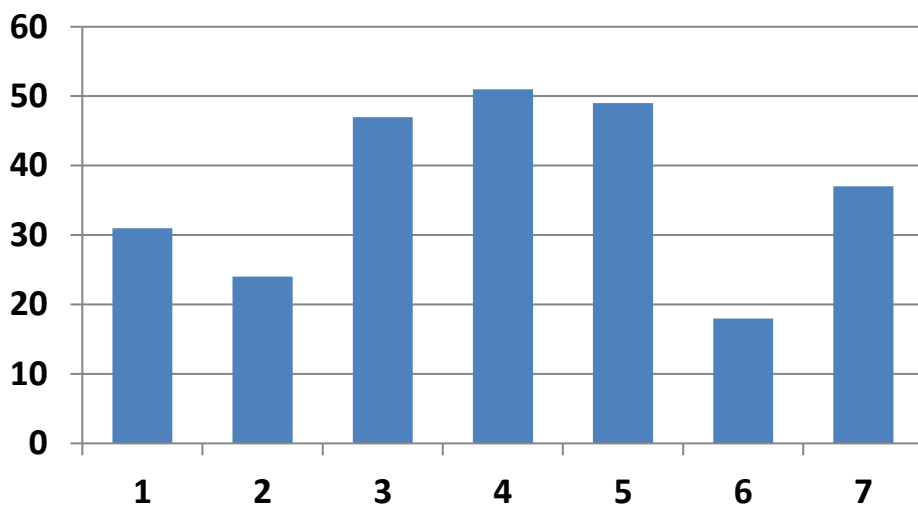
#	Services Provided	# of Responses
1	Public monitoring	27
2	Security trend analysis	42
3	Intrusion detection	46
4	Technology trend monitoring	37
5	Security alerts and announcements	54
6	Provision of security-related information	49
7	Security audits or reviews	25
8	Operation of security tools, applications, infrastructure, and services	37
9	Development of security tools (including those used by the CSIRT)	15



(Multiple responses; N = 66)

2.2.9. Specific services provided
[Security quality control services]

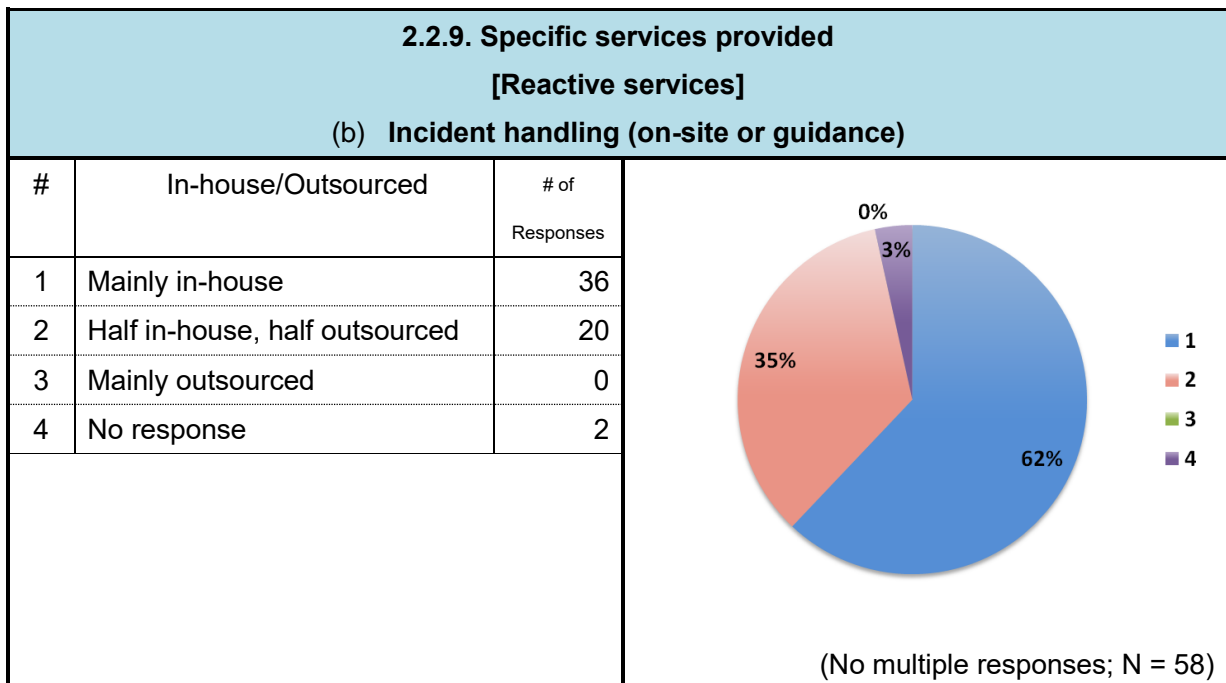
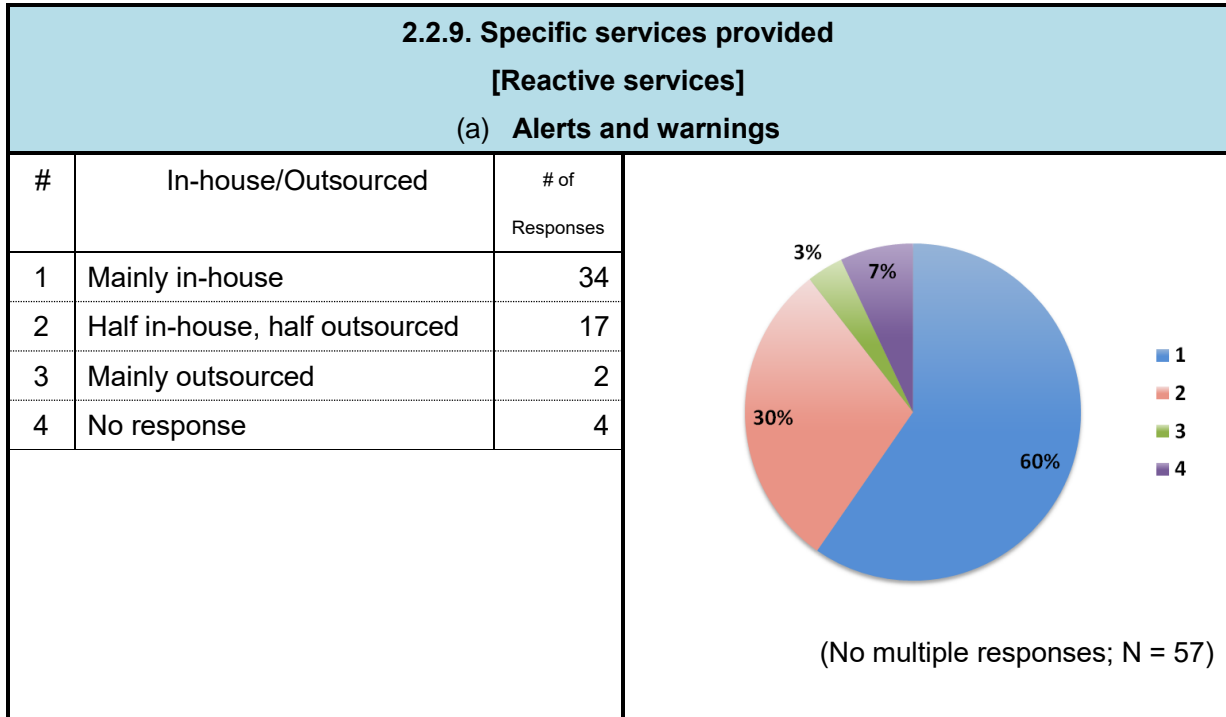
#	Services Provided	# of Responses
1	Involvement in risk assessment of new services, systems, etc.	31
2	Involvement in business continuity and fault recovery plans	24
3	Handling consultation about security-related matters	47
4	Awareness-raising activities	51
5	Education/training	49
6	Evaluation or certification of products	18
7	Involvement in the formulation of security policies	37

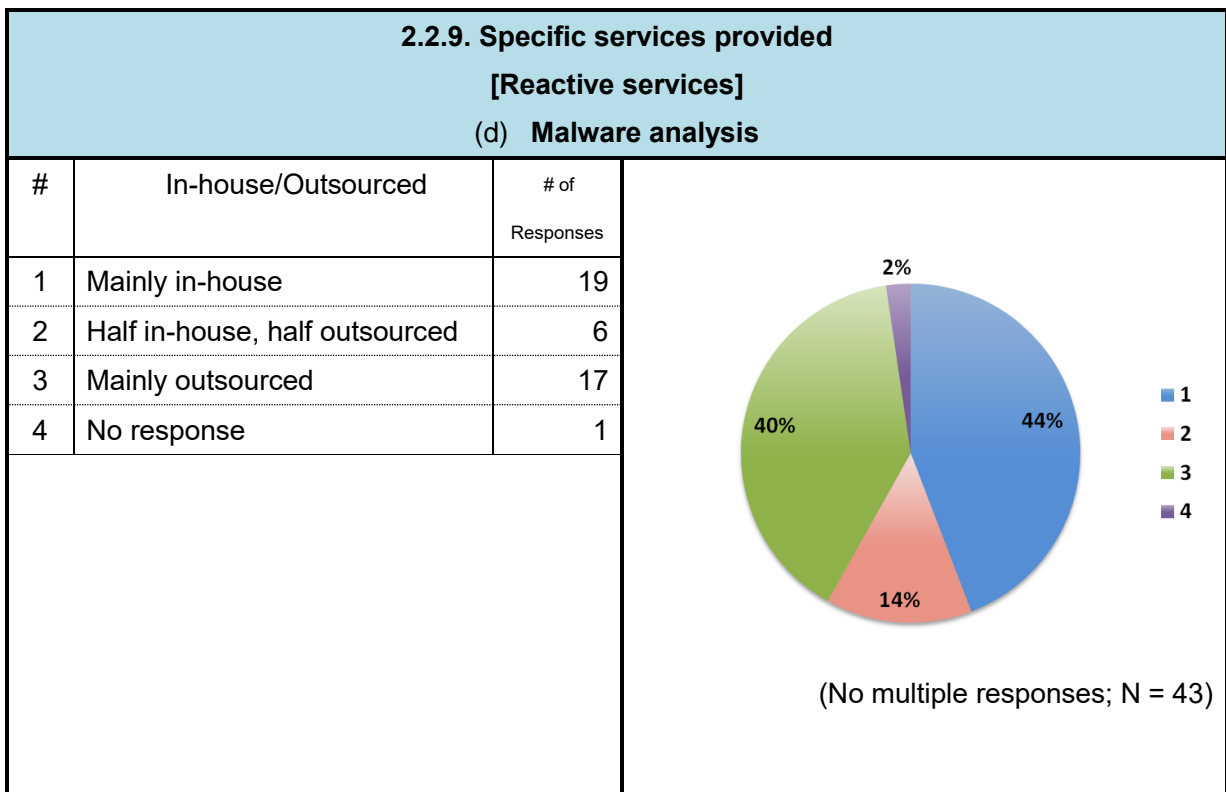
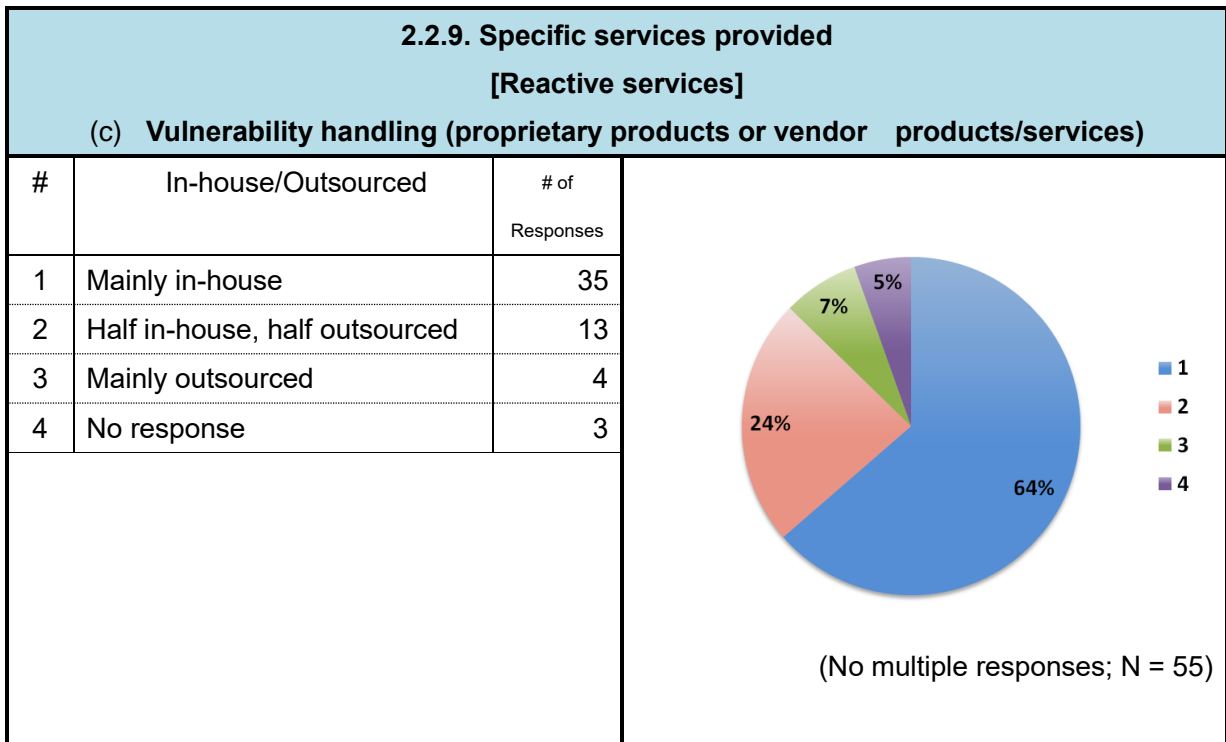


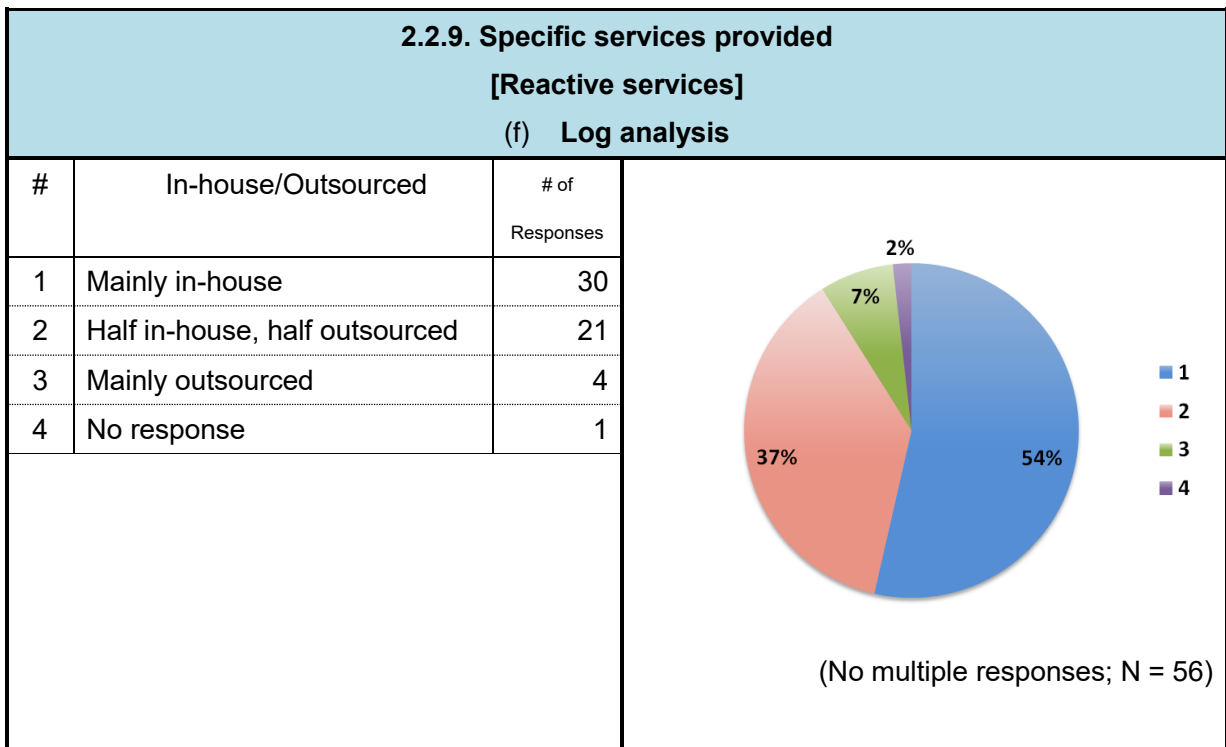
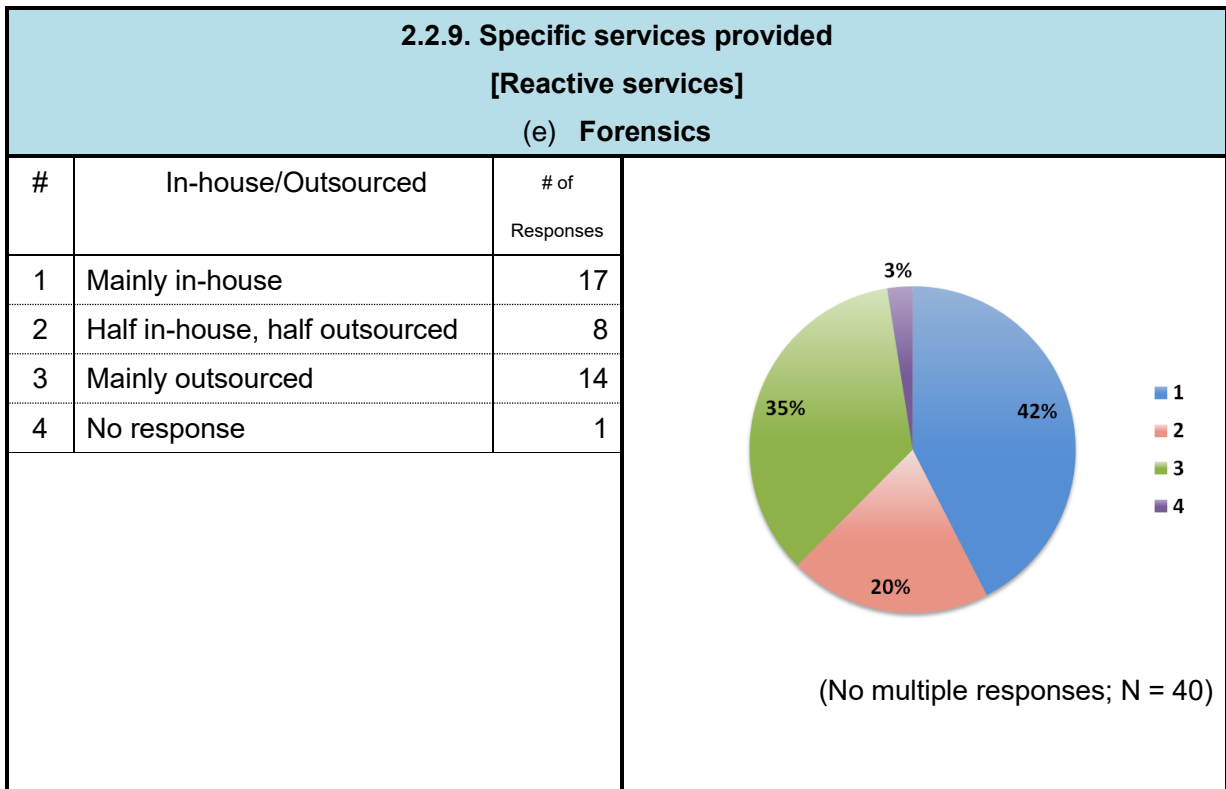
(Multiple responses; N = 66)

The proportions of services provided by the CSIRTs in-house and outsourced to external service providers are as follows.

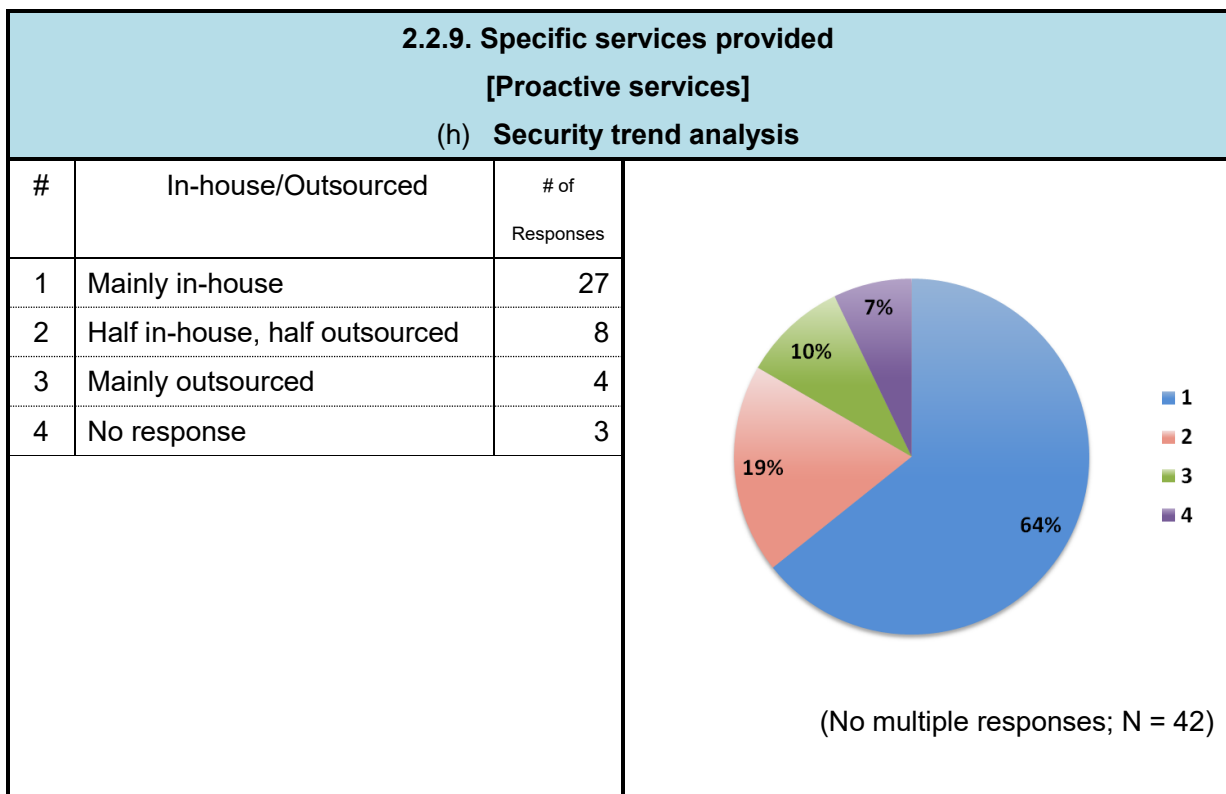
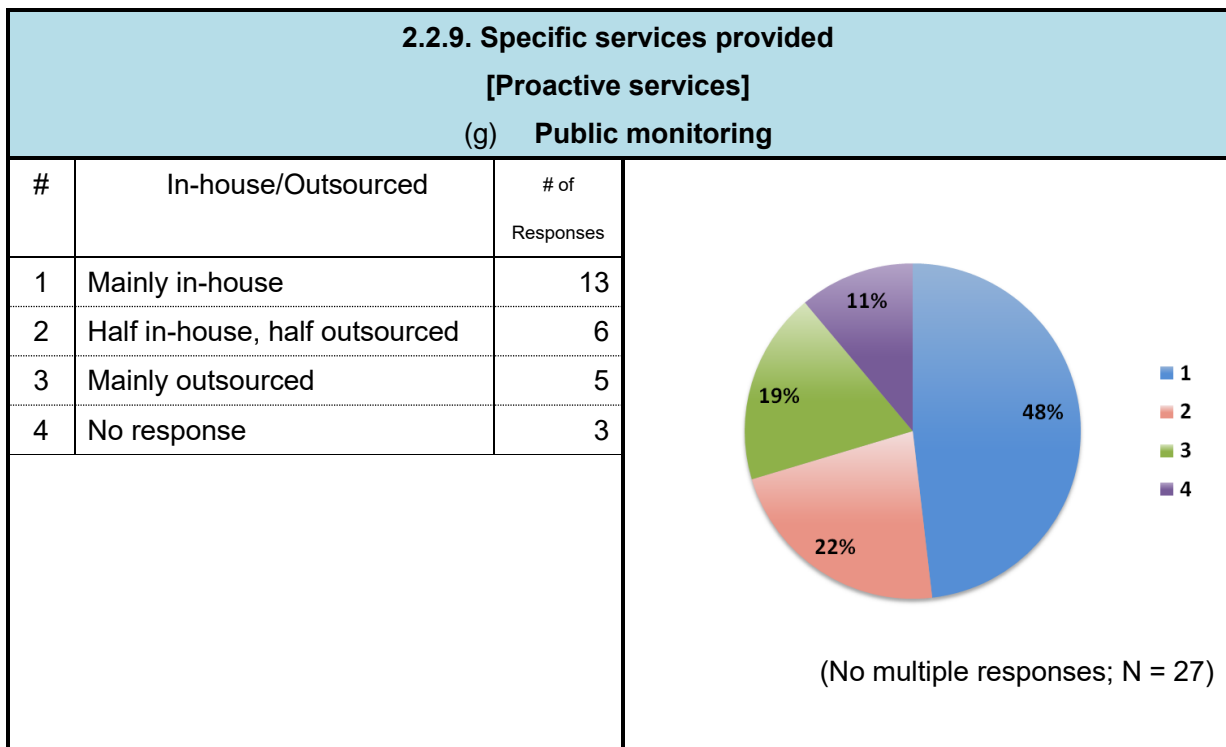
[Reactive services]

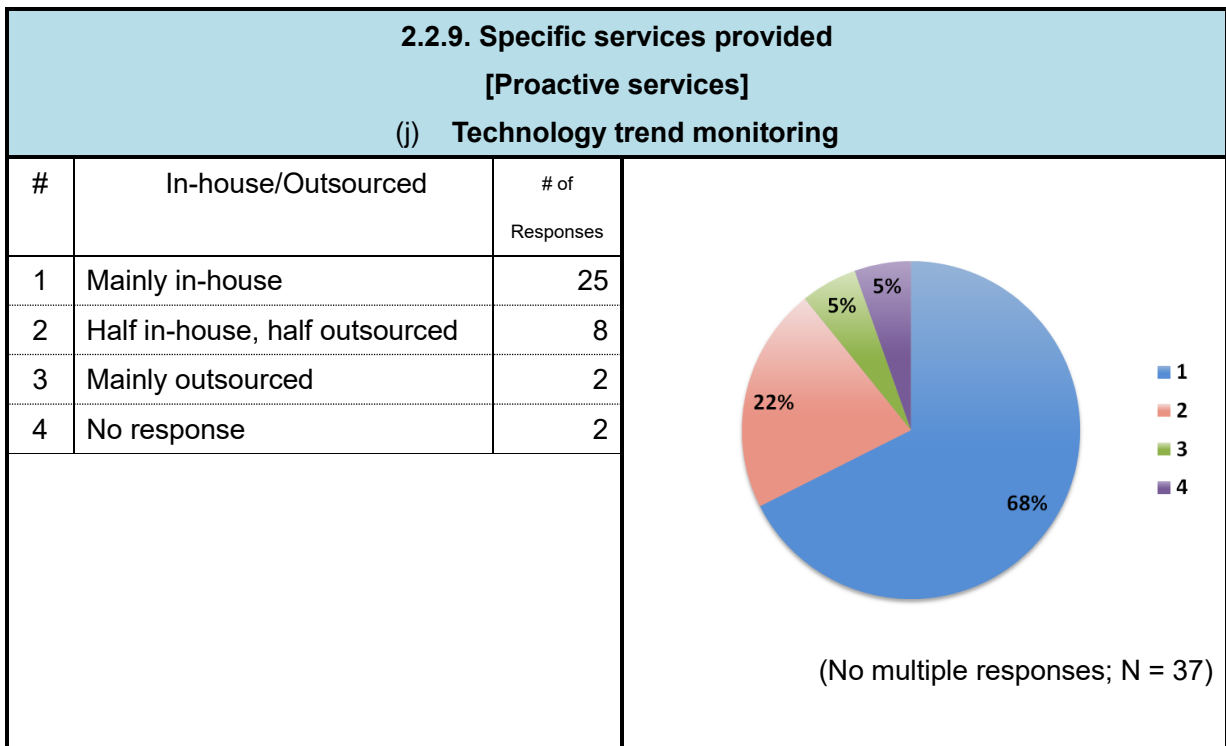
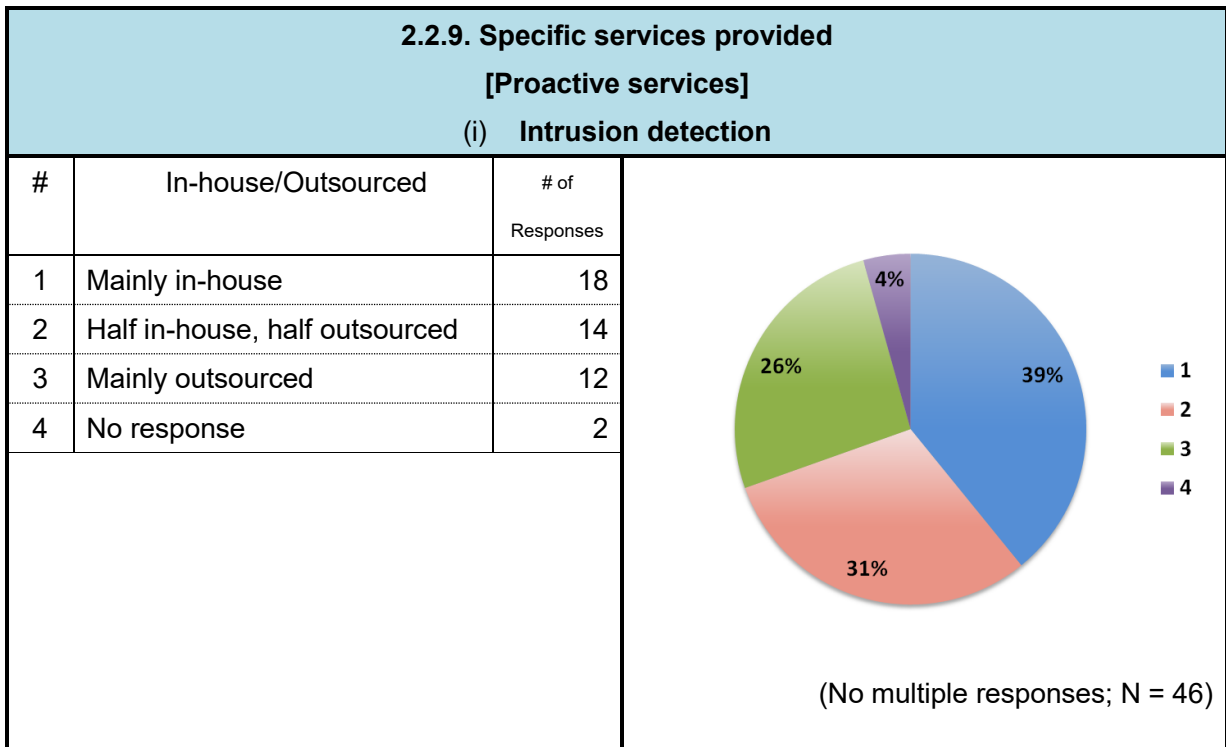


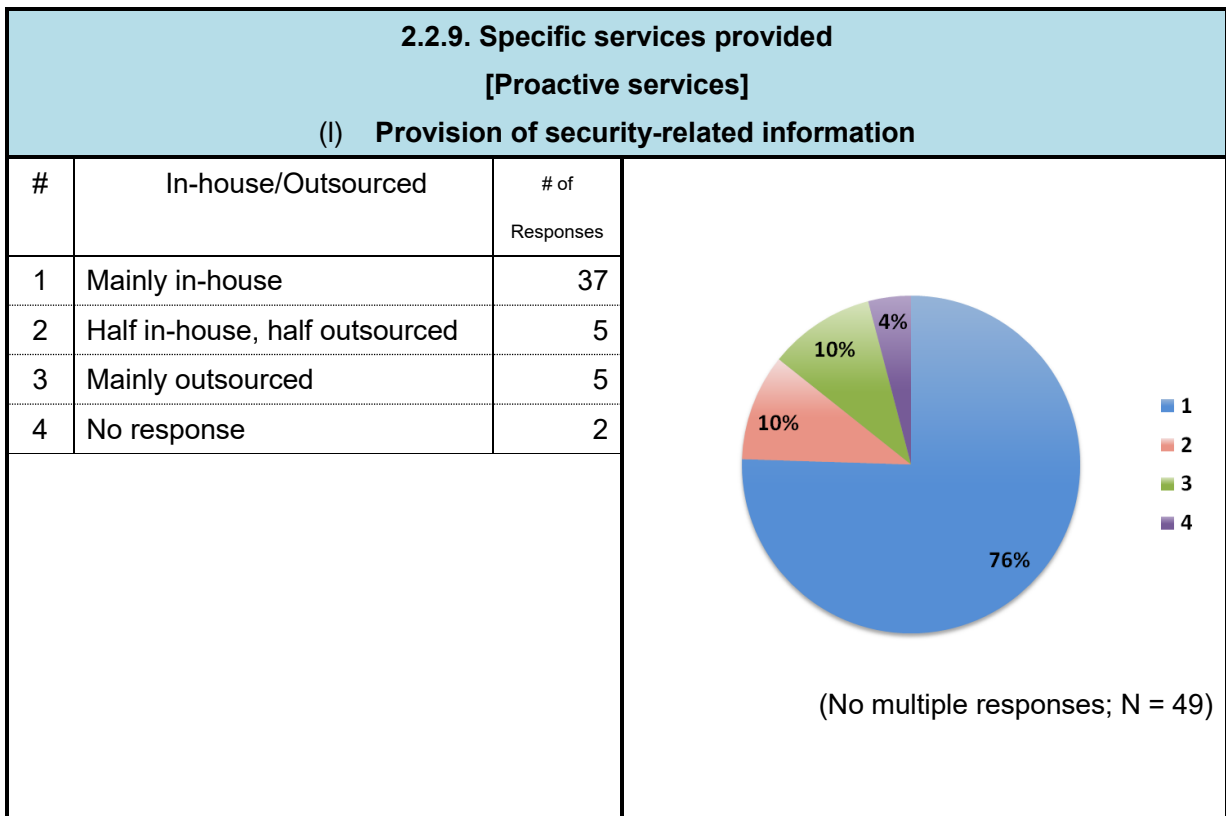
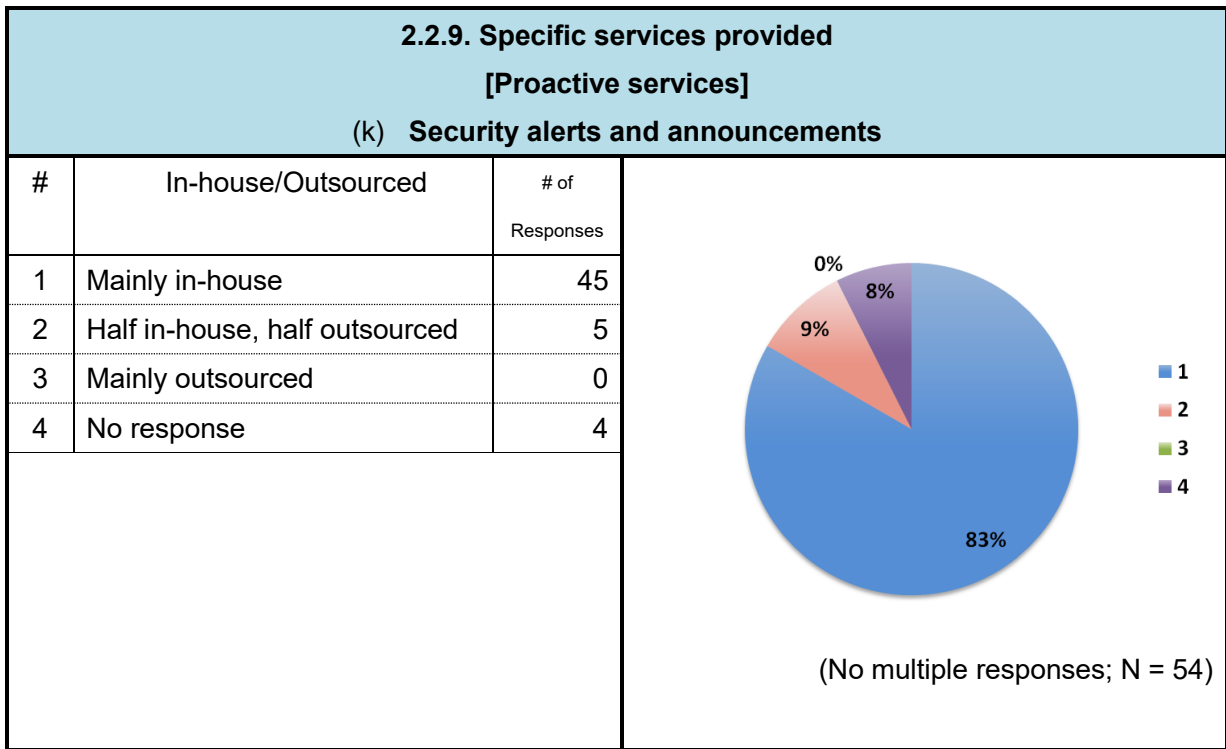


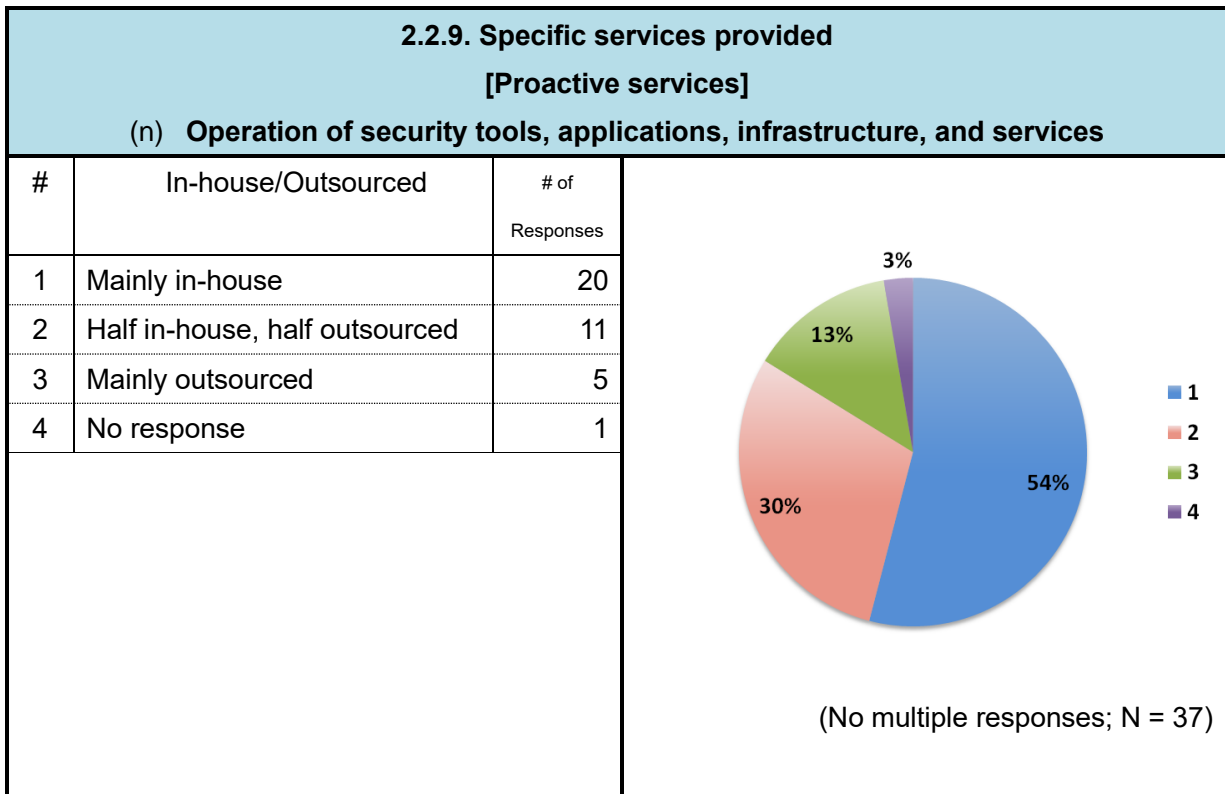
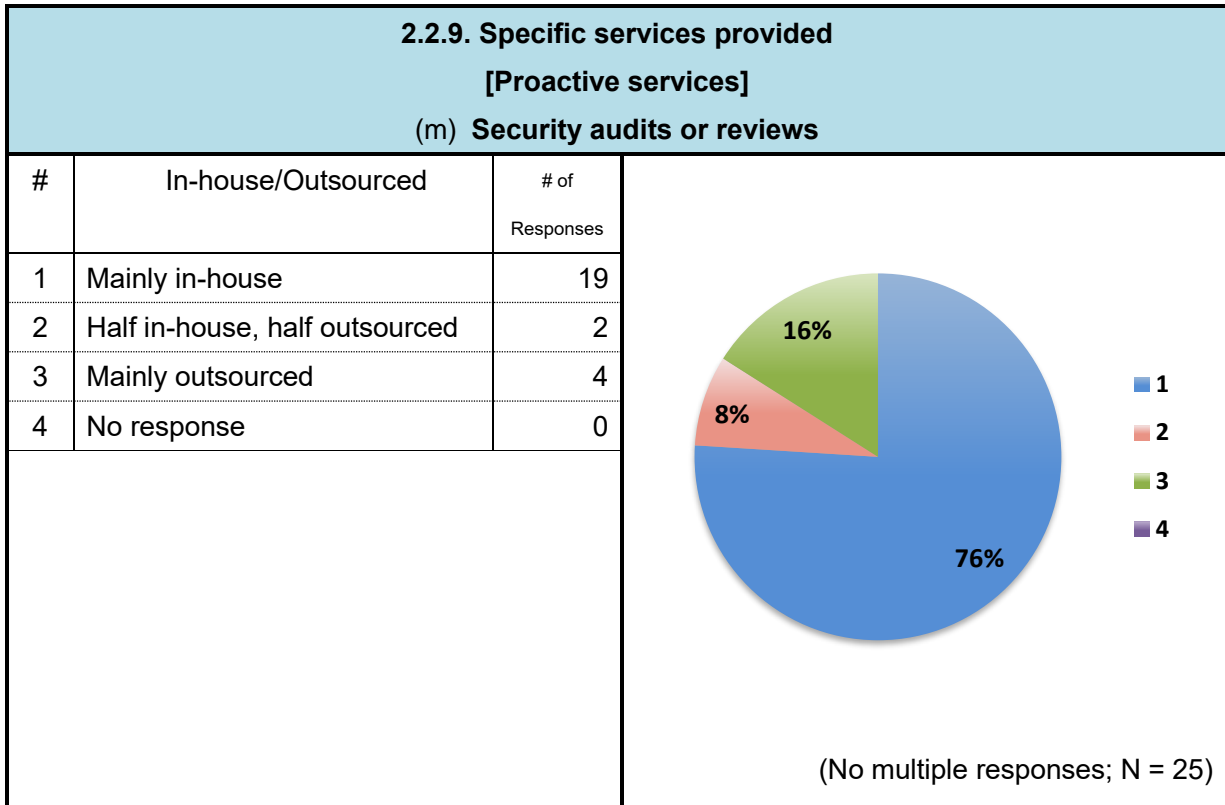


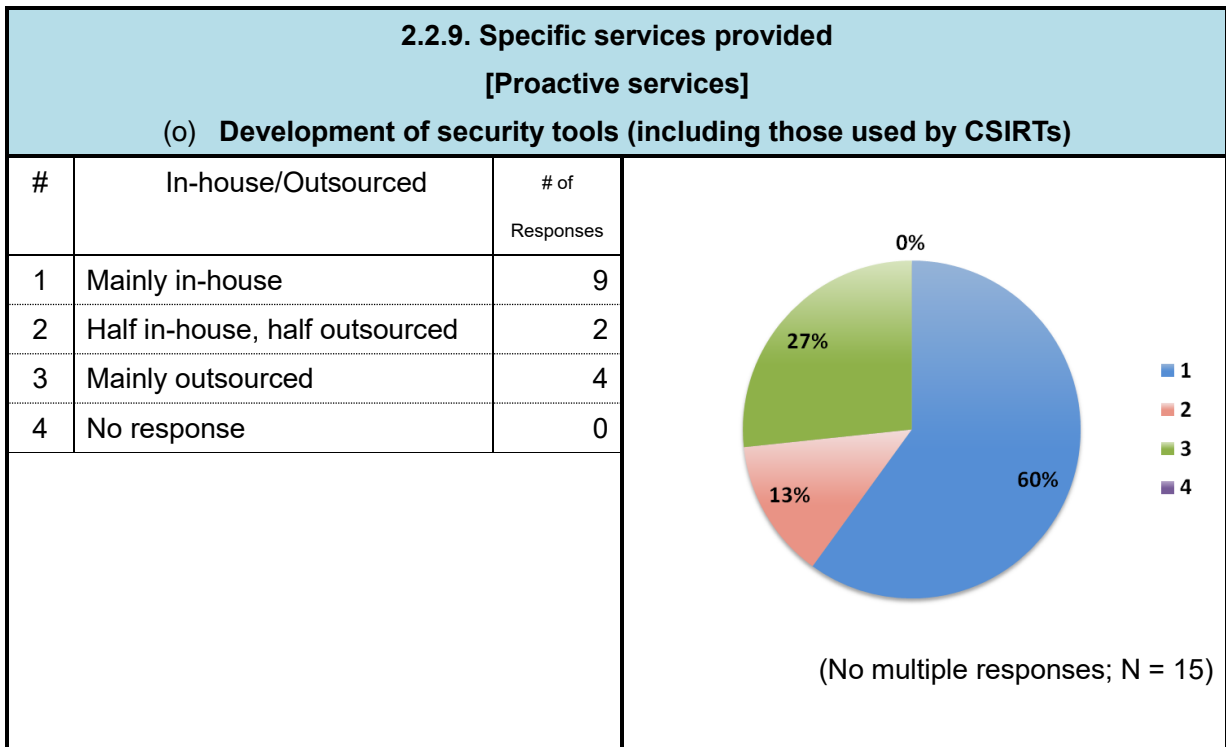
[Proactive services]



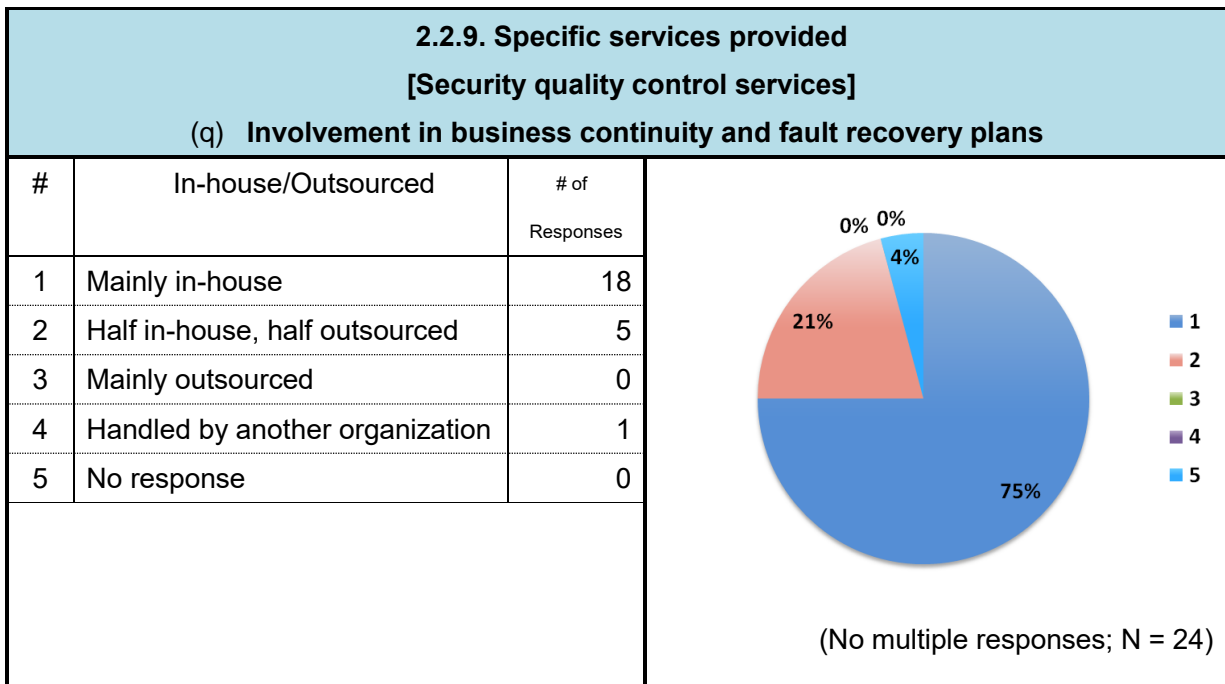
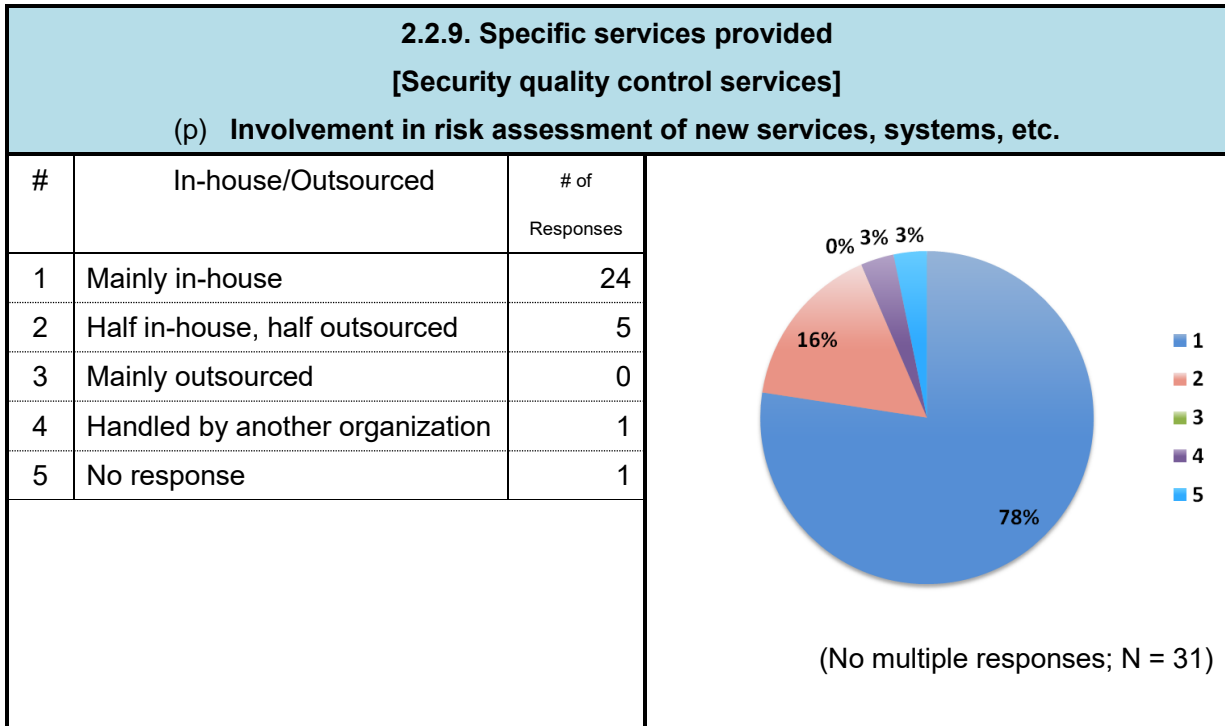


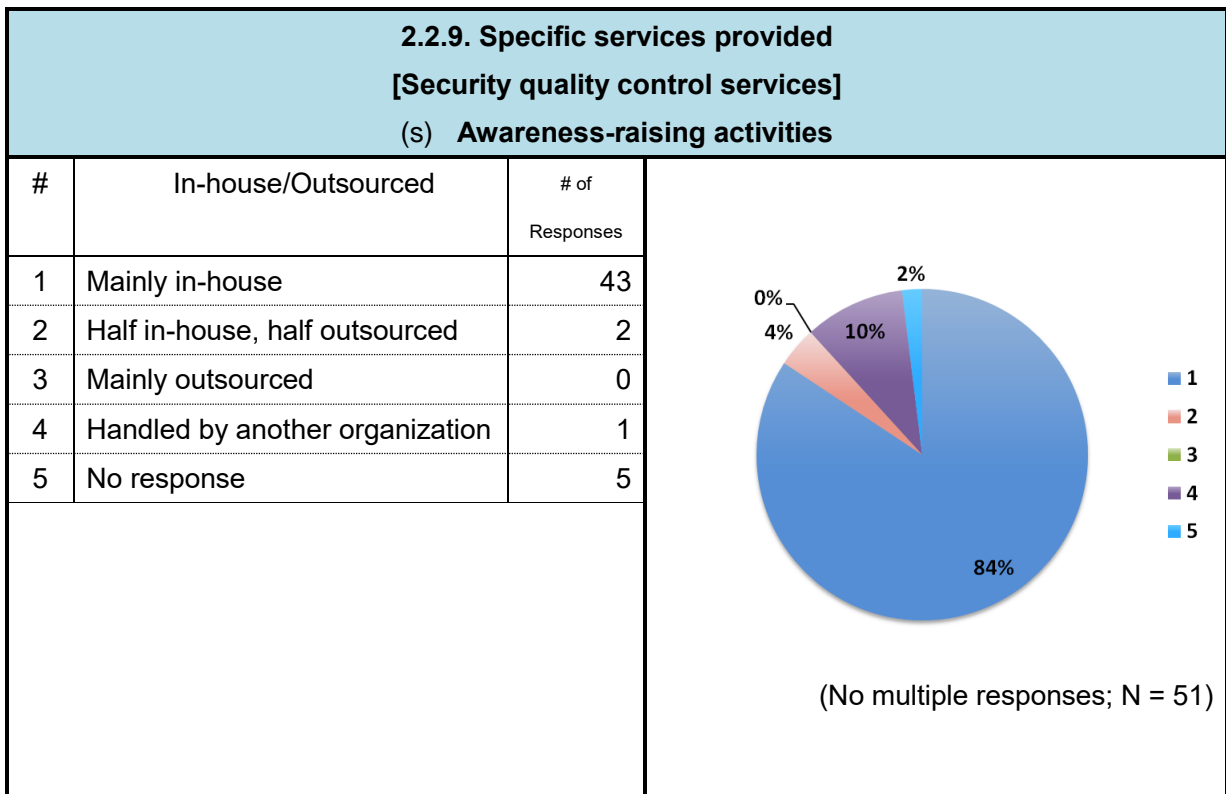
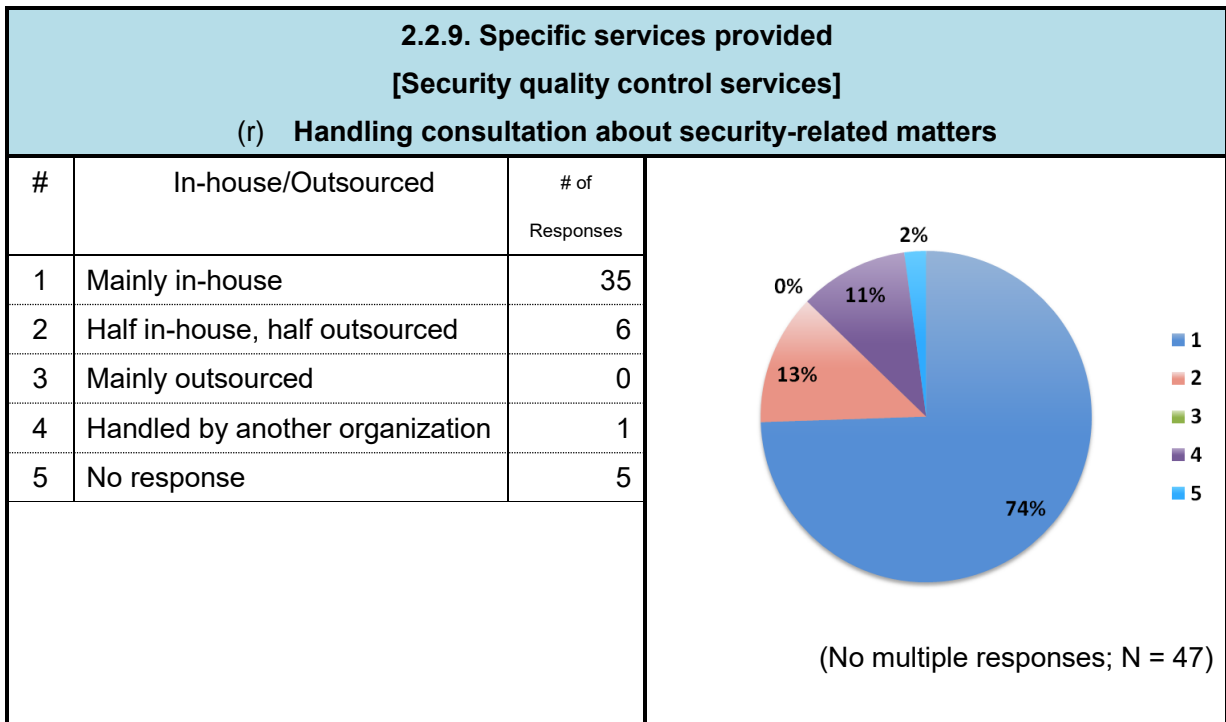


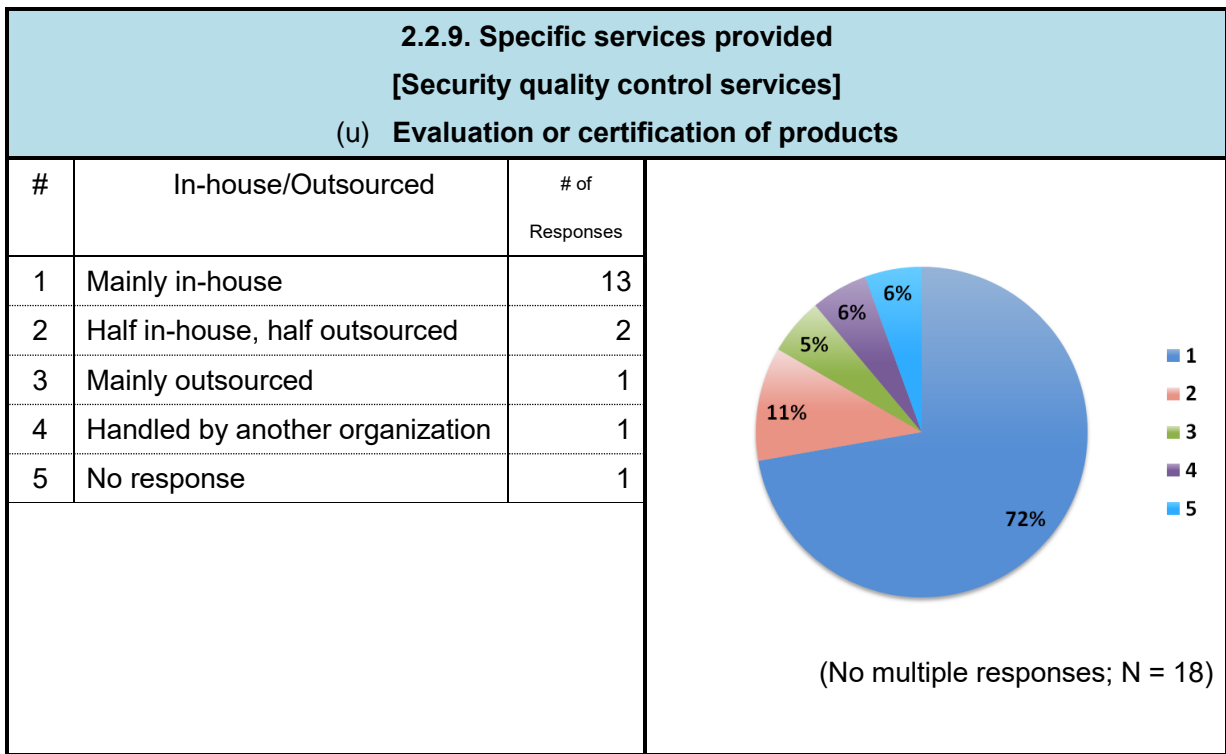
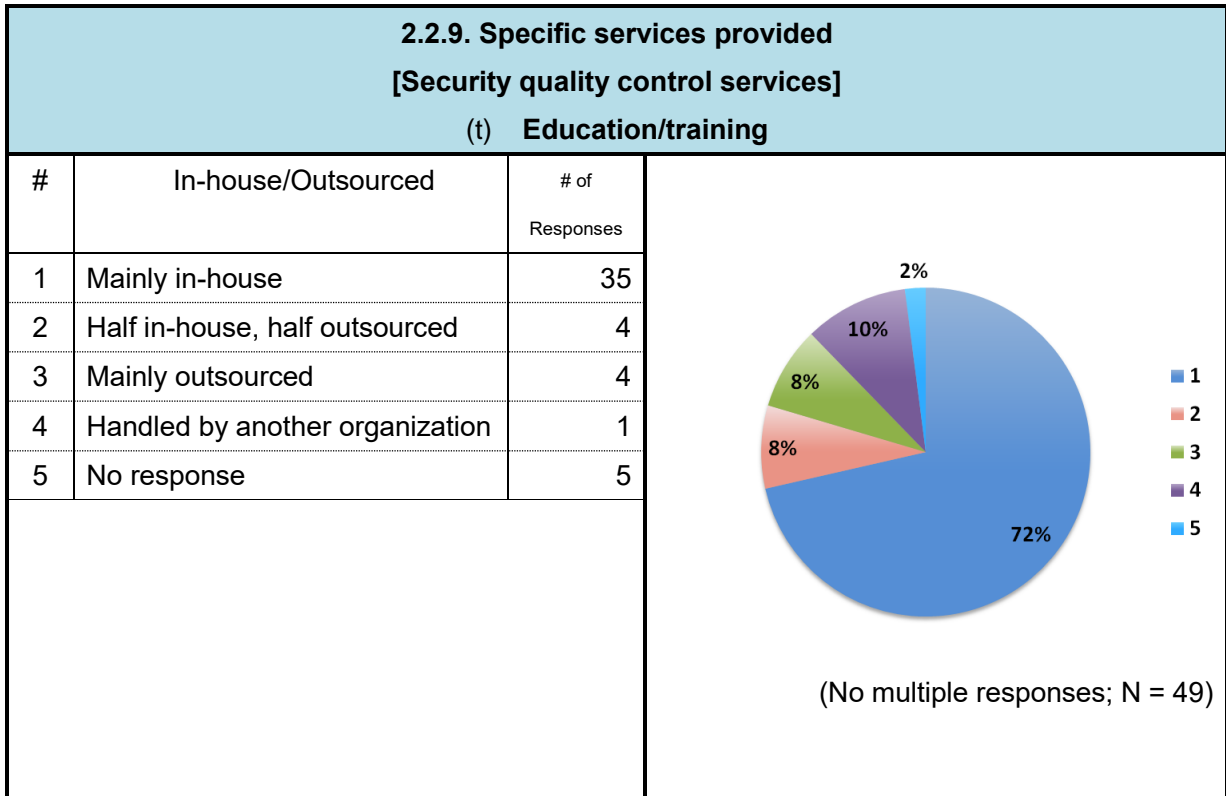


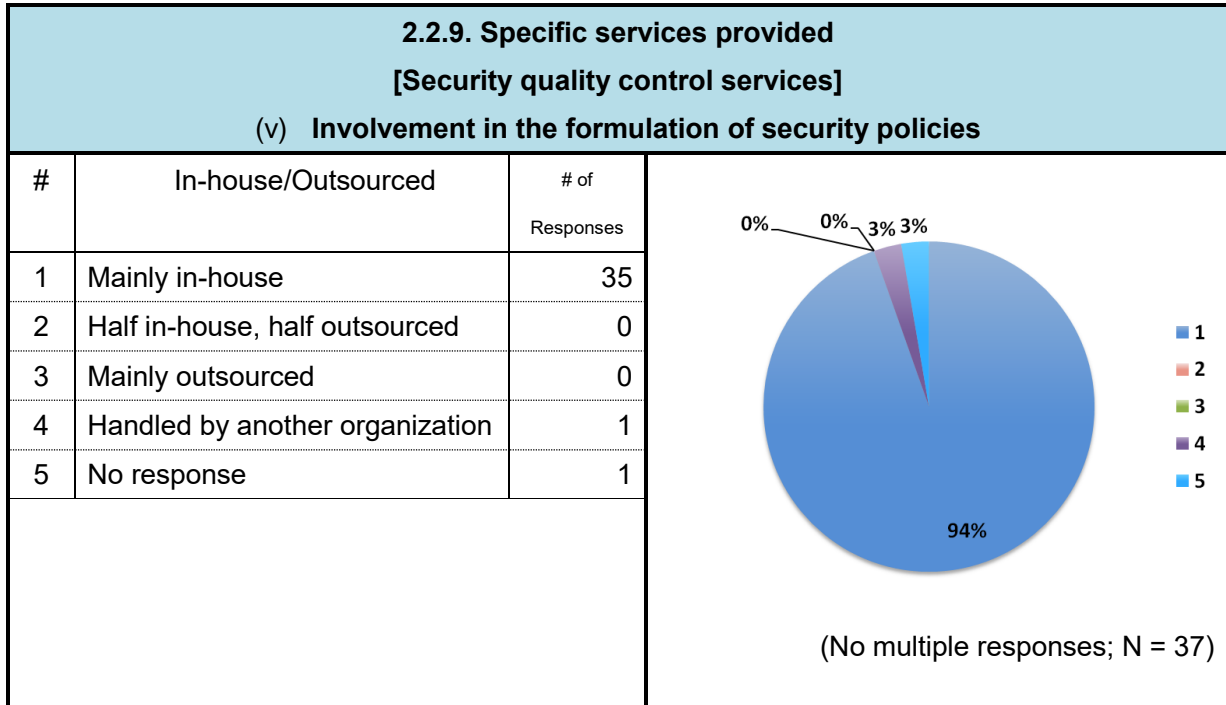


[Security quality control services]







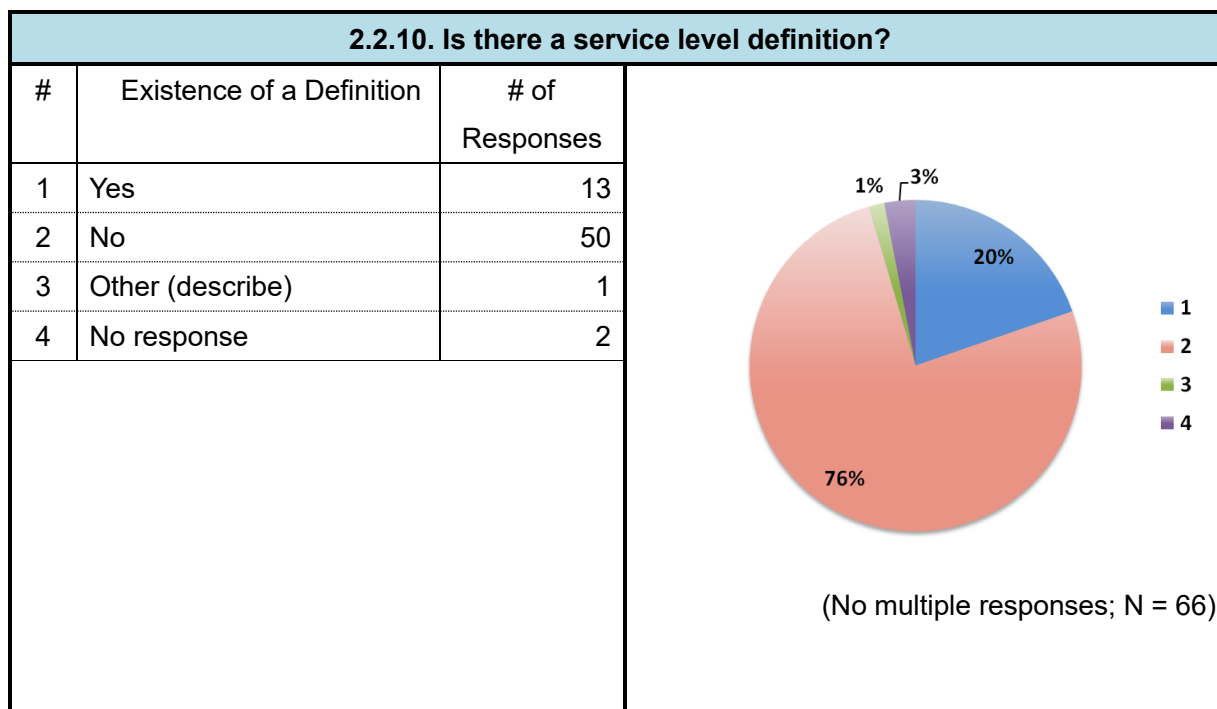


One organization listed "vulnerability diagnosis (mainly in-house)" as a services provided, other than reactive services, proactive services, and security quality control services.

2.2.9. Specific services provided [Other]		
(w) Other		
1	Vulnerability diagnosis (mainly in-house)	1

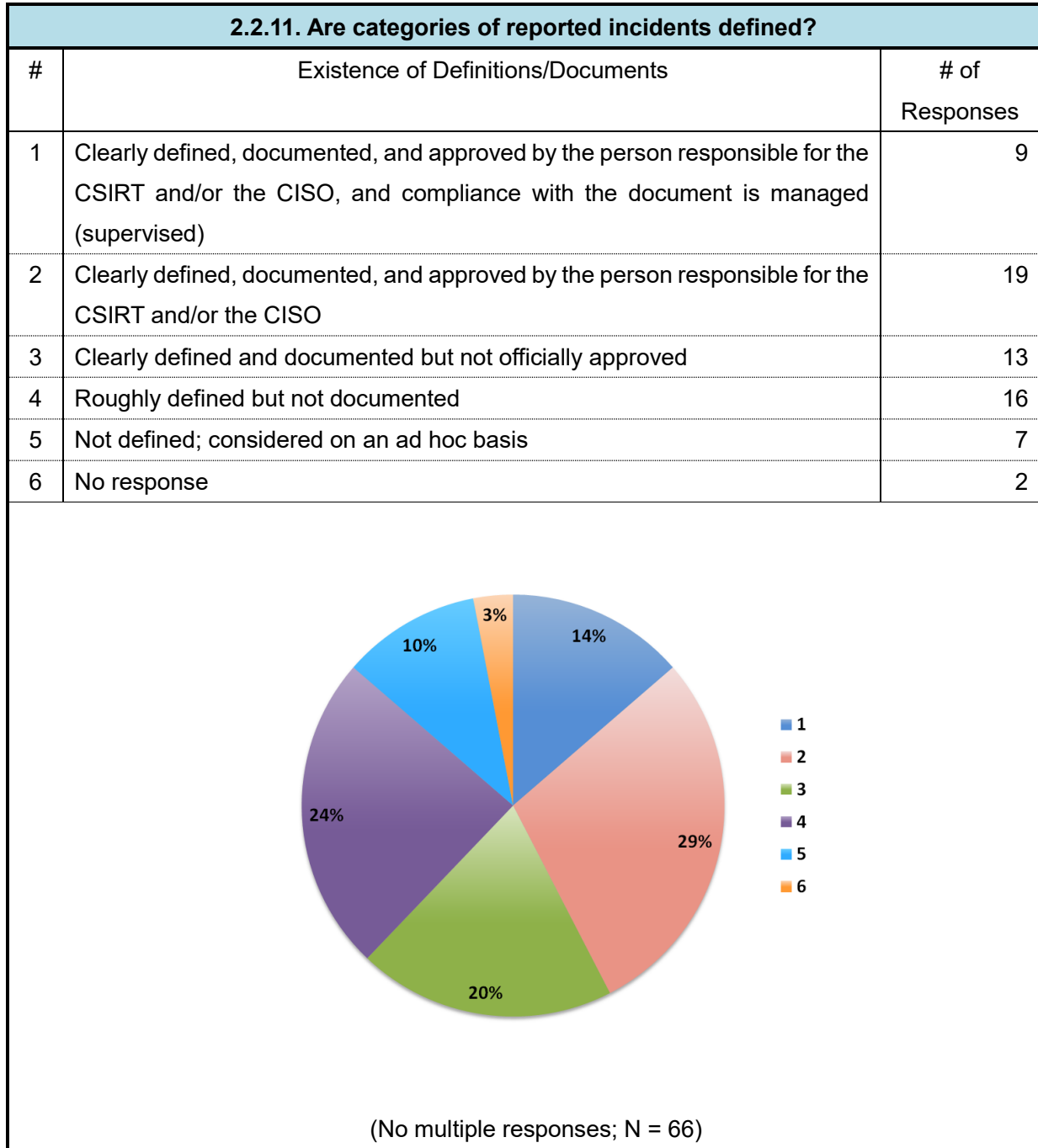
2.2.10. IS THERE A SERVICE LEVEL DEFINITION?

Many of the CSIRTs do not have a service level definition.



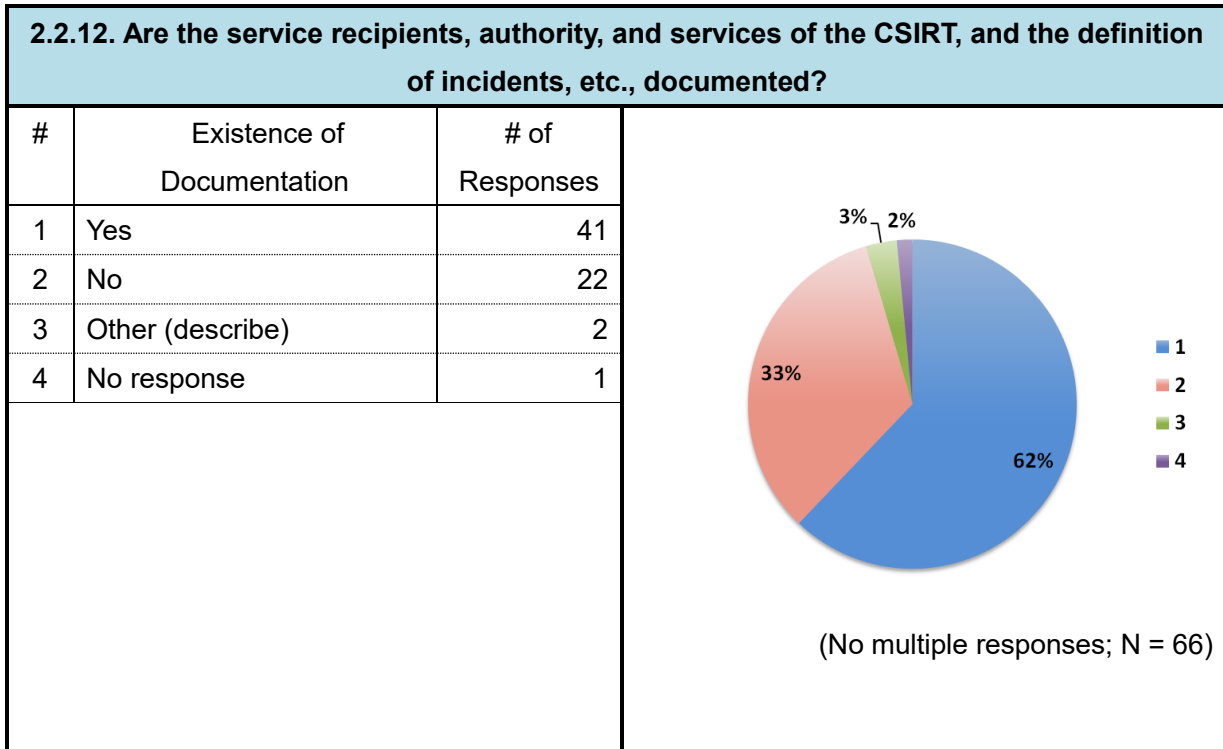
2.2.11. ARE CATEGORIES OF REPORTED INCIDENTS DEFINED?

While not necessarily documented, many of the organizations have pre-defined categories for reported incidents, and they respond to incidents according to each category.



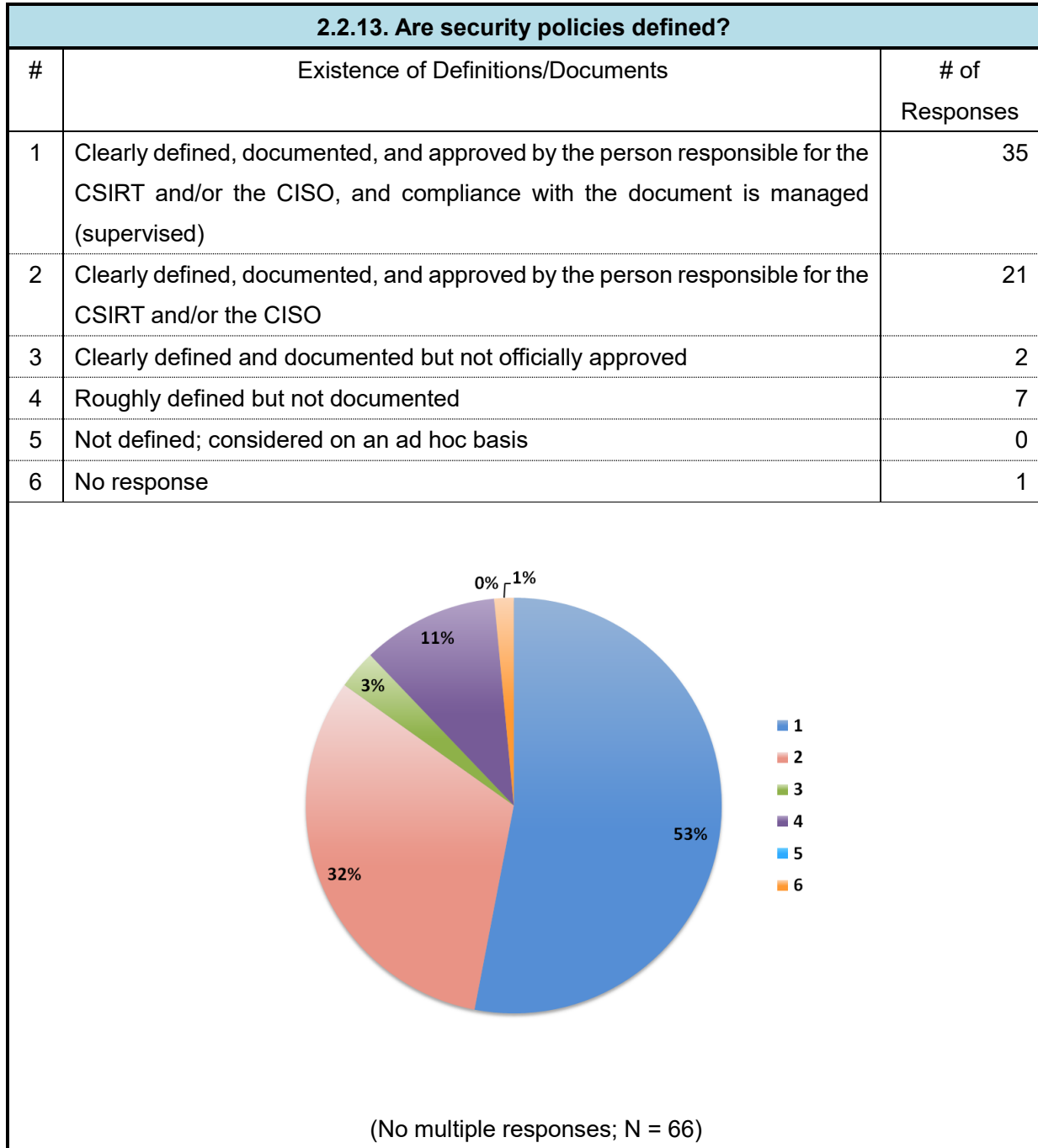
2.2.12. ARE THE SERVICE RECIPIENTS, AUTHORITY, AND SERVICES OF THE CSIRT, AND THE DEFINITION OF INCIDENTS, ETC., DOCUMENTED?

Many of the CSIRTs have documented definitions of roles and incidents, etc. Two respondents also said that they are currently working on documentation.



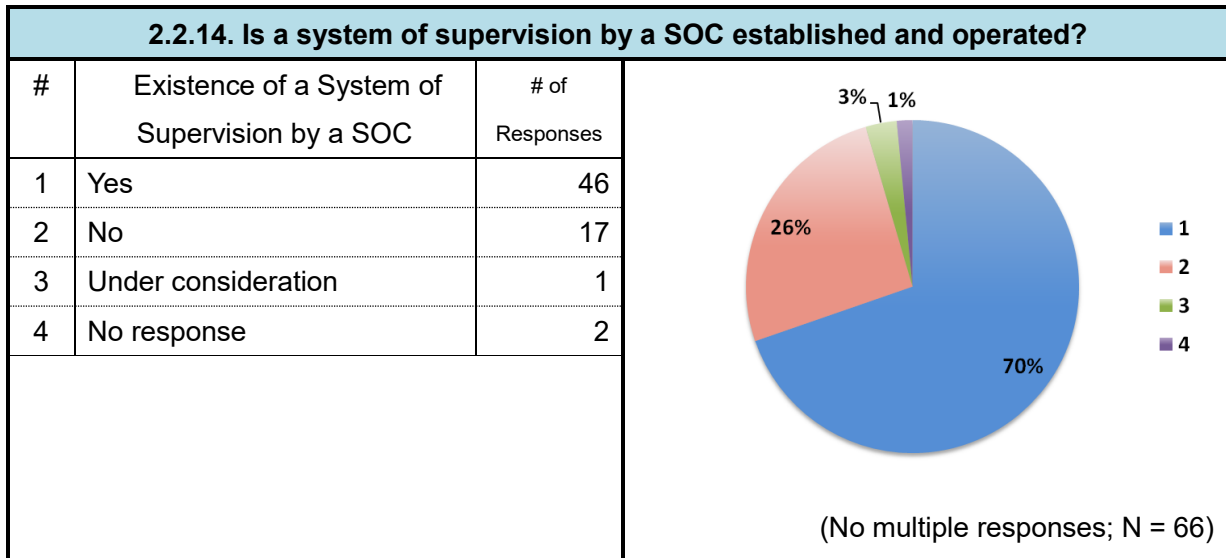
2.2.13. Are security policies defined?

Many of the organizations have documented security policies, which also indicates that their policies are standardized and operated.



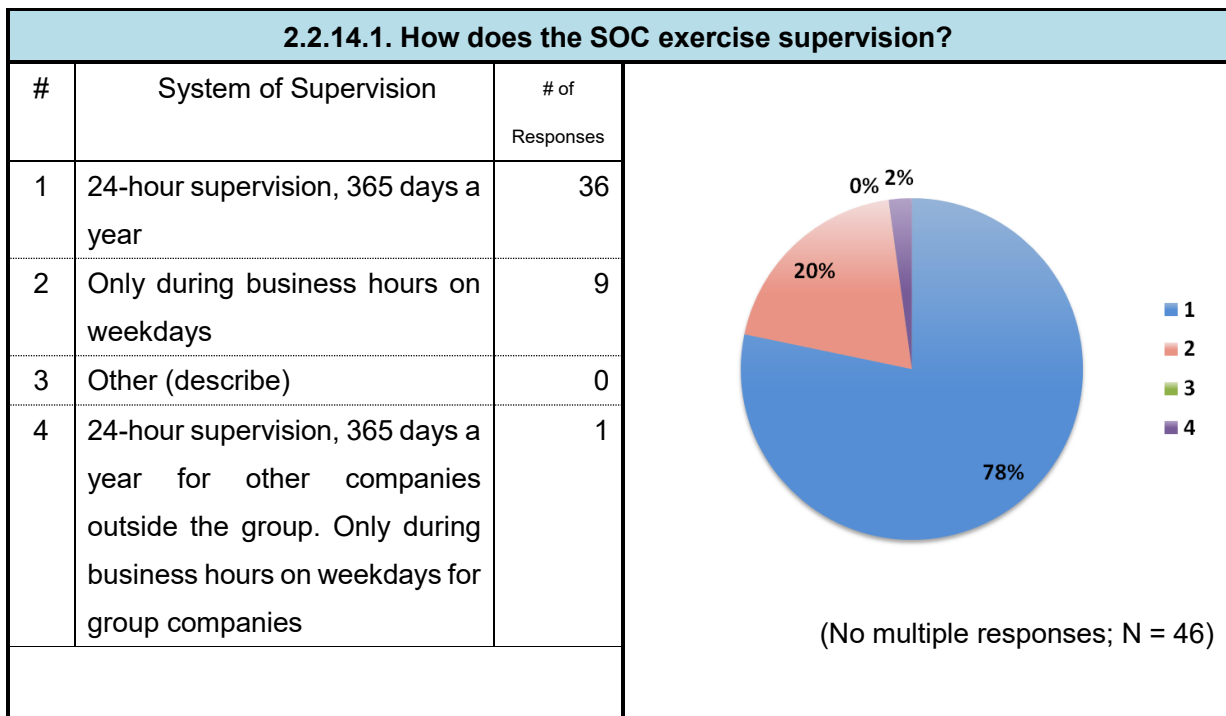
2.2.14. IS A SYSTEM OF SUPERVISION BY A SOC ESTABLISHED AND OPERATED?

Many of the organizations have a system of supervision by a SOC established and operated.



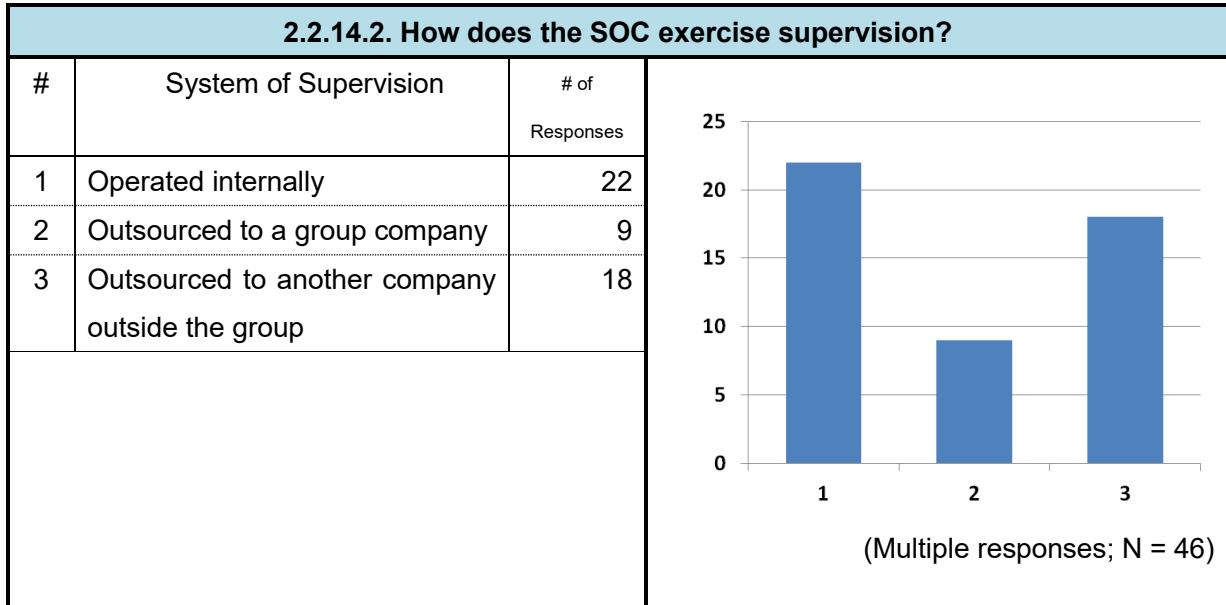
2.2.14.1. HOW DOES THE SOC EXERCISE SUPERVISION?

Most of the SOCs that are set up are operated 24 hours a day, 365 days a year.



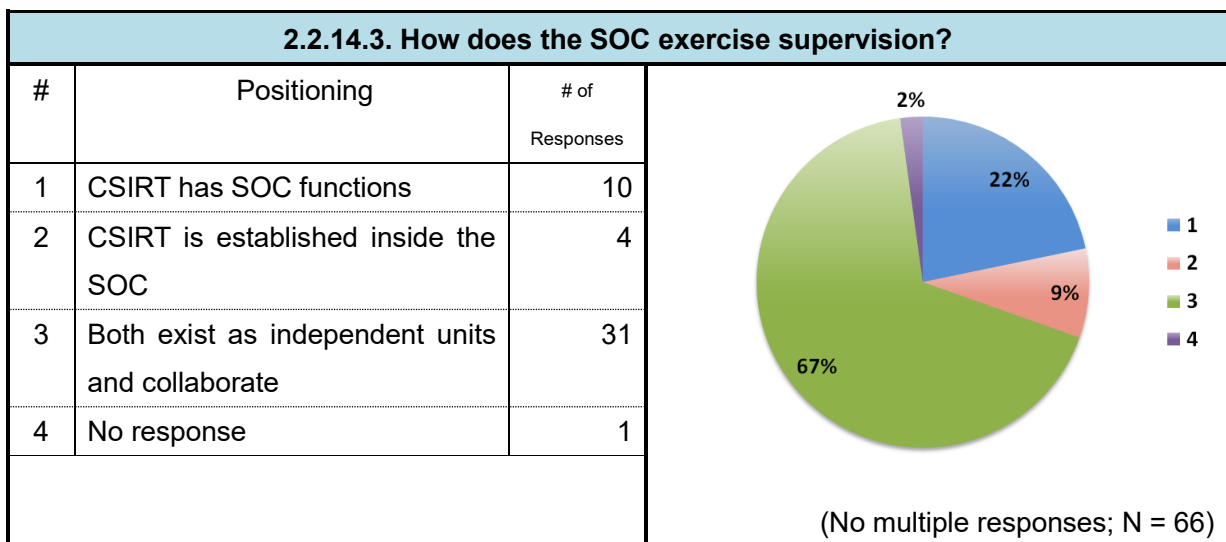
2.2.14.2. HOW IS THE SOC OPERATED?

Slightly fewer than half of the organizations with SOC's operate their centers internally, and the others outsource the operation to a group company or another company outside the group.



2.2.14.3. WHAT IS THE RELATIONSHIP BETWEEN THE SOC AND CSIRT?

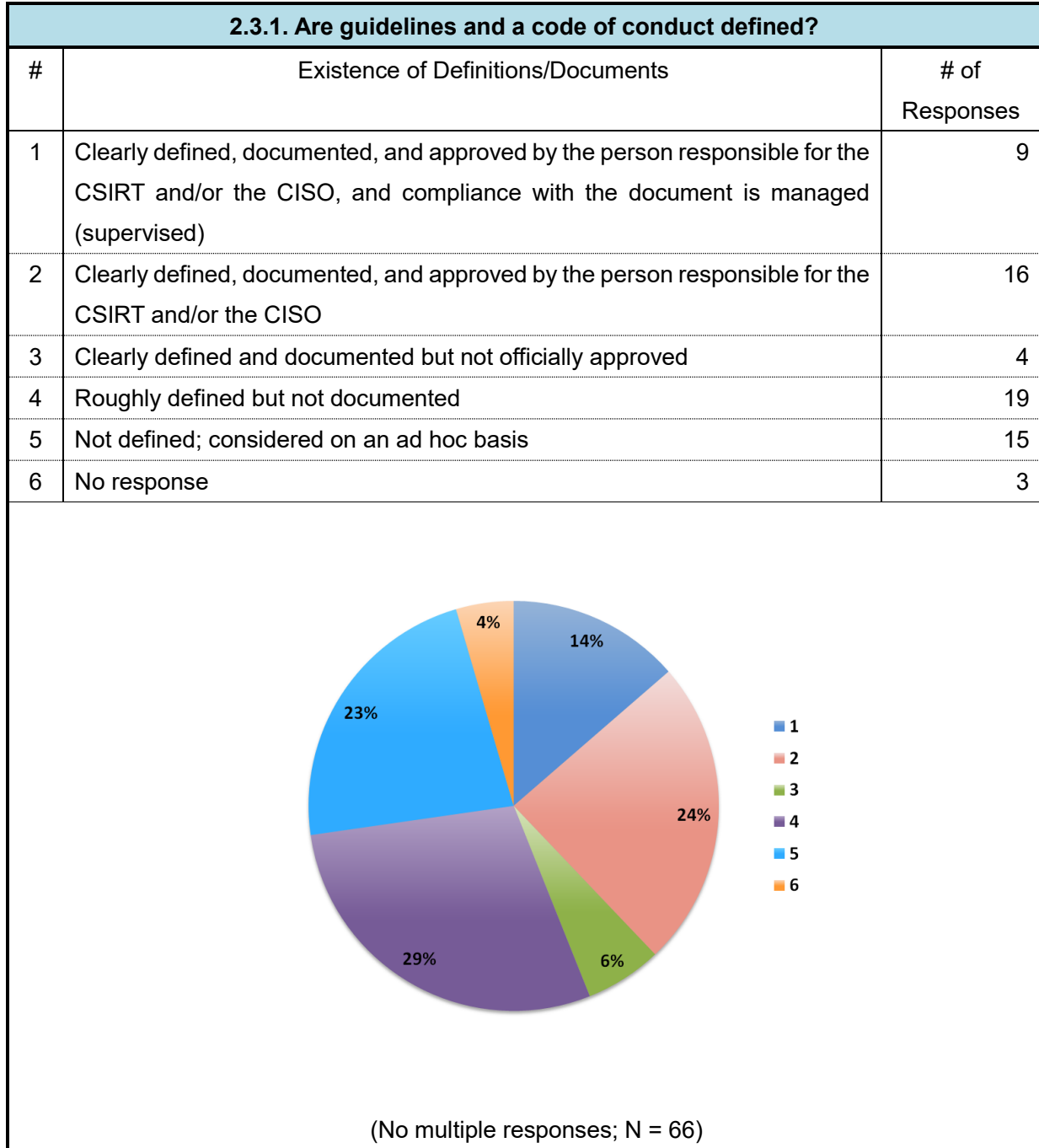
Many of the organizations operate the SOC and CSIRT separately.



2.3. CSIRT MEMBERS

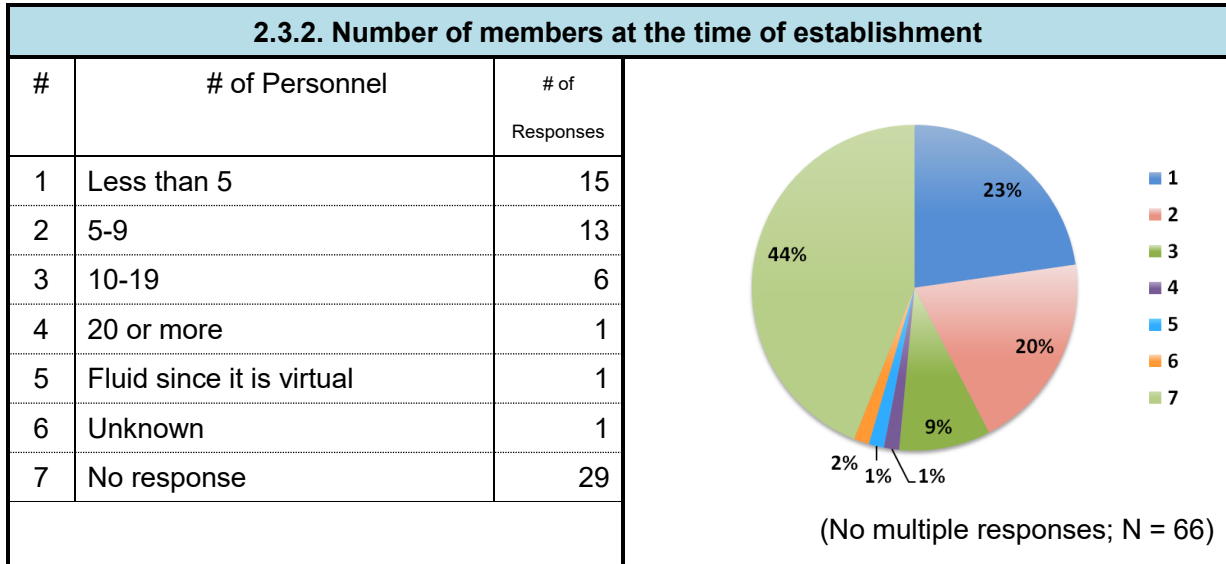
2.3.1. ARE GUIDELINES AND A CODE OF CONDUCT DEFINED?

Many of the CSIRTs have defined guidelines and a code of conduct for their members, though not necessarily clearly documented.



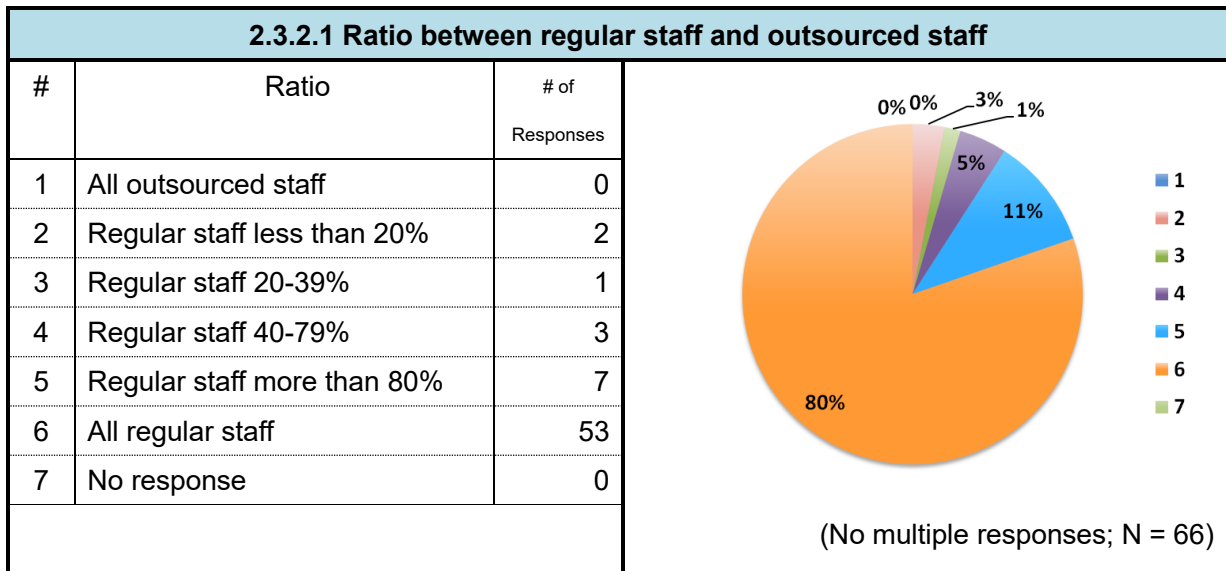
2.3.2. NUMBER OF MEMBERS AT THE TIME OF ESTABLISHMENT

Most of the CSIRTs had less than 5 members at the time of establishment, with more than half saying they had less than 10, excluding blank responses.



2.3.2.1. RATIO BETWEEN REGULAR STAFF AND OUTSOURCED STAFF

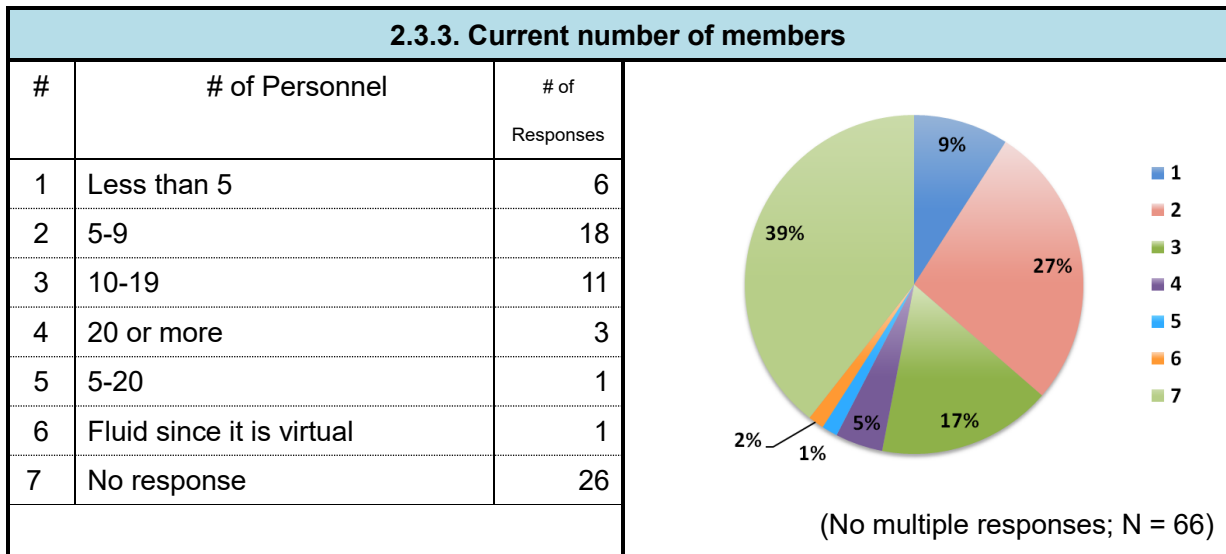
As for the ratio between regular staff and outsourced staff, many of the organizations used only their regular staff as founding members of their CSIRT. None of the organizations use only outsource staff.



2.3.3. CURRENT NUMBER OF MEMBERS

As for the current number of members, most of the CSIRTs have 5-9 members, and almost all of them have

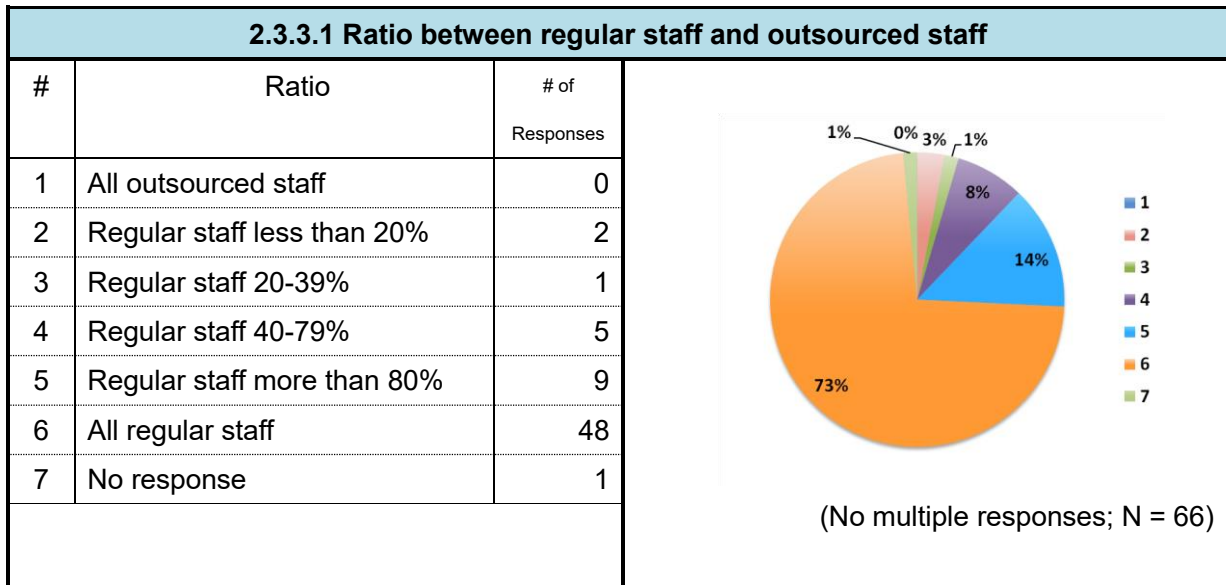
less than 20.



2.3.3.1. RATIO BETWEEN REGULAR STAFF AND OUTSOURCED STAFF

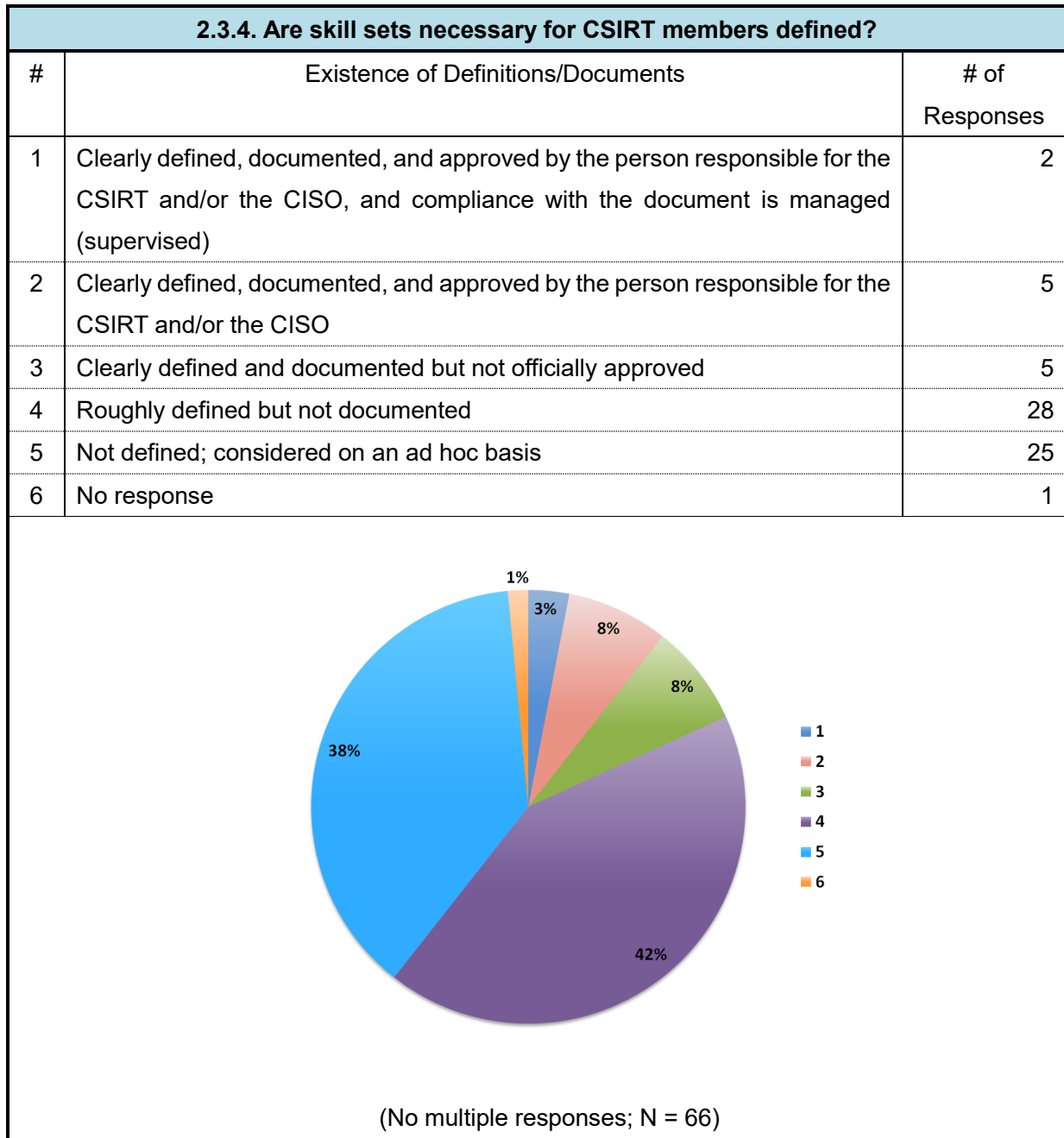
Many of the organizations use only their regular staff as their current CSIRT members

None of the organizations use only outsource staff.



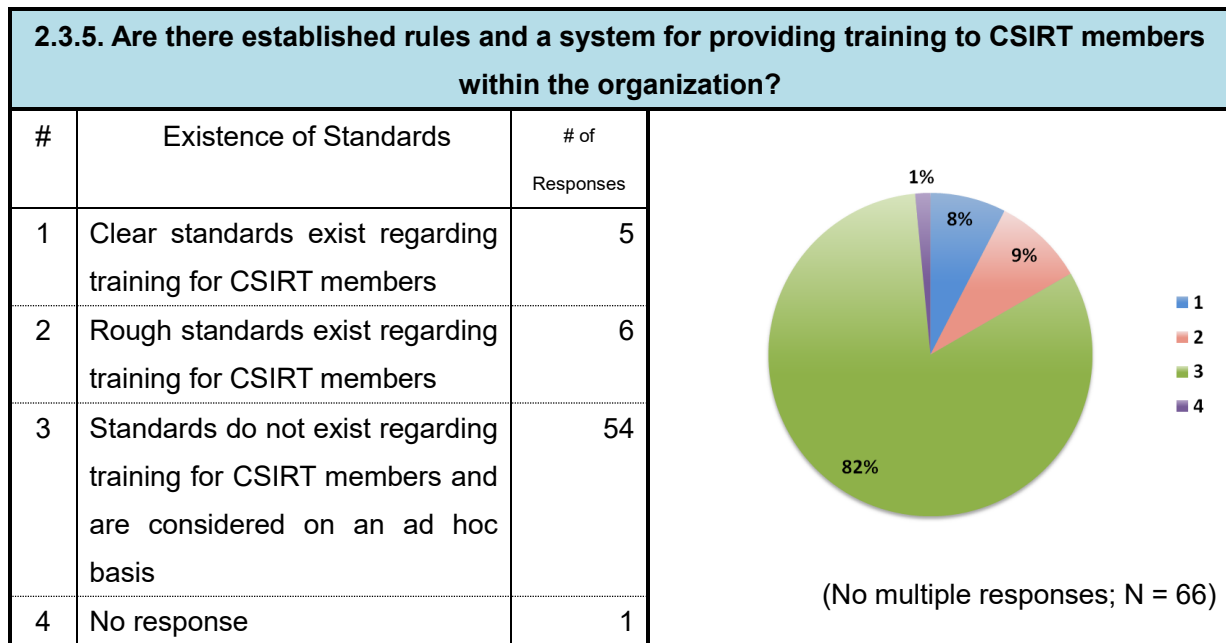
2.3.4. ARE SKILL SETS NECESSARY FOR CSIRT MEMBERS DEFINED?

Only a few of the organizations define skill sets necessary for CSIRT members, while many roughly set skill levels or determine required skill sets on an ad hoc basis.



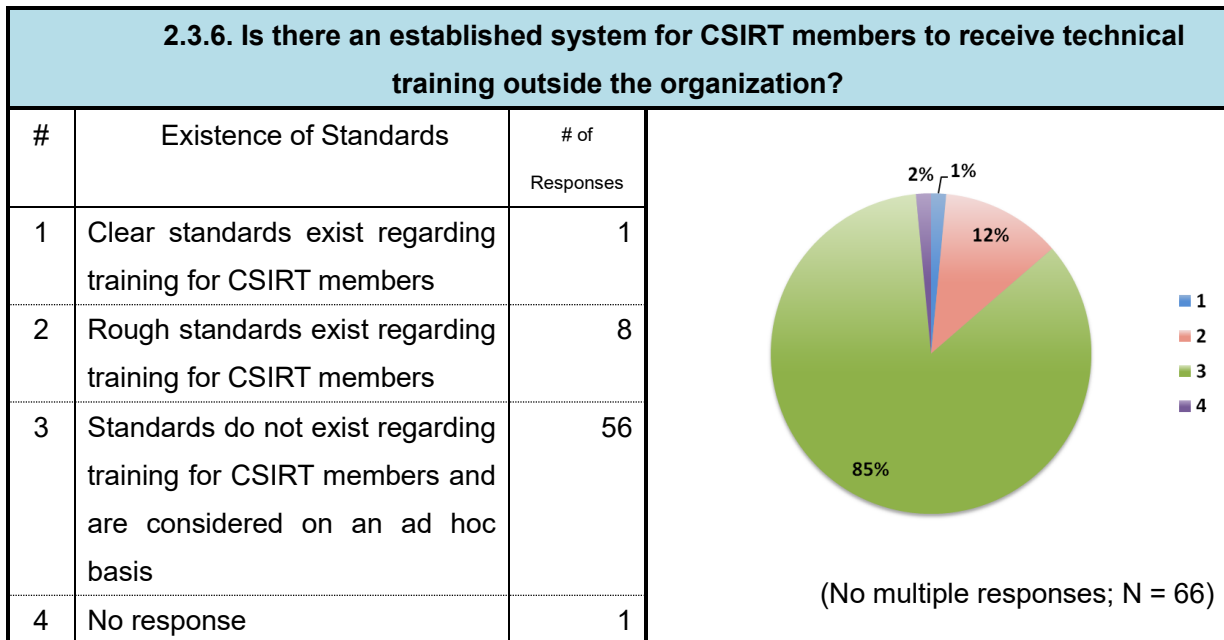
2.3.5. ARE THERE ESTABLISHED RULES AND A SYSTEM FOR PROVIDING TRAINING TO CSIRT MEMBERS WITHIN THE ORGANIZATION?

Overall, only a few of the organizations clearly prescribe internal training that CSIRT members should participate in, and most organizations determine which members should participate in which training on an ad hoc basis.



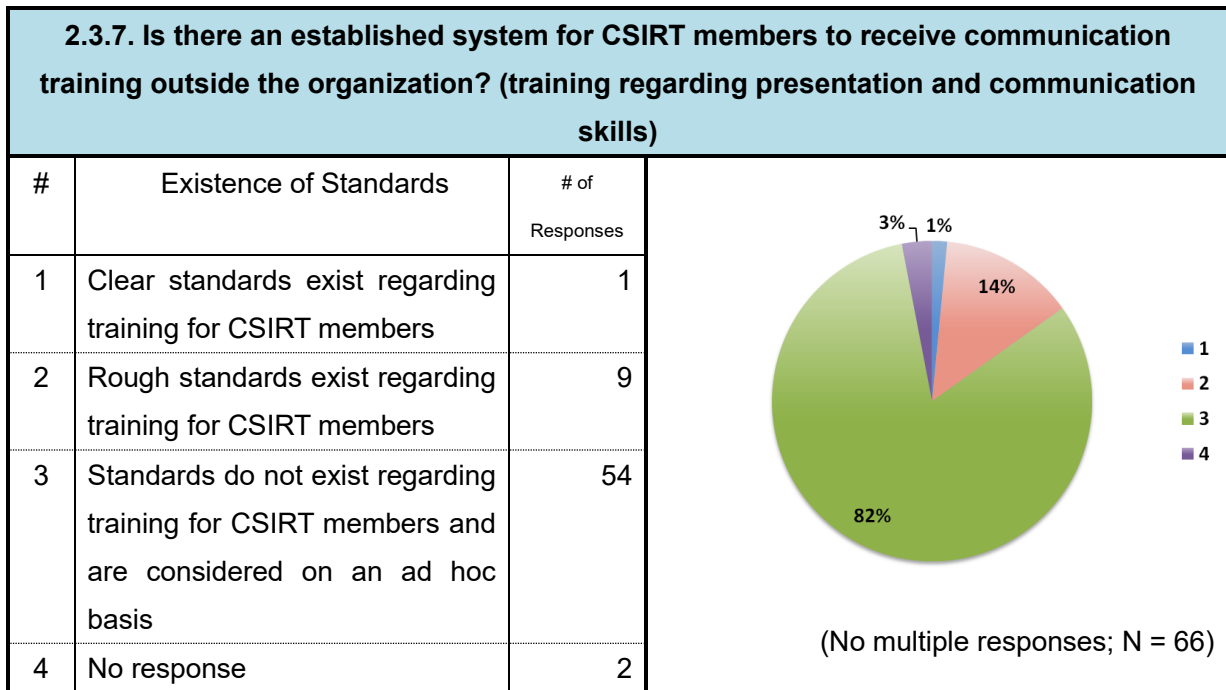
2.3.6. IS THERE AN ESTABLISHED SYSTEM FOR CSIRT MEMBERS TO RECEIVE TECHNICAL TRAINING OUTSIDE THE ORGANIZATION?

Only a few of the organizations clearly prescribe external training that CSIRT members should participate in. Most of the organizations determine participation in external training on an ad hoc basis.



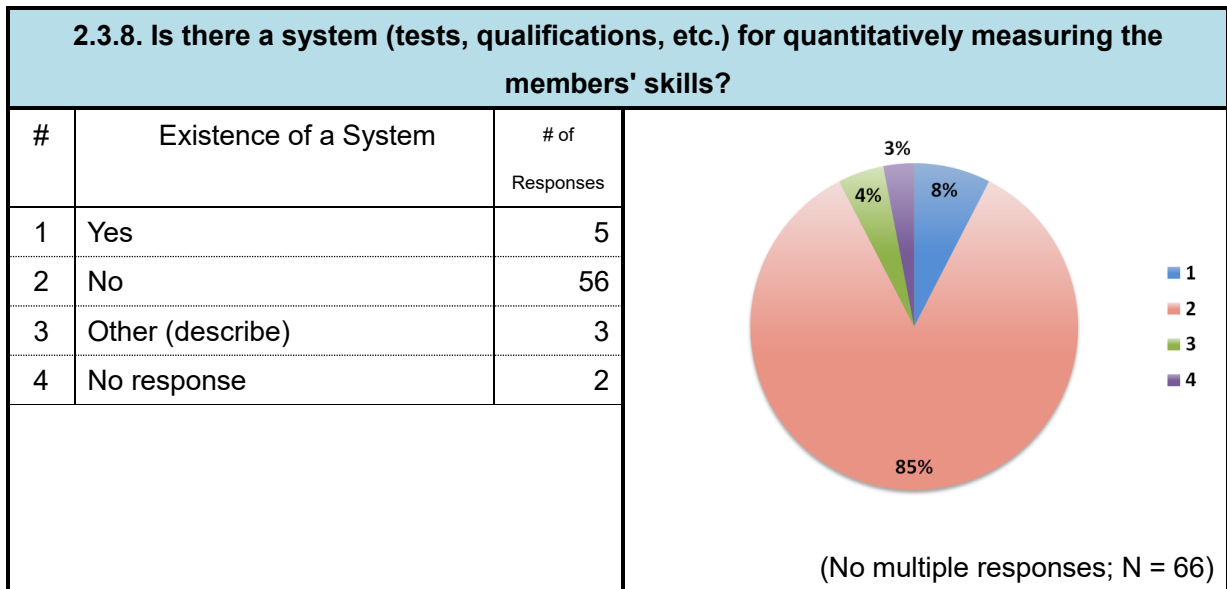
2.3.7. IS THERE AN ESTABLISHED SYSTEM FOR CSIRT MEMBERS TO RECEIVE COMMUNICATION TRAINING OUTSIDE THE ORGANIZATION? (TRAINING REGARDING PRESENTATION AND COMMUNICATION SKILLS)

Only a few of the CSIRTs have clear rules. Decisions are made on an ad hoc basis.



2.3.8. IS THERE A SYSTEM (TESTS, QUALIFICATIONS, ETC.) FOR QUANTITATIVELY MEASURING THE MEMBERS' SKILLS?

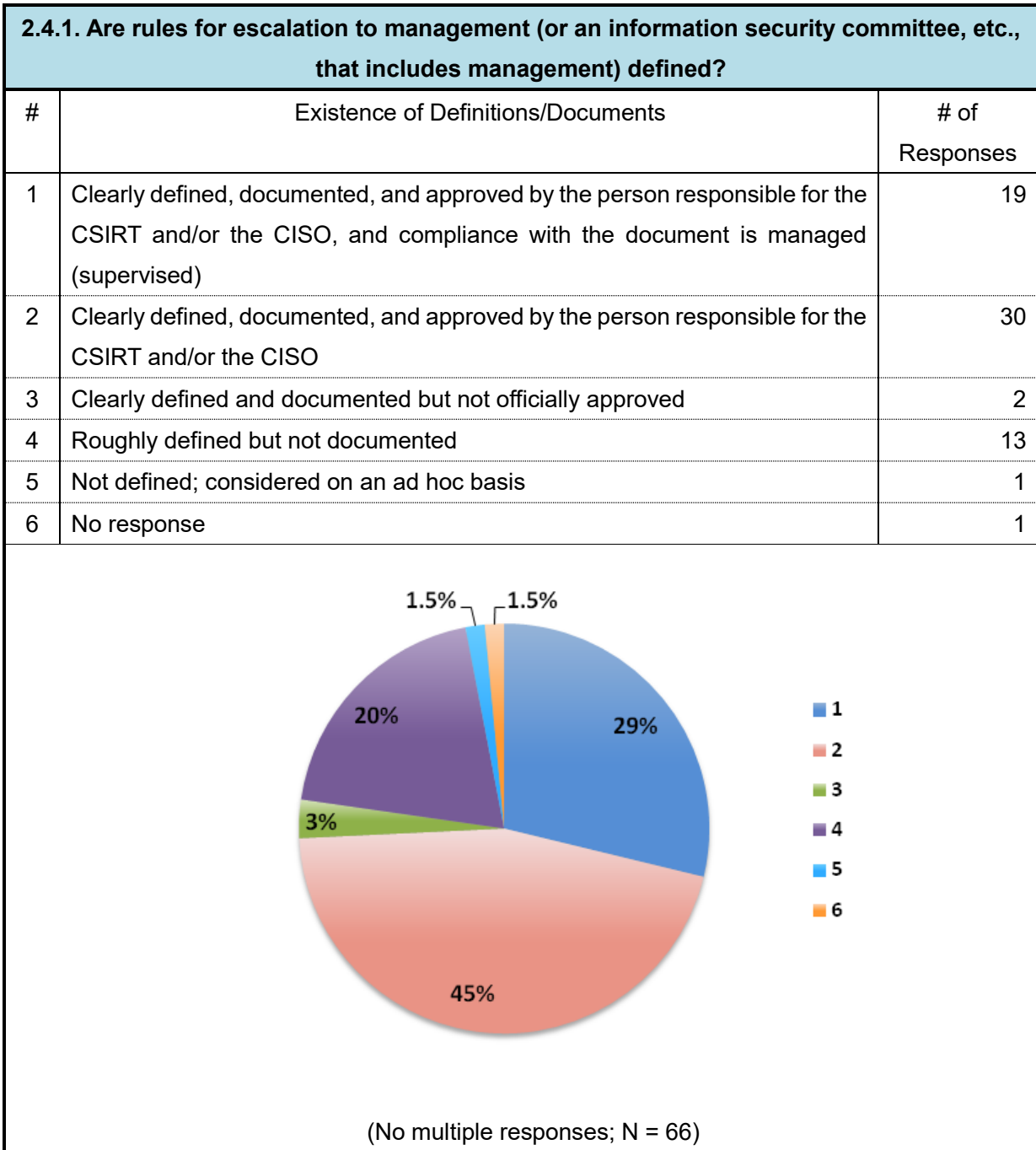
Only a few of the organizations have a system for quantitatively measuring the skills of CSIRT members. One organization gave "external qualification (CISM, etc.)" for its response.



2.4. PROCESSES AND RULES

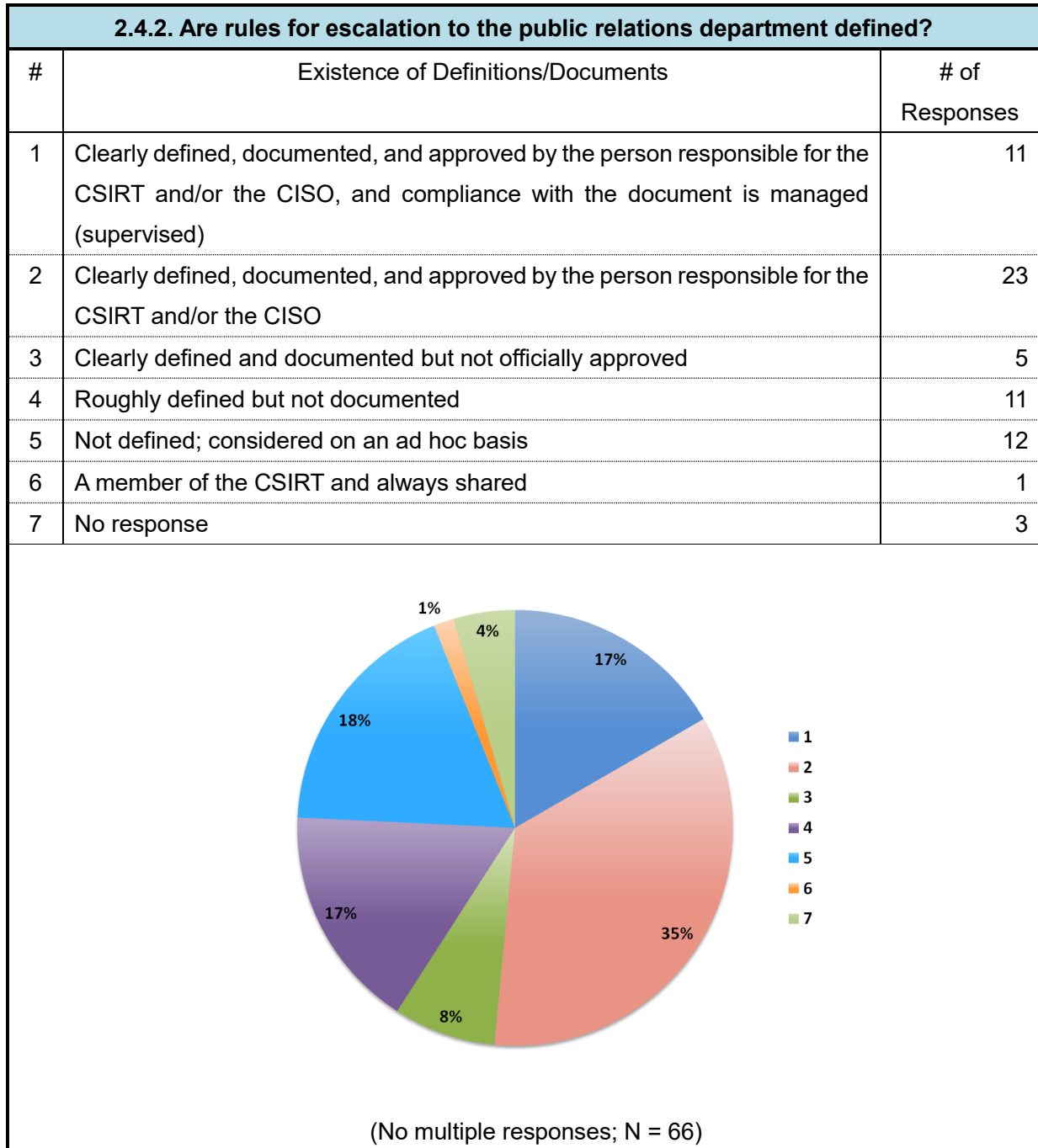
2.4.1. ARE RULES FOR ESCALATION TO MANAGEMENT (OR AN INFORMATION SECURITY COMMITTEE, ETC., THAT INCLUDES MANAGEMENT) DEFINED?

Many of the organizations have clearly defined and documented rules for escalation to management.



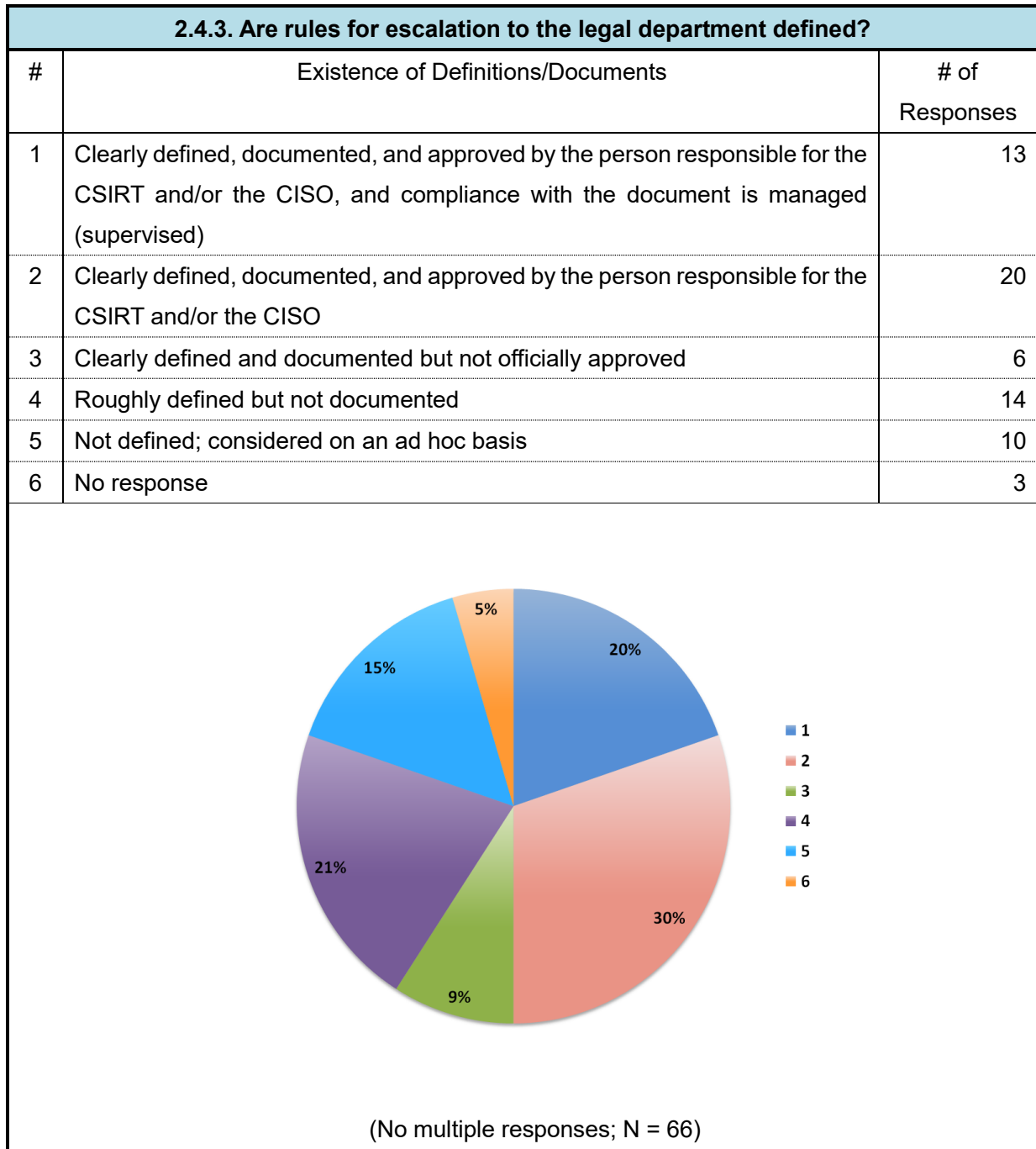
2.4.2. ARE RULES FOR ESCALATION TO THE PUBLIC RELATIONS DEPARTMENT DEFINED?

Many of the organizations have clearly defined and documented rules for escalation to the public relations department.



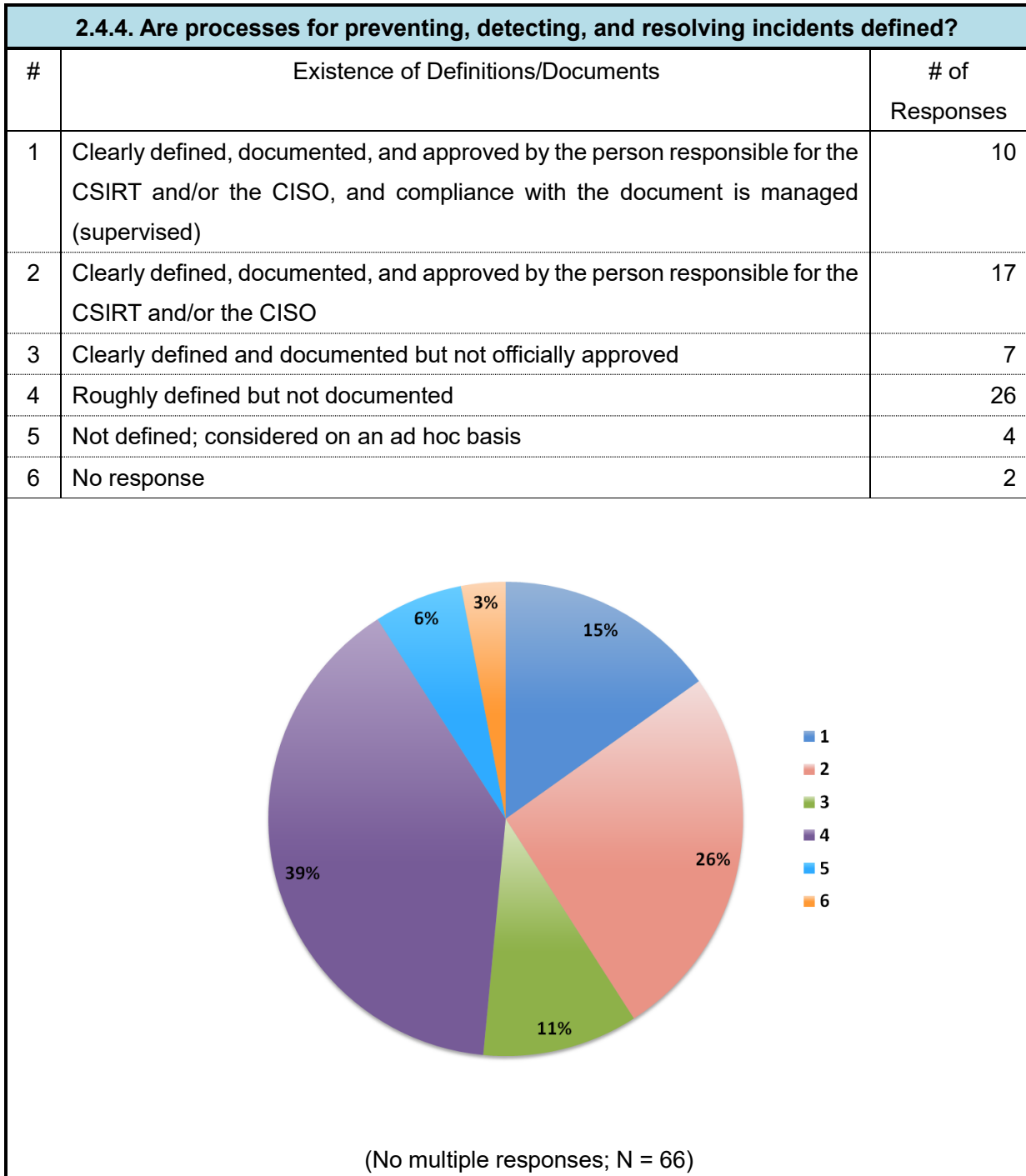
2.4.3. ARE RULES FOR ESCALATION TO THE LEGAL DEPARTMENT DEFINED?

Many of the organizations have clearly defined and documented rules for escalation to the legal department.



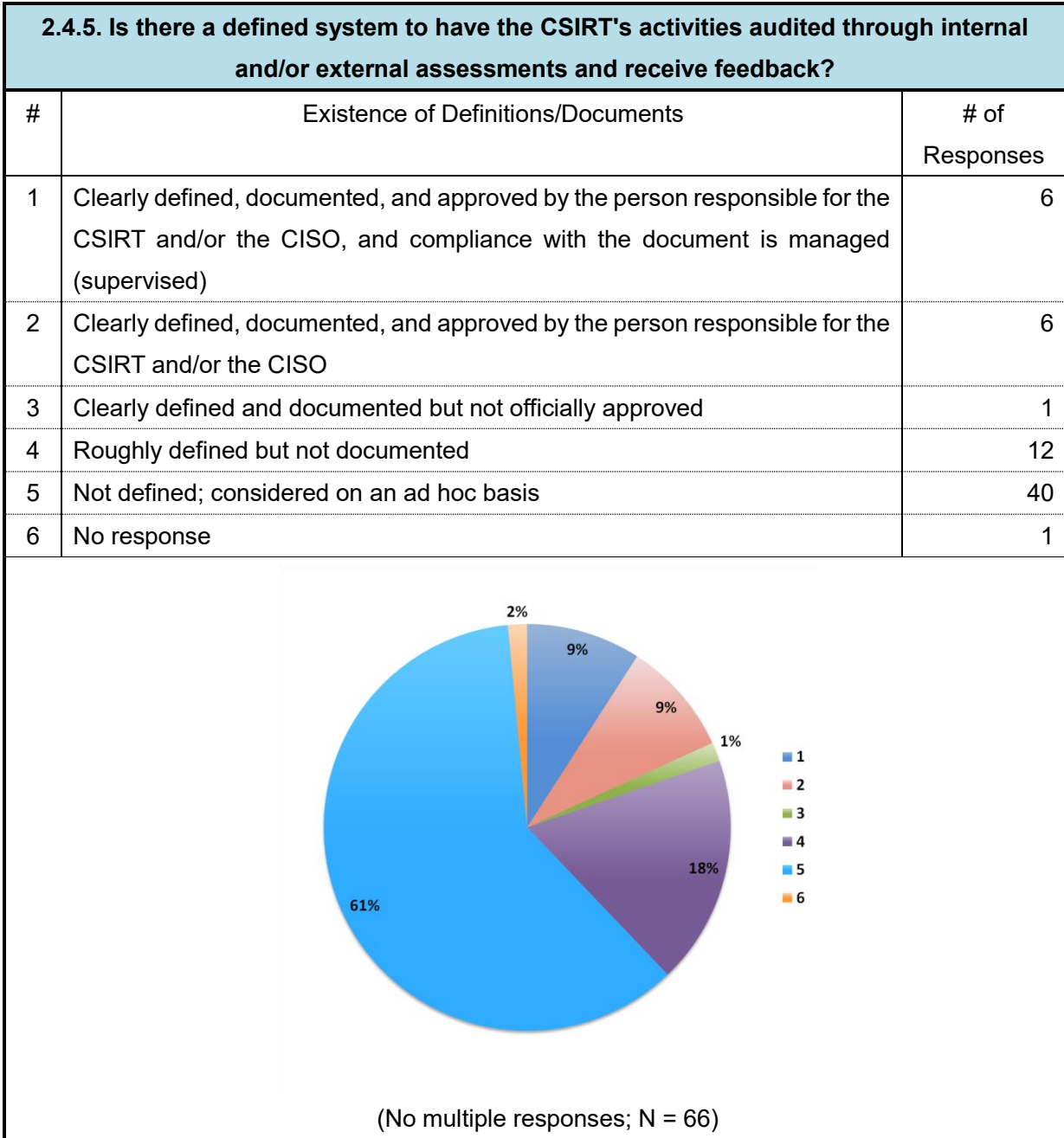
2.4.4. ARE PROCESSES FOR PREVENTING, DETECTING, AND RESOLVING INCIDENTS DEFINED?

Many of the organizations have defined processes for handling incidents from the moment they occur until they are resolved, though they may not be documented.



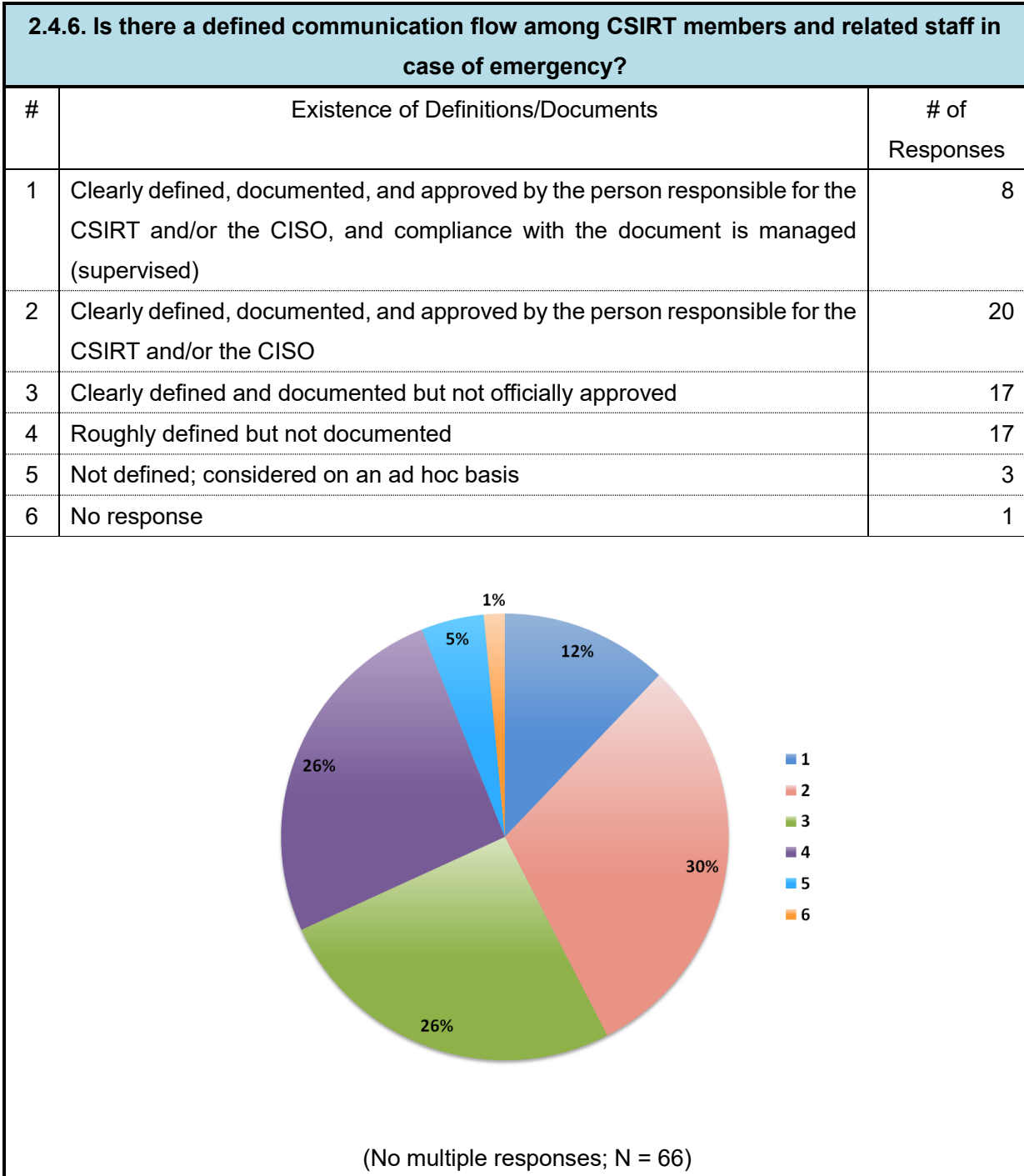
2.4.5. IS THERE A DEFINED SYSTEM TO HAVE THE CSIRT'S ACTIVITIES AUDITED THROUGH INTERNAL AND/OR EXTERNAL ASSESSMENTS AND RECEIVE FEEDBACK?

Only a few of the organizations have a clearly defined system for internal and/or external assessments of the CSIRT's activities.



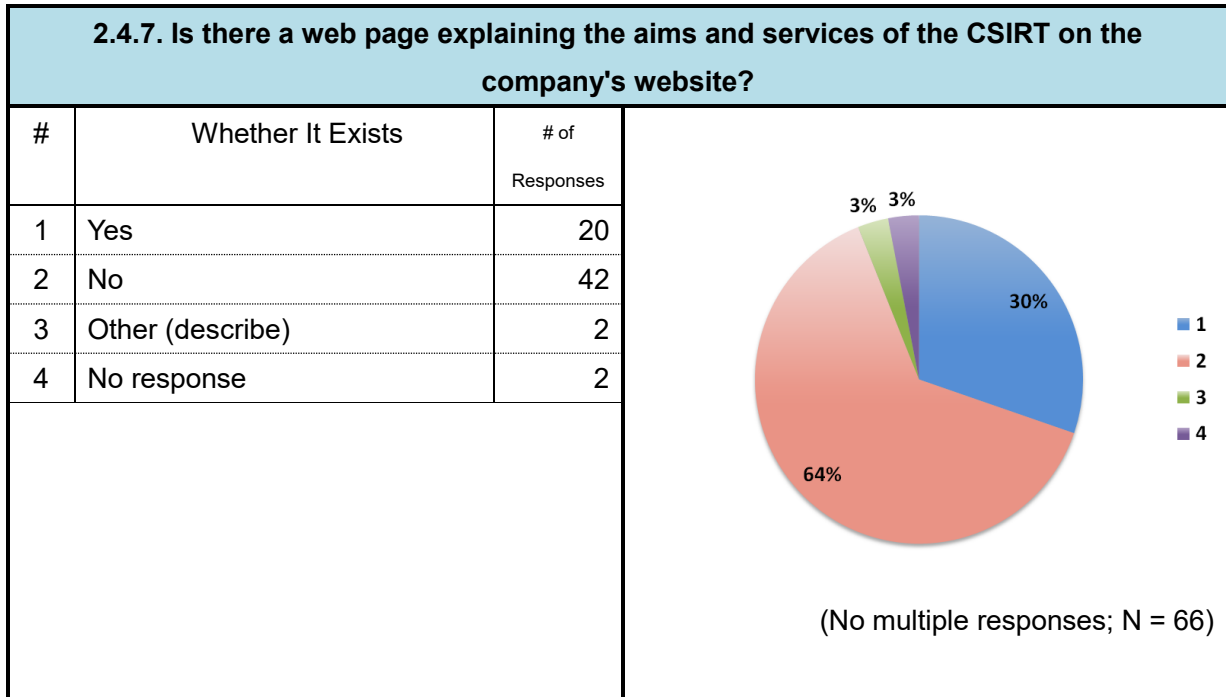
2.4.6. IS THERE A DEFINED COMMUNICATION FLOW AMONG CSIRT MEMBERS AND RELATED STAFF IN CASE OF EMERGENCY?

More than half of the CSIRTs have a defined communication flow among CSIRT members and related staff in case of emergency.



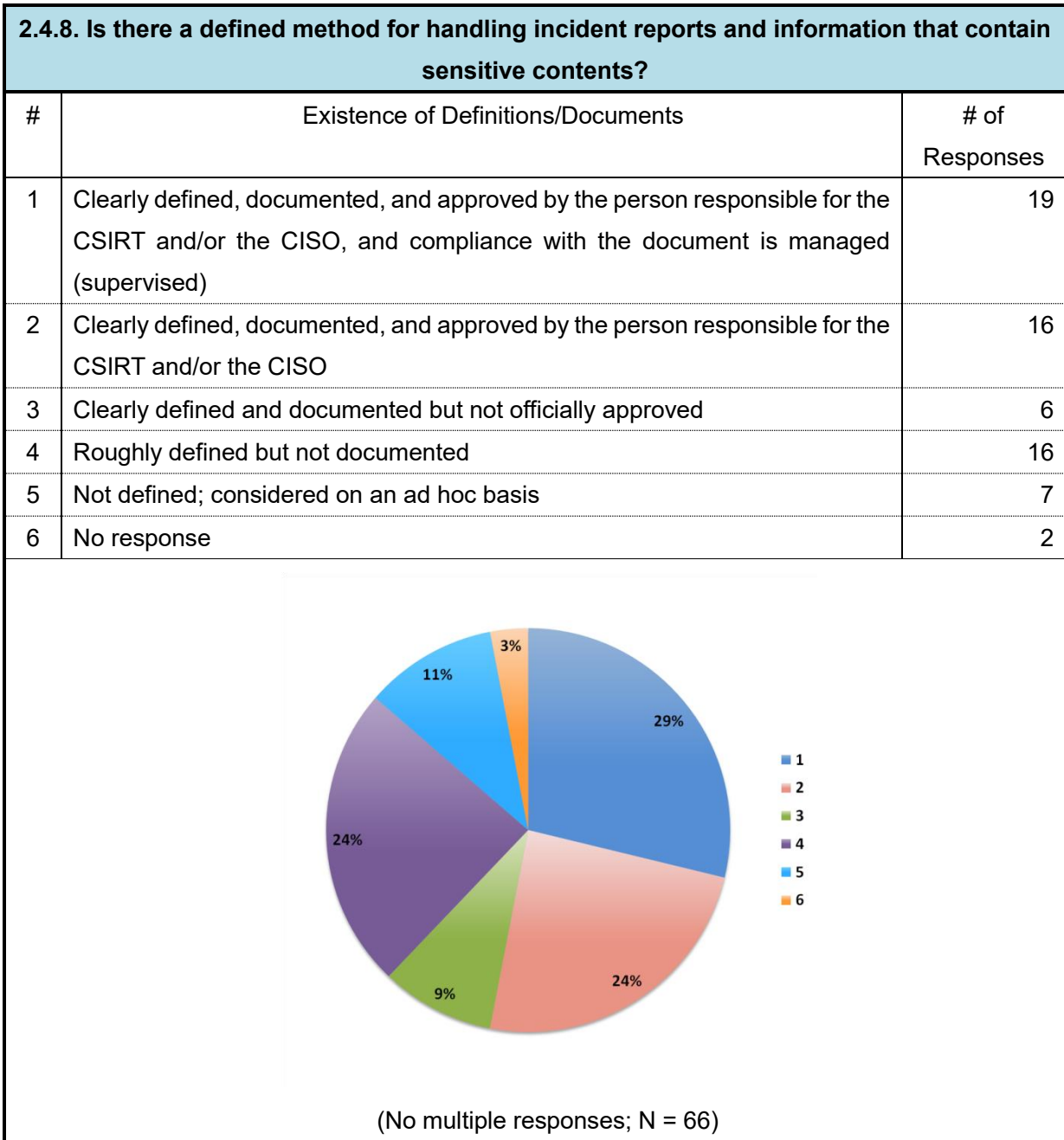
2.4.7. IS THERE A WEB PAGE EXPLAINING THE AIMS AND SERVICES OF THE CSIRT ON THE COMPANY'S WEBSITE?

Approximately 30% of the organizations have web pages explaining the aims and services of the CSIRT on their company's websites.



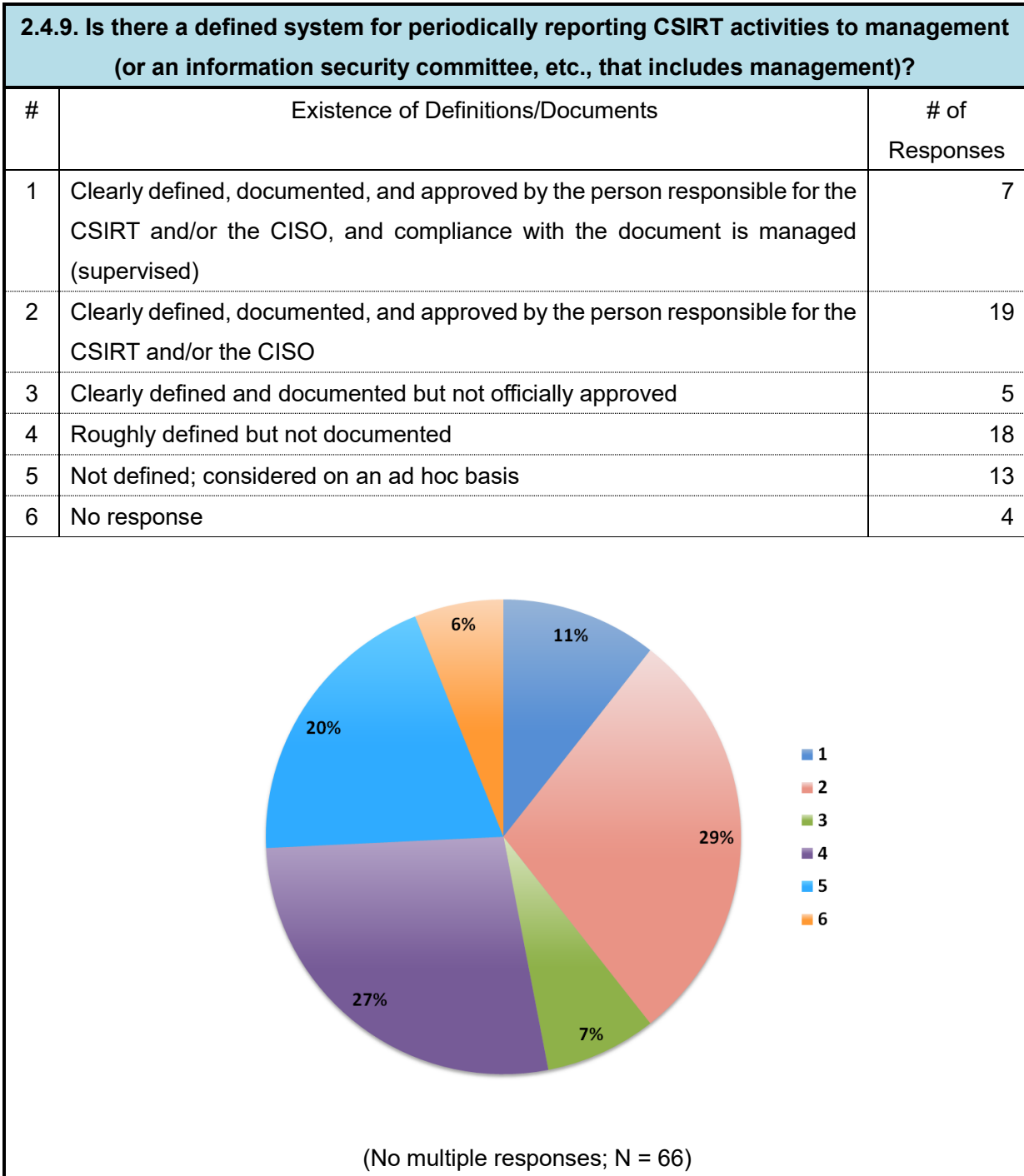
2.4.8. IS THERE A DEFINED METHOD FOR HANDLING INCIDENT REPORTS AND INFORMATION THAT CONTAIN SENSITIVE CONTENTS?

More than half of the organizations have clearly defined and documented methods for handling incident reports and information that contain sensitive contents, and they appropriately handle critical information.



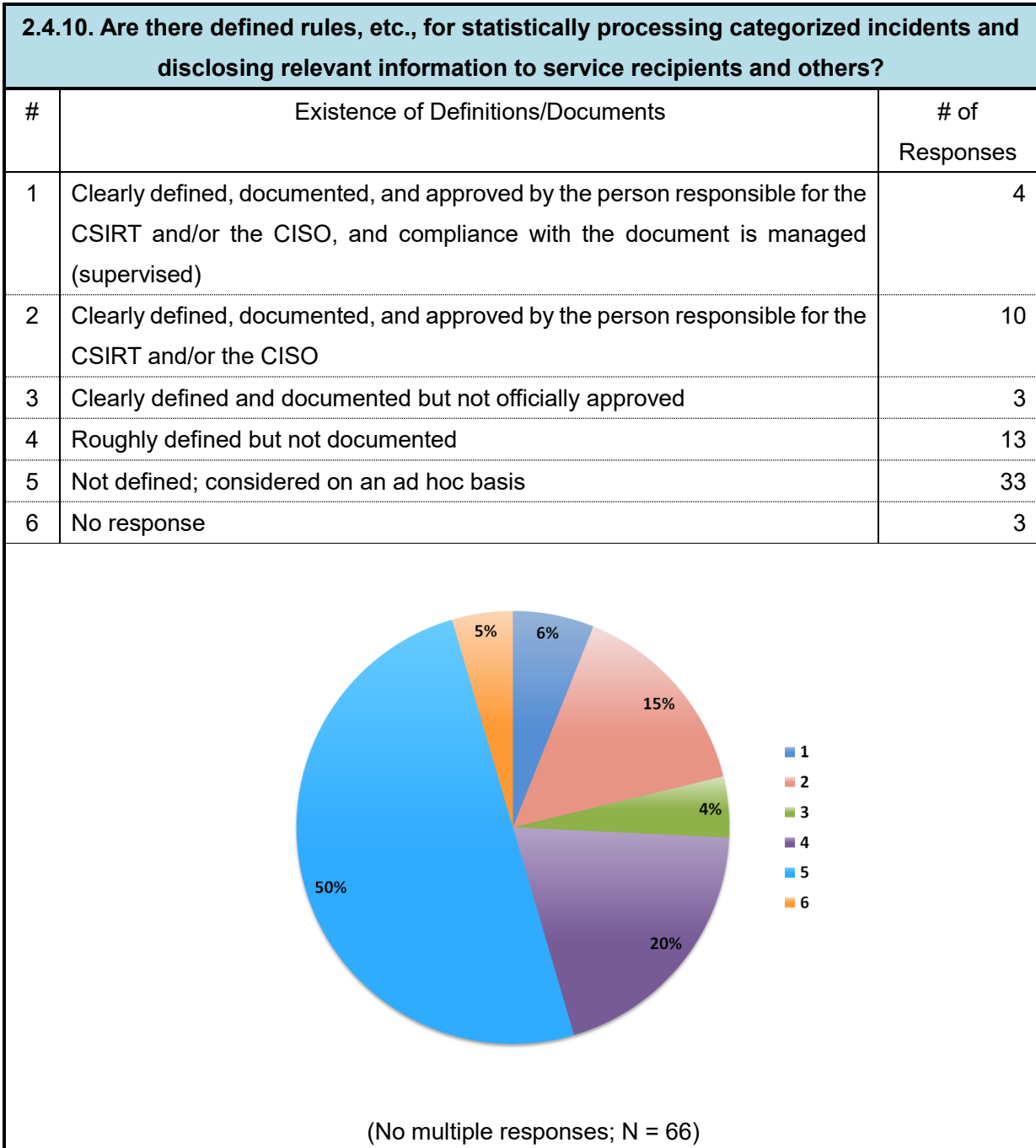
2.4.9. IS THERE A DEFINED SYSTEM FOR PERIODICALLY REPORTING CSIRT ACTIVITIES TO MANAGEMENT (OR AN INFORMATION SECURITY COMMITTEE, ETC., THAT INCLUDES MANAGEMENT)?

Approximately half of the organizations mandate periodic activity reports to an information security committee, etc., that includes management.



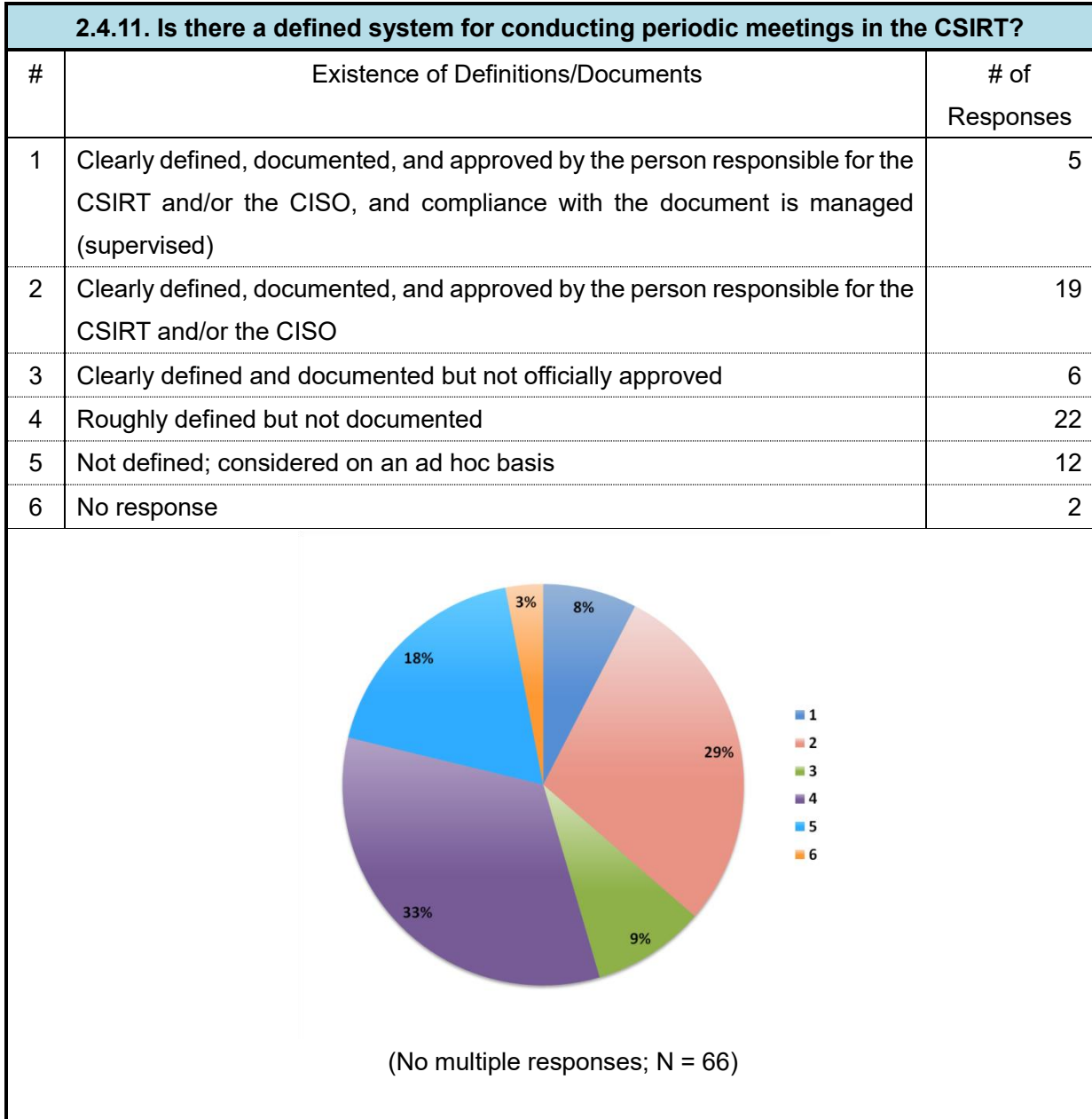
2.4.10. ARE THERE DEFINED RULES, ETC., FOR STATISTICALLY PROCESSING CATEGORIZED INCIDENTS AND DISCLOSING RELEVANT INFORMATION TO SERVICE RECIPIENTS AND OTHERS?

Less than half of the CSIRTs are mandated to categorize incidents and disclose them as statistical information to service recipients. Half of the CSIRTs consider such handling on an ad hoc basis.



2.4.11. IS THERE A DEFINED SYSTEM FOR CONDUCTING PERIODIC MEETINGS IN THE CSIRT?

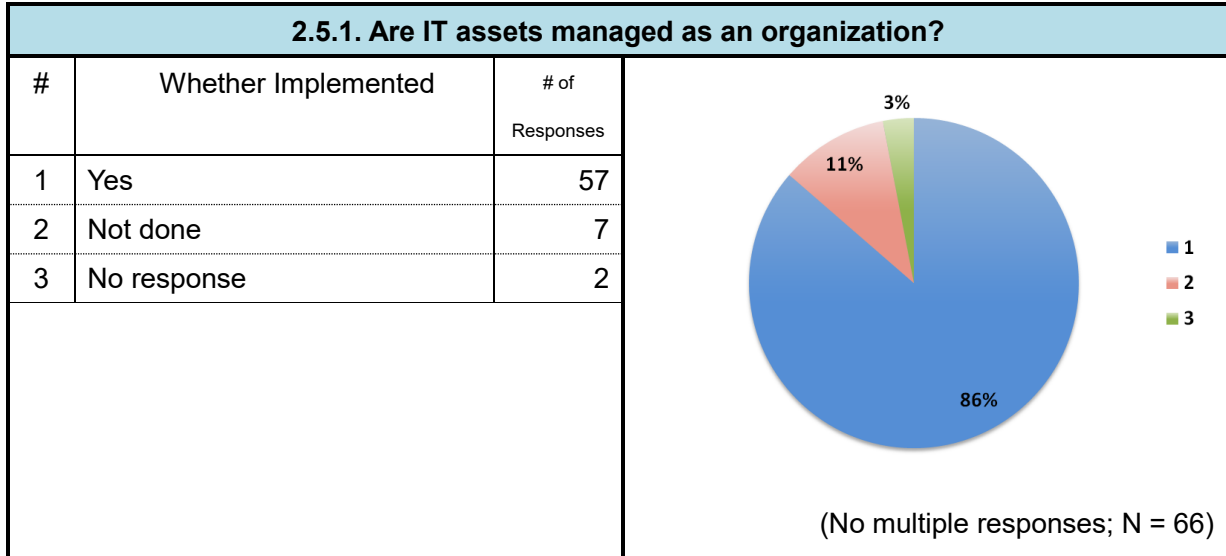
Many of the organizations hold periodic meetings in the CSIRT to share information, though this may not be documented.



2.5. TOOLS

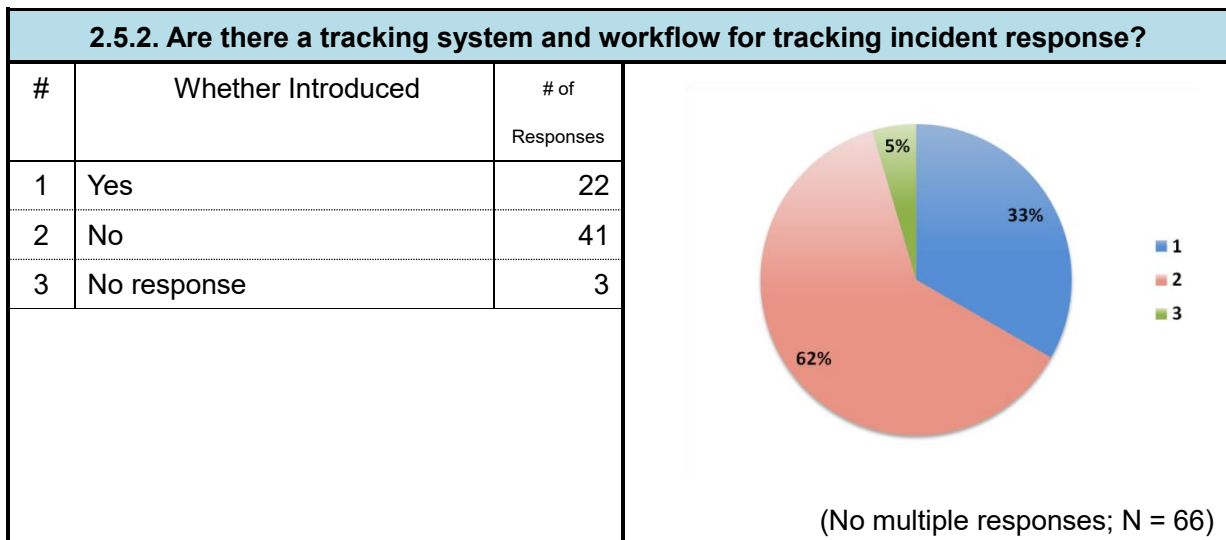
2.5.1. ARE IT ASSETS MANAGED AS AN ORGANIZATION?

More than 80% of the organizations have defined organizational methods for managing information and IT assets, and they conduct appropriate management according to the defined methods.



2.5.2. ARE THERE A TRACKING SYSTEM AND WORKFLOW FOR TRACKING INCIDENT RESPONSE?

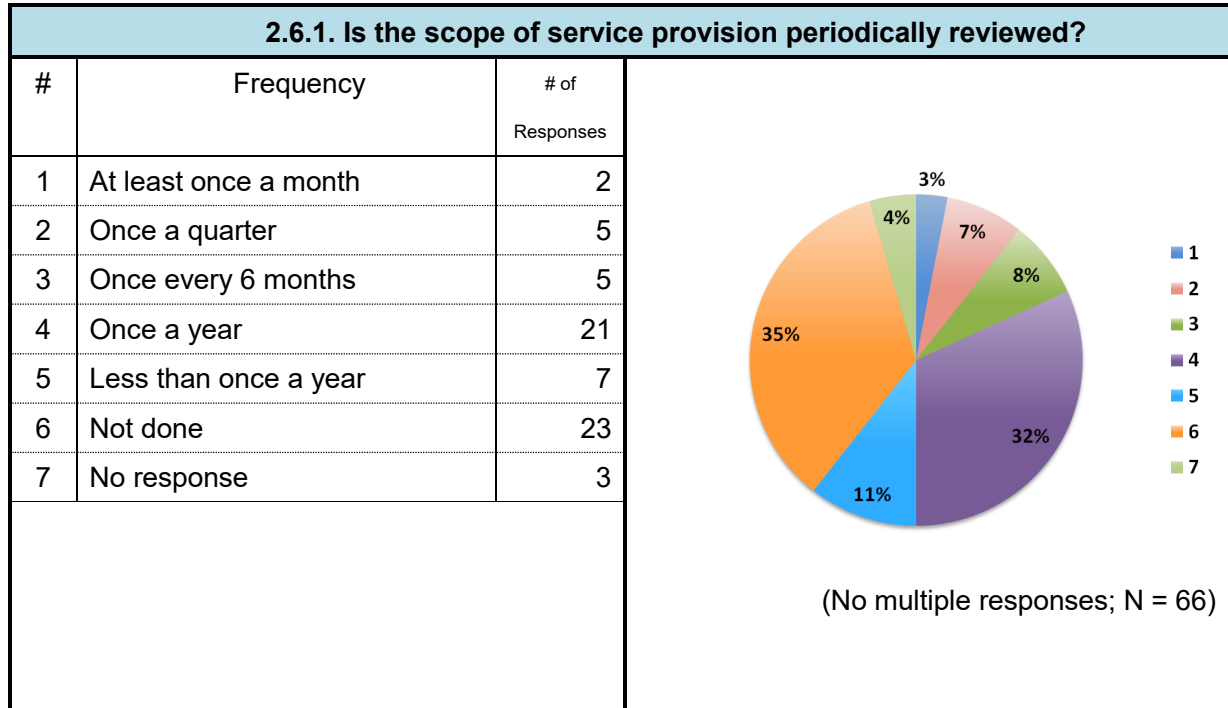
Approximately 30% of the CSIRTs have a tracking system and workflow for tracking incident responses.



2.6. REVISION OF SYSTEM AND RULES

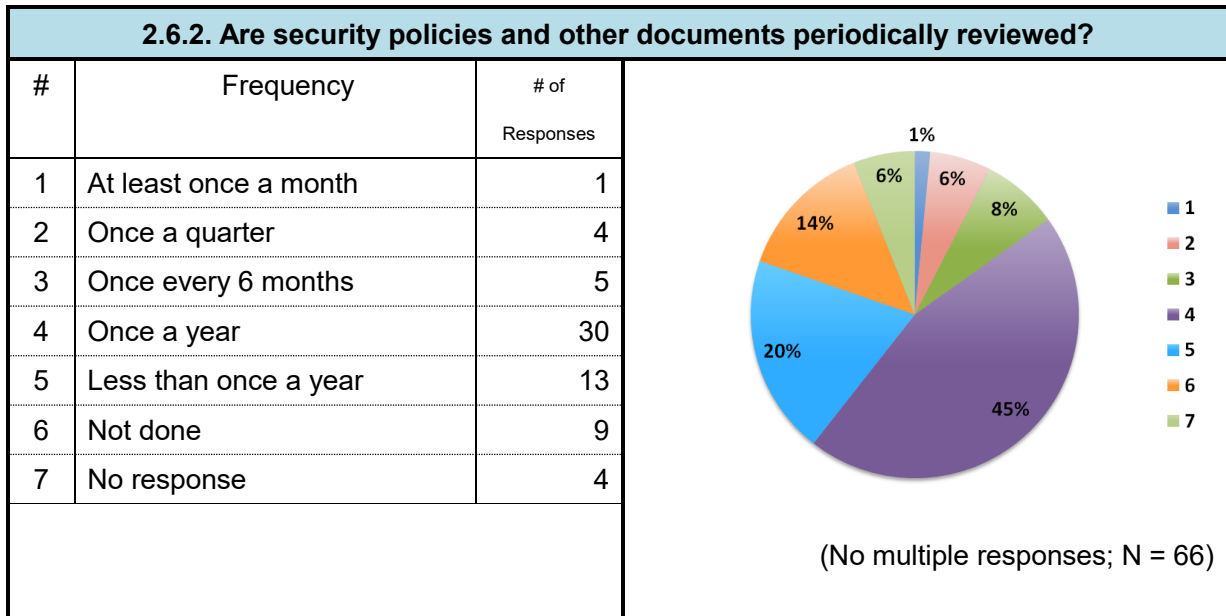
2.6.1. IS THE SCOPE OF SERVICE PROVISION PERIODICALLY REVIEWED?

More than half of the CSIRTs review the scope of service provision at least once a year.



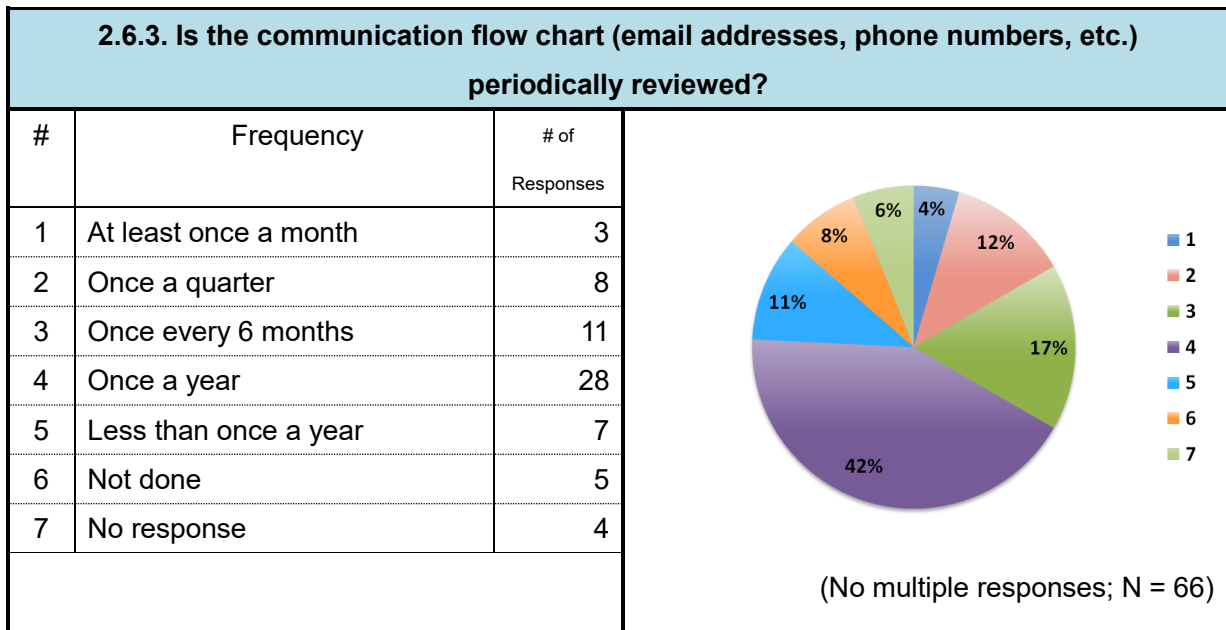
2.6.2. ARE SECURITY POLICIES AND OTHER DOCUMENTS PERIODICALLY REVIEWED?

A majority of the CSIRTs review security policies at least once a year.



2.6.3. IS THE COMMUNICATION FLOW CHART (EMAIL ADDRESSES, PHONE NUMBERS, ETC.) PERIODICALLY REVIEWED?

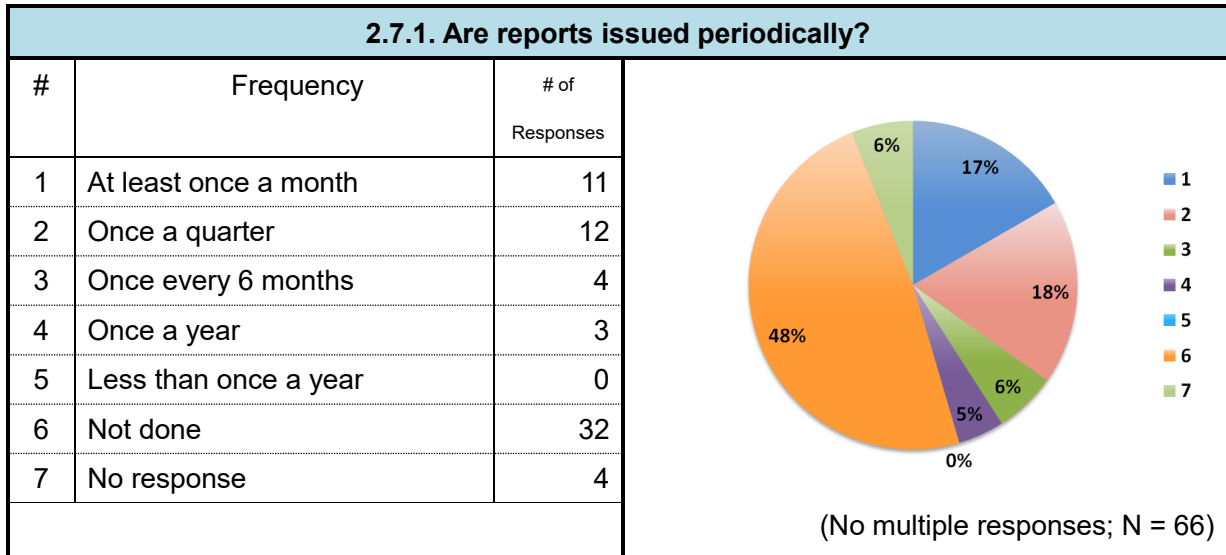
More than 70% of the CSIRTs review the communication flow chart at least once a year.



2.7. REPORTS

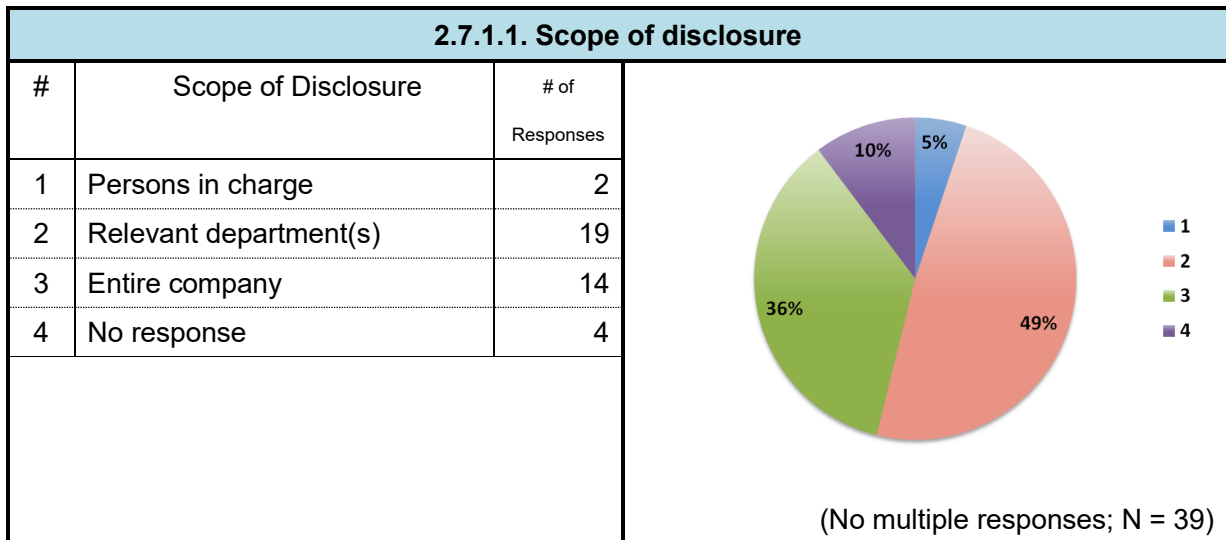
2.7.1. ARE REPORTS ISSUED PERIODICALLY?

Approximately half of the CSIRTs issue periodic reports, which are issued at least once a month in most of the cases.



2.7.1.1. SCOPE OF DISCLOSURE

Approximately half of the CSIRTs disclose their reports only within relevant departments.



3. RESULTS OF INTERVIEWS WITH NCA MEMBER CSIRTS

3.1. INTERVIEW WITH ASY-CSIRT

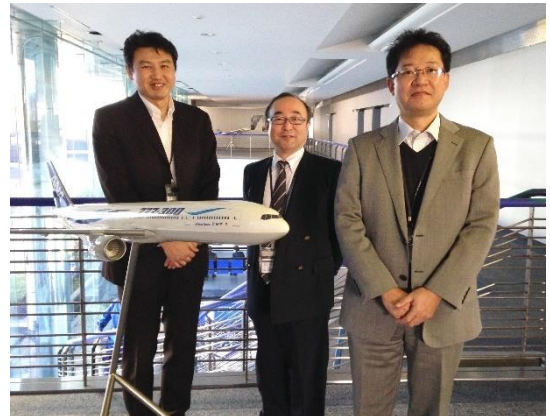
ASY-CSIRT	
Organization Name	ANA Systems Co., Ltd.
Line of Business	Air transport business
CSIRT Structure	
Organizational Model	Internal distributed CSIRT
Number of Staff	Approximately 10
Affiliation	ANA Holdings
Operational Budget	ANA Holdings prepares the budget for activity expenses in normal operation. Expenses for incident response are separately included in operational expenses, such as in the case of system failures.
Main Service Recipients	ANA Holdings Group companies around the world



3.1.1. OVERVIEW OF THE ORGANIZATION

ANA Systems Co., Ltd. Computer Security Incident Response Team (ASY-CSIRT) is a CSIRT operated by ANA Systems Co., Ltd. It operates for the purpose of achieving early recovery from security incidents and minimizing the scope of their impact for the entire ANA Group.

Fig. 1 ASY-CSIRT points of contact:
 Kyoichi Abe (center), Takahiro Ooyanagai (left),
 Shigetoshi Saito (right)
 (the picture was taken on January 17, 2017)



3.1.2. STRUCTURE AND AUTHORITY OF THE CSIRT

ASY-CSIRT is organized by members who belong to ANA Systems Co., Ltd.'s Quality and Security Supervision Office, a department that specializes in security-related matters. ASY-CSIRT forms a part of the ANA Group Information Security Center as a virtual organization under ANA Holdings. Instructions given by ASY-CSIRT are recognized as instructions from ANA Holdings' Security Center.

ASY-CSIRT operates in two fields—information system and human resources including governance—to serve as a one-stop spot that handles all matters related to security.

Airline companies generally practice risk management with a focus on terrorism, hijacking, and so on. Information security is also regarded as a business risk, and therefore, the activities of ASY-CSIRT are positioned within the existing risk management framework.

Although ASY-CSIRT does not have the authority to order the suspension of systems in the event of an emergency, it offers guidance to those responsible for system operation. It is also stated for ASY-CSIRT to examine new systems before they are put into service in order to verify whether they conform to security guidelines.

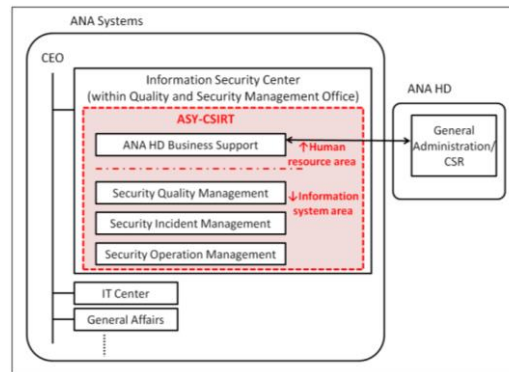


Fig. 2 ASY-CSIRT structure chart

3.1.3. OUTPUTS OF CSIRT ACTIVITIES

3.1.3.1. ACTIVITY REPORT TOWARDS THE MANAGEMENT LAYER

ASY-CSIRT submits semiannual reports to the management on annual plans and their reviews. Additional reports are submitted on an ad hoc basis in the event of a critical incident. ASY-CSIRT members try to avoid the use of technical jargon in their reports to the management to facilitate understanding. ASY-CSIRT also strives to quickly identify and analyze new security-related issues and trends in society and report its findings. For example, when the “Cybersecurity Management Guidelines” was released from the Ministry of Economy, Trade and Industry, ASY-CSIRT submitted a report to the management layer regarding the status of conformity with the guidelines within ANA two business days later.

3.1.3.2. ISSUANCE OF PERIODIC REPORTS

Departments which operate a system submit monthly reports summarizing the operation status of the entire system and these also include reports on any security incidents that have occurred during the month. These reports are intended for the perusal of Group employees and the management level.

3.1.3.3. QUANTITATIVE METRICS FOR THE CSIRT

Prevention of "critical incidents" which is defined in advance is positioned as the most important metrics for evaluating activity outputs. ASY-CSIRT also analyzes the data collected by security sensors (traffic monitors, spam filters, etc.) deployed at each site to confirm the situation for the ANA Group, and uses the number and nature of security incidents handled as one of the metrics.

3.1.4. EDUCATION/TRAINING OF CSIRT MEMBERS

3.1.4.1. INCIDENT HANDLING EXERCISES

ASY-CSIRT educates all executives and employees of the ANA Group through security news, guidelines, and other means provided every other month. ASY-CSIRT members regularly participate in incident handling exercise programs outside the company. Incident handling exercises are also conducted internally every week.

3.1.4.2. QUANTITATIVE METRICS FOR TECHNICAL SKILLS

The Information Security Center as a whole defines technical skills required of ASY-CSIRT members. Skills are divided into the three categories of "knowledge," "planning," and "communication," and the skills required in each category are defined and documented. For example, these documents specify the necessity of information security specialist and ISMS skills in the "knowledge" category, the ability to formulate policies and guidelines in the "planning" category, and the ability and presentation skills to explain the status of incident response without using technical jargon.

3.1.4.3. HUMAN RESOURCE DEVELOPMENT

While matters concerning to skills are maintained as described in 3.1.4.2, skills developed through practice are considered important. The Information Security Center divides practical operations into three and sets a human resource development path for each. As for operations related to documentation, education, assessment, and auditing, senior employees with many connections within the Group are assigned to facilitate the performance of operations.

Operations	Assigned Personnel	Knowledge and Skills to be Acquired after the Assignment
Verification of conformity	Personnel experienced in system development	<ul style="list-style-type: none"> - Knowledge about security and management - Creation of policies and guidelines - Verification of conformity, etc.
SOC, CSIRT, IRT (incident handling)	Personnel experienced in system development or system failure response	<ul style="list-style-type: none"> - Knowledge about security and management - Creation of policies and guidelines - Incident handling
Documentation, education, assessment, auditing	Personnel including senior staffs and presentation skills	<ul style="list-style-type: none"> - Knowledge about security and management - Creation of educational materials, employee development

3.1.5. STRUCTURE AND SERVICES OF THE CSIRT, AND REVIVING PERIOD OF MANAGEMENT FUNCTIONS

3.1.5.1. SERVICE RECIPIENTS AND SERVICES PROVIDED

The scope of service provided by ASY-CSIRT was defined in the three-year plan which was created on the establishment of the Information Security Center. This definition will be reviewed at the end of the three-year plan.

3.1.5.2. SECURITY POLICIES AND OTHER DOCUMENTS

The policies themselves are rarely reviewed. Guidelines containing details on system construction are reviewed twice a year.

3.1.5.3. COMMUNICATION FLOW

The same line of communication is used for responding to both incidents and failures. This line of communication is reviewed periodically.

3.1.5.4. INCIDENT MANAGEMENT

There are no dedicated management tools for incident handling. Management tools for handling queries are used to manage incidents.

3.1.6. SUMMARY

There is an established framework for risk management based on years of experience as an airline company, and information security risks are seen as an extension along the same line. ASY-CSIRT not only contributes to enhancing information security for the entire Group, but it also focuses on enhancing the security of newly developed systems. The framework ensures that the status of security implementation can be verified from the development design stage.

3.2. INTERVIEW WITH DeNA CERT

DeNA CERT	
Organization Name	DeNA Co., Ltd.
Line of Business	Service business
CSIRT Structure	
Organizational Model	Internal combined CSIRT
Number of Staff	Approximately 10
Affiliation	Security Department, Systems Head Office
Activities Budget	Mainly secured as a budget of the Security Department, which is composed as DeNA CERT
Main Service Recipients	DeNA headquarters and Group companies around the world



3.2.1. OVERVIEW OF THE ORGANIZATION

While DeNA Co., Ltd.'s main line of business is gaming, it also provides a wide range of services in other areas including e-commerce, curation platforms, and healthcare. In recent years, it has been actively pursuing various new businesses, aspiring to "change the structure of conventional mega-industries through the Internet" as one of its strategies.



Fig. 1 Fumie Watanabe, a member of DeNA CERT

DeNA CERT was established with the aim of maintaining the security of services provided by DeNA Group companies and of their internal systems, and quickly addressing incidents that occur within the Group companies.

3.2.2. STRUCTURE AND AUTHORITY OF THE CSIRT

DeNA CERT is mainly formed by members of the Security Department, Systems Head Office, but members who serve concurrent duties are also gathered from other related departments such as the Information Systems

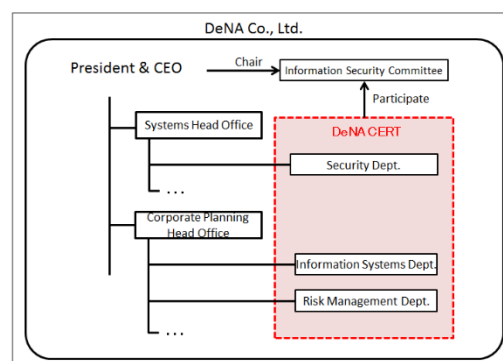


Fig. 2 DeNA CERT structure chart

Department and Corporate Department (Risk Management Department).

The Security Department consists of the Security Promotion Group, whose tasks include formulating policies and monitoring their operation, and the Security Technology Group, whose tasks include diagnosing vulnerabilities, dealing with fraud, and monitoring networks. The core members of DeNA CERT belong to the Security Promotion Group and are focused almost entirely on the work for DeNA CERT.

In the DeNA Group, the Information Security Committee, which is chaired by the president, is the highest decision-making body on security-related matters in general, and DeNA CERT itself does not have any authority. The Information Security Committee formulates security policies, under which employees are required to report any incidents they notice to DeNA CERT and not attempt to handle incidents on their own judgment, and DeNA CERT to provide guidance to said employees.

3.2.3. OUTPUTS OF CSIRT ACTIVITIES

3.2.3.1. ACTIVITY REPORT TO MANAGEMENT

DeNA CERT reports important incidents, monitoring results, new measures, and other matters at Information Security Committee meetings held every month. The Security Department submits monthly reports that include minor incidents to the Systems Head Office.

3.2.3.2. DOCUMENTS ISSUED TOWARD AUDIENCES INSIDE AND OUTSIDE THE COMPANY

There is an internal website for providing security-related information that includes DeNA CERT's activity reports and statistical data of incident occurrence inside the company and so on. Information is updated on a monthly basis. On the same website, DeNA CERT members post several security-related columns each month.

The website is managed by the Security Promotion Group, and articles are prepared by the Security Promotion Group and Security Technology Group. There is also a website for partners where security-related articles are posted occasionally.

3.2.3.3. METRICS FOR EVALUATING CSIRT ACTIVITIES

No metrics currently exist for evaluating DeNA CERT activities. However, there are specific targets for the ratio of employees taking e-learning courses for security education and the ratio of employees passing the completion exam. DeNA provides compliance training each month through e-learning, and three of the ten questions asked in the completion exam are related to security. The training deals in particular with topics related to security and protecting personally identifiable information. Further, employees who have consulted with DeNA CERT on security-related matters in the past are asked to cooperate with a

questionnaire to gain feedback, which is used for reviewing the handling of consultations, countermeasures taken, as well as rules.

3.2.4. EDUCATION/TRAINING OF CSIRT MEMBERS

3.2.4.1. INCIDENT HANDLING EXERCISES

The company is planning to conduct exercises targeting the Security Department, DeNA CERT, and employees several times a year. Last year, the company conducted training for all employees on targeted email attacks, and a cyber drill for DeNA CERT members with Mr. Nawa, a renowned cyber defense expert, serving as facilitator.

3.2.4.2. QUANTITATIVE METRICS FOR TECHNICAL SKILLS

No quantitative metrics exist for evaluating the technical skills of DeNA CERT members. Any requests to participate in external seminars or take official certification exams are considered and decided upon on a case-by-case basis. There is an organizational culture that respects the will of each employee, not just within DeNA CERT but within the entire company.

3.2.4.3. HUMAN RESOURCES DEVELOPMENT

No development plans currently exist. Security-related columns published internally are written by the members in turn, partly as an opportunity to increase knowledge and skills.

3.2.5. REVIEW PERIOD OF STRUCTURE, SERVICES AND MANAGEMENT FUNCTIONS OF THE CSIRT

3.2.5.1. SERVICE RECIPIENTS AND SERVICES PROVIDED

The current structure was established in fiscal 2014. Since approximately two years have passed, the company is making concrete plans to enhance and expand CSIRT functions. More specifically, the efforts include human resources development and providing opportunities for collaboration and workshops with other CSIRTs.

3.2.5.2. SECURITY POLICIES AND OTHER DOCUMENTS

Security policies are reviewed once a year. Manuals and other documents are reviewed every half year to check for any discrepancies with actual operation.

3.2.5.3. COMMUNICATION FLOW

The communication flow is checked and reviewed during companywide voluntary audits performed once every three months.

3.2.5.4. INCIDENT MANAGEMENT

A third-party project management system used companywide is used to manage incidents. No special tools are used.

3.2.6. SUMMARY

The president and every single employee demonstrate exceptional literacy. This can be seen in the fact that CSIRT activities are carried out without the need to give orders or instructions. The company's high literacy level has been achieved through its efforts to imbue its employees with an attitude to think through things, which is clearly stated in its corporate philosophy "DeNA Quality*6." As a result, the company as a whole is moving in the direction of increasing security in a self-propelling manner.

With a workforce with an average age of slightly over 30, the members of DeNA CERT are also young. The Security Technology Department, which supports DeNA CERT from a technical perspective, also actively hires new graduates and helps them acquire knowledge and skills related to security. In some cases, members are transferred to development or other business departments according to circumstances and demands within the company, as part of an effort to secure and develop a sufficient pool of security experts for the company.

*6 TOP>Company>Corporate Identity: DeNA Quality (Japanese Only) <http://dena.com/jp/company/policy/>

3.3. INTERVIEW WITH FJC-CERT

FJC-CERT	
Organization Name	Fujitsu Limited
Line of Business	Information and telecommunications business
CSIRT Structure	
Organizational Model	Internal centralized CSIRT
Number of Staff	Approximately 40
Affiliation	Security Management Services Division
Activities Budget	Each division that provides services to external clients bears FJC-CERT's activity expenses
Main Service Recipients	Mainly Fujitsu cloud service users (Corporate and product vulnerabilities are outside the scope of FJC-CERT's services and handled by another team)



3.3.1. OVERVIEW OF THE ORGANIZATION

Fujitsu Limited is a leading electronics company that manufactures and sells products such as telecommunications systems and devices and information processing systems. It also provides cloud services. Fujitsu Cloud CERT (FJC-CERT) is a CSIRT that was established to assist the latter.



Fig. 1 FJC-CERT representative: Shinichiro Yamashita (right)
Point of contact: Kayama Kosetsu (left)

When Fujitsu launched its public cloud services globally (in six countries), FJC-CERT was established with the purpose of responding quickly to security threats (cyber terrorism, unauthorized use, information leakage, etc.) in the cloud. The costs of operating FJC-CERT are borne by departments that receive its services (beneficiary departments).

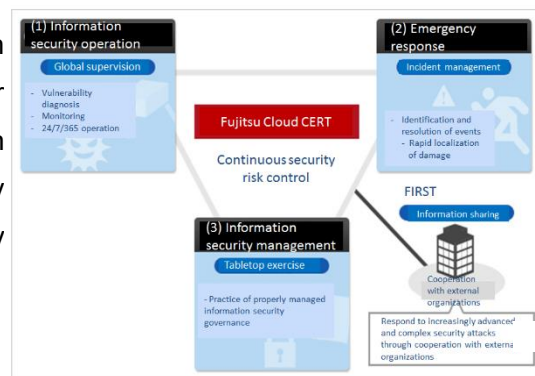


Fig. 2 Conceptual diagram of FJC-CERT activities

3.3.2. STRUCTURE AND AUTHORITY OF THE CSIRT

FJC-CERT is made up of members (approximately 40) of the Cyber Defense Center, Security Management Services Division.

FJC-CERT itself does not have an authority to order the suspension of systems in the event of a service emergency. Rather, it is in a position to offer technical advice and cooperation to service owners.

Its main activities consist of collecting information about vulnerabilities and cyber threats and monitoring unauthorized access to services.

FJC-CERT also handles security management for services in concert with departments responsible for product security and those that defend internal environments. When an incident occurs, it analyzes the events and responds appropriately to minimize damage.

3.3.3. OUTPUTS OF CSIRT ACTIVITIES

3.3.3.1. ACTIVITY REPORT TO MANAGEMENT

FJC-CERT reports the status of its activities at Security Committee meetings (held semiannually), in which the management also participates. It also provides monthly reports that contain information such as the number of incidents handled and the results of monitoring unauthorized access to beneficiary departments.

3.3.3.2. DOCUMENTS ISSUED TOWARD AUDIENCES INSIDE AND OUTSIDE THE COMPANY

FJC-CERT operates with the aim of "achieving zero critical security incidents," and it posts information about its daily activities on an internal website accessible to all employees.

3.3.3.3. METRICS FOR EVALUATING CSIRT ACTIVITIES

Since operating costs are borne by beneficiary departments, activity targets stated at the start of the fiscal year to these departments are used as metrics for CSIRT activities.

3.3.4. EDUCATION/TRAINING OF CSIRT MEMBERS

3.3.4.1. INCIDENT HANDLING EXERCISES

To enable rapid response in the event of a critical incident, related department members and service owners are regularly gathered for a tabletop incident response exercise.

3.3.4.2. QUANTITATIVE METRICS FOR TECHNICAL SKILLS

A Security Meister Accreditation System is provided for the entire Fujitsu Group instead of only the technical staff of FJC-CERT. This represents the company's efforts to raise motivation to increase security-related technical skills by quantitatively assessing the skills and achievements of its security personnel.

The Security Meister Accreditation System is categorized into three domains: the "field domain," which targets those engaged in system development and service operation work; the "expert domain," which targets those who possess advanced skills specialized in security; and "high meister domain," which targets those who possess skills on the level of a white hat hacker. These domains are further segmented into 15 fields that define personnel models*7. The Security Meister Accreditation System is not related to personnel evaluation, incentive payment, and other systems. It is provided for the purpose of finding and developing talents with exceptional skills related to cyber security, and supporting secure and reliable operation of ICT for the customers.

3.3.4.3. HUMAN RESOURCES DEVELOPMENT

FJC-CERT uses an education program of the Security Meister Accreditation System to develop human resources. The education program consists of two courses: common education and specialized education. For example, in the common education course for the expert domain, a program focused on training practical skills is provided using a cyber range (a virtual exercise environment) built within Fujitsu's environment. In addition, FJC-CERT hosts a Fujitsu Cyber Security Contest twice a year, where participants from across the Fujitsu Group are tested for practical knowledge and skills related to security. This event is one of the company's initiatives to find talents who are knowledgeable about security. By creating an environment for finding and developing future security meisters, the company is seeking to raise both skill levels and motivation.

3.3.5. REVIEW PERIOD OF STRUCTURE, SERVICES AND MANAGEMENT FUNCTIONS OF THE CSIRT

3.3.5.1. SERVICE RECIPIENTS AND SERVICES PROVIDED

The scope and details of services provided are reviewed as needed. In particular, since FJC-CERT provides vulnerability handling services, it also provides security consulting services including the study of security in the design stage.

*7 FUJITSU Security Initiative Security Meister Accreditation System: Fujitsu
<http://jp.fujitsu.com/solutions/safety/security-initiative/security-meister/>

3.3.5.2. SECURITY POLICIES AND OTHER DOCUMENTS

Security policies are reviewed as needed, but no review has been performed recently. However, procedures and guidelines are reviewed together when service details are reviewed.

3.3.5.3. COMMUNICATION FLOW

The communication flow is reviewed as appropriate. Tabletop training conducted quarterly often provides an opportunity to review the flow.

3.3.5.4. INCIDENT MANAGEMENT

As FJC-CERT quantifies results and provides the numerical information to beneficiary departments, it uses an open source ticket management system.

3.3.6. SUMMARY

To recap, the following three points characterize FJC-CERT.

1. FJC-CERT is defined as an organization that is responsible for the security of services provided by divisions to external clients.
2. It performs "preventive measures" (eliminating vulnerabilities during service design), prevents current attacks with "Symptomatic measures" (beach defense), and controls risks continually with "causal measures" (vulnerability diagnosis).
3. It performs activities to increase partners within the company through human resources development and internal security contests, with a view to ensuring ongoing cooperation with related departments.

3.4. INTERVIEW WITH Fuji Xerox CERT

Fuji Xerox CERT	
Organization Name	Fuji Xerox Co., Ltd.
Line of Business	Manufacturing business
CSIRT Structure	
Organizational Model	Internal distributed CSIRT
Number of Staff	Approximately 20
Affiliation	General Affairs Department
Activities Budget	The budget is included in the General Affairs Department's activities expenses
Main Service Recipients	Fuji Xerox and its group companies around the world



3.4.1. OVERVIEW OF THE ORGANIZATION

Fuji Xerox Co., Ltd. is a major electronics company that mainly manufactures and sells multifunctional printers and provides consultation for comprehensive document management solutions. It provides services extensively both in and outside Japan.



Fig. 1 Fuji Xerox CERT representative: Akira Kanbayashi (center)
Point of contact: Yoshihiro Masuda (right)
Kenji Urushima (left)

The company launched CSIRT activities in 2010 to respond to security threats globally. In 2014, Fuji Xerox CERT officially became a member of the NCA. Fuji Xerox CERT works to prevent, detect, and rapidly respond to cyber attacks and other threats across the organization for Fuji Xerox and its group companies around the world.

3.4.2. STRUCTURE AND AUTHORITY OF THE CSIRT

Fuji Xerox CERT is a virtual organization made up of members of the Information Systems Department and an information subsidiary who handle incidents that occur

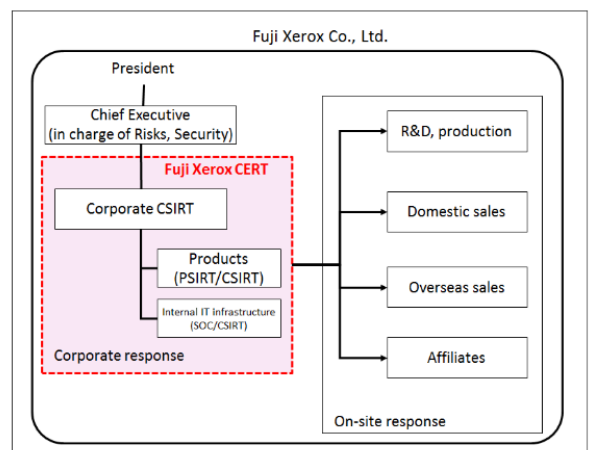


Fig. 2 Fuji Xerox CERT structure chart

within the internal infrastructure, and members of the Quality Assurance Department and Development Department who handle incidents related to products and services (including PSIRT functions, which deals with vulnerability handling).

The Information Security Center, General Affairs Department, which is responsible for risk management, serves as the administrative office.

Members of the Information Security Center, General Affairs Department come from various departments, including development, sales, and legal. Some of the members can even perform forensic investigations. Further, the information subsidiary, which operates the internal infrastructure, serves SOC functions (some of which are outsourced to professional vendors). The company cooperates with U.S. Xerox not through CSIRTs but on a departmental level.

Fuji Xerox CERT itself does not have an authority to give orders or instructions to suspend services, but the Risk Management Department, Information System Department, Quality Assurance Department and others that make up Fuji Xerox CERT give orders or instructions if necessary. Chief Executives in charge of information security and systems (i.e., CISOs or their equivalents) may also give orders or instructions.

Fuji Xerox CERT is basically positioned as a technical advisor, coordinator with related internal departments and external CSIRTs, and risk manager. For example, when incidents occur within the internal infrastructure, the situation is escalated to Fuji Xerox CERT, which determines the degree of risk, and the Information System Department the information subsidiary respond appropriately. As for incidents related to product vulnerabilities and services, the departments in charge of each product and service respond, and the Chief Executives in charge of each department make decisions such as whether to suspend services.

Although in the past, security-related information was provided under the name of the department to which relevant CERT members belong, going forward information will be provided under the name of Fuji Xerox CERT to raise its profile among Group companies around the world.

3.4.3. OUTPUTS OF CSIRT ACTIVITIES

3.4.3.1. ACTIVITY REPORT TO MANAGEMENT

The implementation status of information security measures and other relevant matters are explained to the management twice a year. Incidents, including minor ones, are reported on a weekly basis to the Chief Executive in charge of risk management. In addition, monthly reports are submitted to relevant members of the management. All reports are submitted under instructions from the management.

3.4.3.2. ISSUANCE OF PERIODIC REPORTS

An Information Security Report is issued about once a year. The report contains information that is relatively safe to make public, taken from activity reports submitted to the management.

3.4.3.3. QUANTITATIVE METRICS FOR THE CSIRT

While this may be different from quantitative metrics, Fuji Xerox CERT develops annual plans as a CSIRT including documentation of procedures and implementation of training, and reviews their progress in monthly meetings.

3.4.4. EDUCATION/TRAINING OF CSIRT MEMBERS

3.4.4.1. INCIDENT HANDLING EXERCISES

Exercises are performed at least once a year. The following are examples of training and exercises given.

- Employee training for handling targeted attacks
- Joint tabletop exercise by CSIRT members and relevant department members

3.4.4.2. QUANTITATIVE METRICS FOR TECHNICAL SKILLS

No particular metrics exist for CSIRT members. All employees of the company (especially the information subsidiary) are encouraged to obtain official certifications.

3.4.4.3. HUMAN RESOURCES DEVELOPMENT

No particular human resources development is performed for CSIRT members. New employees are given training to develop skills on a level that would allow them to pass the Information Technology Passport Examination, a national examination administered by JITEC (Japan Information-Technology Engineers Examination Center). Currently, there is a plan to require second and third year employees to pass the Information Security Management Examination, also a national examination administered by JITEC, as a means to step up to the next level.

3.4.5. REVIEW PERIOD OF STRUCTURE, SERVICES AND MANAGEMENT FUNCTIONS OF THE CSIRT

3.4.5.1. SERVICE RECIPIENTS AND SERVICES PROVIDED

There is a scheme to review the scope of services provided each year, and reviews are conducted accordingly.

3.4.5.2. SECURITY POLICIES AND OTHER DOCUMENTS

Security policies and other documents are reviewed each year to check for any discrepancies with actual operation.

3.4.5.3. COMMUNICATION FLOW

Those concerned meet once a month to review and confirm relevant matters.

3.4.5.4. INCIDENT MANAGEMENT TOOLS

As a CSIRT, there are no incident management tools yet, for managing only cyber security (currently under consideration). Information security incidents as a whole, are managed by the Information Security Center, General Affairs Department, using products developed in-house. For reporting and responding to incidents, an in-house developed Tools namely, “Incident Report Management System” and “Vulnerability Information Automatic Delivery System”, are used.

3.4.6. SUMMARY

Based on an organizational culture cultivated through years of experience as a manufacturer, the company has always provided quality assurance with a focus on safety. The management's interest in information security is high, and new employees are given activities designed to raise their safety awareness.

3.5. INTERVIEW WITH I-SIRT

I-SIRT	
Organization Name	Imperial Hotel, Ltd.
Line of Business	Service business
CSIRT Structure	
Organizational Model	Internal distributed CSIRT
Number of Staff	5 (administrative office)
Affiliation	Information Systems Department
Activities Budget	The budget is included in the Information System Department's activities expenses
Main Service Recipients	Imperial Hotel and the Imperial Hotel Group as a whole



3.5.1. OVERVIEW OF THE ORGANIZATION

Imperial hotel-Security Incident Response Team (I-SIRT) is a CSIRT of Imperial Hotel and the Imperial Hotel Group and the first CSIRT to have joined the NCA in the hotel industry. I-SIRT operates with the goal of preventing IT-related security incidents within the Group, minimizing potential risks and handling matters in the event of an incident.



Fig. 1 I-SIRT representative: Toru Imai (second from left)
 Point of contact: Koichi Shirasaka (far left)
 Other I-SIRT members

3.5.2. STRUCTURE AND AUTHORITY OF THE CSIRT

I-SIRT is a virtual organization that is made up of members from across the organization who provide existing risk management functions and also serve a new role of maintaining security. The Information System Department provides administrative office functions, and an IT security manager is assigned in each department to serve as a point of contact for I-SIRT.

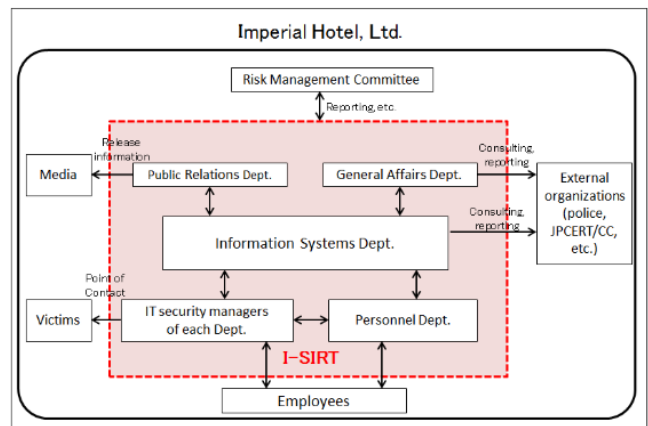


Fig. 2 I-SIRT structure chart

Before the establishment of I-SIRT, Imperial Hotel had the Risk Management Committee to deal with and

respond to various risks including terrorism and food hygiene. While the Information System Department used to handle matters related to IT security independently, I-SIRT was later established in an effort to take a more company-wide approach.

When an incident occurs, I-SIRT's administrative office provides guidance and instructions to those in charge at the relevant department and the Information System Department communicates with each relevant department that is a member of I-SIRT, and reports as needed to the Risk Management Committee, which manages risks for the entire company. If the incident calls for advanced expertise, it also seeks cooperation from external professional organizations.

3.5.3. OUTPUTS OF CSIRT ACTIVITIES

3.5.3.1. ACTIVITY REPORT TO MANAGEMENT

Activities are reported every half year at Risk Management Committee meetings, which are attended by the management as well. As a result, the management is now well aware that cyber-attacks are a critical business risk.

3.5.3.2. ISSUANCE OF PERIODIC REPORTS

In addition to activity reports sent to the Risk Management Committee, a monthly report called "IT Security Report" is issued for IT security managers at each department, with the aim of increasing their knowledge. This report explains the threat of cyber-attacks such as targeted attack emails, the importance of observing security policies, and so on.

3.5.3.3. QUANTITATIVE METRICS FOR THE CSIRT

Currently, no quantitative metrics exist for evaluating I-SIRT activities.

3.5.4. EDUCATION/TRAINING OF CSIRT MEMBERS

3.5.4.1. INCIDENT HANDLING EXERCISES

In internal training dealing with targeted attack emails, employees are instructed to follow a prescribed escalation flow, which, for example, requires that they report to the IT security manager of their own department if they accidentally open such an email. The training is conducted in a realistic setting, where I-SIRT members head to the affected site upon receiving a report from an IT security manager. Since the training, security awareness has clearly increased among employees, as can be seen in the increased number of people reporting suspicious emails to the I-SIRT administrative office.

3.5.4.2. QUANTITATIVE METRICS FOR TECHNICAL SKILLS

Currently, no metrics exist for quantitatively evaluating technical skills. Since the main line of business is providing services, activities do not focus on quantitative evaluation of technical skills.

3.5.4.3. HUMAN RESOURCES DEVELOPMENT

As part of human resources development, there is a system for providing aid and support for obtaining general IT certifications. However, I-SIRT currently has no clear arrangements on the definition of human resources qualified for its work. Members of the I-SIRT administrative office include those from the Sales Department who have little experience in IT-related work. As such, training is conducted on the job according to a medium-term plan, but hiring new talent with expert knowledge in security is also considered necessary.

3.5.5. REVIEW PERIOD OF STRUCTURE, SERVICES AND MANAGEMENT FUNCTIONS OF THE CSIRT

3.5.5.1. SERVICE RECIPIENTS AND SERVICES PROVIDED

Personal, technical, and physical security measures are reviewed during the budgeting process each year, in addition to reviews conducted as situations change.

3.5.5.2. SECURITY POLICIES AND OTHER DOCUMENTS

After I-SIRT was established, security items were added to the company's policies related to information systems. In order to familiarize employees with the policies, an Information System Safety Management Handbook, which contains easy-to-understand explanations of the policies, was created and distributed.

3.5.5.3. COMMUNICATION FLOW

The I-SIRT administrative office communicates information through the IT security managers of departments. The communication flow chart is reviewed when there is a personnel transfer.

3.5.5.4. INCIDENT MANAGEMENT

No particular incident management tools are used. Relevant information is managed with Excel, and OneNote is used to share the status of incident handling.

3.5.6. SUMMARY

Based on experience in risk management cultivated as a hotel, I-SIRT understands that the personally identifiable information of guests in particular has a high risk of being targeted by attackers and thus needs to be protected. While security measures are considered essential, I-SIRT also operates with a focus on improving convenience as a hotel. Hiring of IT experts is considered necessary. At the same time, I-SIRT is working to increase its ability to collect information through the NCA's working groups, to cooperate with other hotels, and implement effective personal, technical, and physical security measures.

3.6. INTERVIEW WITH MB-SIRT

MB-SIRT	
Organization Name	Mori Building Co., Ltd.
Line of Business	Real estate business
CSIRT Structure	
Organizational Model	Internal distributed CSIRT
Number of Staff	Approximately 5
Affiliation	Information Systems Department
Activities Budget	The budget is included in the Information System Department's activities expenses
Main Service Recipients	Mori Building and its related companies



3.6.1. OVERVIEW OF THE ORGANIZATION

Mori Building Co., Ltd. is a major real estate company that pursues urban redevelopment both in Japan and abroad. The scope of its business activities encompasses not only urban redevelopment and real estate rental and management but also culture and art.

Mori Building Security Incident Response Team (MB-SIRT) was established following an incident in March 2014 in which a website run by Mori Building was compromised. MB-SIRT's activities include responding to security incidents targeting Mori Building and its group companies, educating employees in an effort to prevent incidents, and establishing security rules.

3.6.2. STRUCTURE AND AUTHORITY OF THE CSIRT

MB-SIRT is made up of members in charge of information security in the Information Systems Department.



Fig. 1 MB-SIRT point of contact:
Yoshinori Sato

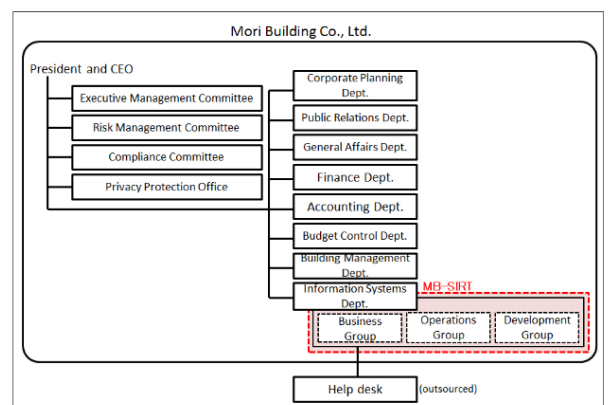


Fig. 2 MB-SIRT structure chart

Before MB-SIRT was established, the Information Systems Department led Mori Building's incident handling activities. The officer in charge of the department serves the role of a CISO. MB-SIRT operates according to a framework created mainly by the Information Systems Department. Decisions are made by the Information Systems Department and other relevant departments; MB-SIRT does not operate on its own judgment alone.

In addition to the operation and administration of information systems within the company, the Information Systems Department also engages in planning and development. It is responsible for IT-related operations of the Mori Building Group, including many of its related companies. The department also oversees the budget in some cases (although the management systems for buildings managed by Mori Building are administered by another department, further cooperation will likely be necessary).

In the event of a security incident, MB-SIRT provides technical assistance and support. It also works in concert with the Risk Management Committee, Privacy Protection Office, Public Relations Department, and others. If the incident calls for advanced expertise, it outsources its handling to external professional vendors.

3.6.3. OUTPUTS OF CSIRT ACTIVITIES

3.6.3.1. ACTIVITY REPORT TO MANAGEMENT

An overview of technical assistance and support is provided as activity reports through the Risk Management Committee. Depending on the importance of responding to the information obtained, the Information Systems Department may report the status of response.

3.6.3.2. DOCUMENTS ISSUED TOWARD AUDIENCES INSIDE AND OUTSIDE THE COMPANY

Policies, security information, etc., are provided by the Information Systems Department. Currently, MB-SIRT does not release any documents.

3.6.3.3. METRICS FOR EVALUATING CSIRT ACTIVITIES

As of yet, there are no metrics for quantitatively evaluating CSIRT activities. Details of technical assistance and support are shared with the management through activity reports. The management regards information security as an extension of physical security in real estate and thus an essential element of its business, so its interest in security is high.

3.6.4. EDUCATION/TRAINING OF CSIRT MEMBERS

3.6.4.1. INCIDENT HANDLING EXERCISES

Training on Targeted emails is provided to all employees. Although no incident handling exercises tailored to the CSIRT are conducted, they are on the agenda to be considered for the future.

3.6.4.2. QUANTITATIVE METRICS FOR TECHNICAL SKILLS

Currently, there are no metrics for quantitatively evaluating the IT skills of technical staff.

3.6.4.3. HUMAN RESOURCES DEVELOPMENT

MB-SIRT actively provides support to members who wish to obtain certifications or participate in external seminars. However, there are no specific rules on certifications to be obtained and seminars to be taken. Whether it is appropriate to participate is determined on a case-by-case basis.

3.6.5. REVIEW PERIOD OF STRUCTURE, SERVICES AND MANAGEMENT FUNCTIONS OF THE CSIRT

3.6.5.1. SERVICE RECIPIENTS AND SERVICES PROVIDED

Services are reviewed during the budgeting process of the Information Systems Department.

3.6.5.2. SECURITY POLICIES AND OTHER DOCUMENTS

At Mori Building, a notification is issued once a year to review policies company-wide, and security-related policies are reviewed at this timing. In addition, the Information Systems Department conducts reviews as needed when systems are replaced.

3.6.5.3. COMMUNICATION FLOW

The communication flow is reviewed as appropriate when there is a personnel transfer. It is also reviewed at Risk Management Committee meetings held every other week.

3.6.5.4. INCIDENT MANAGEMENT


MB-SIRT manages incidents as records of the Information Systems Department, but as of now no tools are used for incident management. A help desk run by an external vendor to accept queries from regular employees uses a database system developed in-house to manage incidents.

3.6.6. SUMMARY

The Information Systems Department is entrusted with the entire lifecycle of IT systems from planning to development and operation, and this keeps the technical staff's motivation high. As a result, MB-SIRT members are thoroughly familiar with the structure of IT systems in operation, enabling smooth response in the event of an incident.

3.7. INTERVIEW WITH NTT-CERT

NTT-CERT	
Organization Name	Nippon Telegraph and Telephone Corporation
Line of Business	Information and telecommunications business
CSIRT Structure	
Organizational Model	Coordinating CSIRT
Number of Staff	Approximately 60
Affiliation	NTT Secure Platform Laboratories
Activities Budget	The budget is included in the research expenses of NTT Secure Platform Laboratories
Main Service Recipients	NTT Group companies



3.7.1. OVERVIEW OF THE ORGANIZATION

NTT-CERT is a CSIRT that belongs to NTT Secure Platform Laboratories, which is part of the Service Innovation Laboratory Group of Nippon Telegraph and Telephone Corporation (NTT). NTT Secure Platform Laboratories specializes in research and development related to security such as encryption technologies, cyber security, and security architecture, and it conducts CSIRT operations as part of its security risk management project. NTT-CERT provides security-related information, investigations, analyses, and education to the entire NTT Group as services. It is also one of the founding members of the NCA.

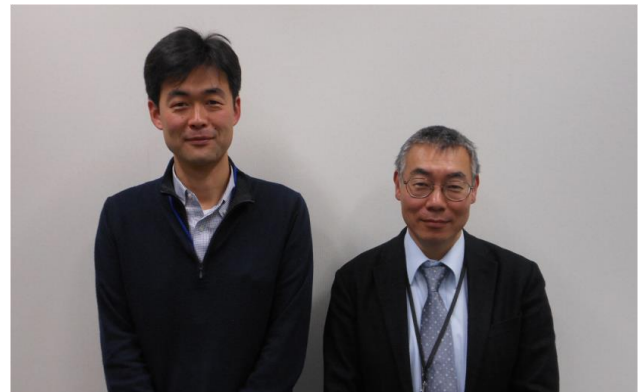


Fig. 1 NTT-CERT point of contact:
 Naoki Sekido (left)
 Seiichi Komura* (right)
 *Currently belonging to NTT Advanced Technology Corporation

3.7.2. STRUCTURE AND AUTHORITY OF THE CSIRT

NTT-CERT accepts security incident information, supports incident response, studies measures to prevent

recurrence, and provides training programs and security-related information concerning the NTT Group. It is incorporated into the NTT Group's risk management structure and operates as the Group's disaster control team. As a coordinating CSIRT, it has approximately 60 members (including support staff from external contractors).

NTT-CERT does not have an authority to give instructions to the Group companies or any control. Its activities include providing technical information and coordinating and handling security-related activities by Group organizations. Each Group company determines how to use the information provided by NTT-CERT. The authority to issue orders to Group companies is vested in the Internal Control Office under NTT's General Affairs Department.

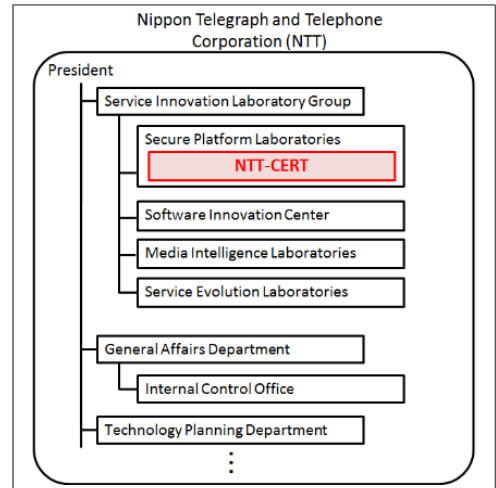


Fig. 2 NTT-CERT structure chart

3.7.3. OUTPUTS OF CSIRT ACTIVITIES

3.7.3.1. ACTIVITY REPORT TO MANAGEMENT

The number of security alerts issued and the number and trend of incidents handled are reported to the management of the Laboratories once a month. Quarterly reports are created and issued based on this information,

3.7.3.2. ISSUANCE OF PERIODIC REPORTS

Security-related analyst reports and vulnerability reports are provided as appropriate through NTT-CERT's website for the Group. An annual report that contains information such as security trends and verification results of security products is made available to the public once a year.

3.7.3.3. QUANTITATIVE METRICS FOR THE CSIRT

Based on a report prepared by the Japan Network Security Association (JNSA), NTT-CERT calculates the estimated value of damage caused by incidents that occurred within the NTT Group and reports this to the management of the Laboratories once a year. This data provides numerical grounds for explaining the effects of CSIRT activities, so it enables an objective comparison of the effects of security measures.

3.7.4. EDUCATION/TRAINING OF CSIRT MEMBERS

3.7.4.1. INCIDENT HANDLING EXERCISES

Once a year, about 100 participants from the ten NTT Group companies gather for an incident handling

exercise.

3.7.4.2. QUANTITATIVE METRICS FOR TECHNICAL SKILLS

In some technical areas, employees are accredited for their skill levels (i.e., elementary, intermediate, etc.) based on the certifications they have. NTT-CERT may provide guidance on recommended certifications related to security.

3.7.4.3. HUMAN RESOURCES DEVELOPMENT

NTT Group plans to train 10,000 security experts within the NTT Group by 2020, and it is currently attempting to define a future vision for them to aim for. NTT-CERT supports this activity and also participates in TRANSITS and has qualified members.

3.7.5. STRUCTURE AND SERVICES OF THE CSIRT, AND OPTIMIZATION OF MANAGEMENT FUNCTIONS

3.7.5.1. SERVICE RECIPIENTS AND SERVICES PROVIDED

The scope of services provided is reviewed once a year during the budgeting process. Last year, NTT-CERT expanded the scope of its services, drawing on its accumulated pool of know-how in handling incidents. It is now considering whether information sharing and other services may not be provided to Group companies abroad going forward.

3.7.5.2. SECURITY POLICIES AND OTHER DOCUMENTS

NTT Group companies' security policies are created by NTT's Internal Control Office, and NTT-CERT offers guidance and technical support when the policies are created. NTT-CERT reviews its own security policies once a year when compiling a budget.

3.7.5.3. COMMUNICATION FLOW

NTT's Technology Planning Department manages the communication flow chart. The established flow enables Group companies to be contacted 24 hours a day, 365 days a year, and it is updated as appropriate when there is a personnel transfer, etc.

3.7.5.4. INCIDENT MANAGEMENT

For incident handling, case management registers that points of contact maintain are used. NTT-CERT also develops unique system tools.

3.7.6. SUMMARY

NTT-CERT is a "CSIRT organization run by a research laboratory." While services are provided to NTT Group companies, NTT-CERT does not have any authority over each department. For this reason, there is an accessible atmosphere that allows the departments to casually consult with it and facilitates communication.

NTT-CERT believes that communication skills are important for a CSIRT and is thus endeavoring to create a network that emphasizes face to face interactions beyond Group companies through incident handling exercises, information sharing meetings, and workshops.

3.8. INTERVIEW WITH T-SIRT

T-SIRT	
Organization Name	Taisei Corporation
Industry group	Construction industry
CSIRT Structure	
Organizational Model	Internal distributed CSIRT
Number of Staff	8
Affiliation	Information Planning Department, Corporate Planning Office
Activities Budget	The budget is included in the Information Planning Department's activities expenses
Main Service Recipients	Taisei Corporation and its Group/related companies



3.8.1. OVERVIEW OF THE ORGANIZATION

Taisei Corporation is one of Japan's leading general construction companies, and Taisei-SIRT (T-SIRT) is its internal CSIRT. T-SIRT is also the first CSIRT to have joined the NCA in the construction industry.

In the past, the Information Planning Department handled incidents and collected information within the organization. Given the rapid increase in cyber attacks in recent years, however, necessary functions were independently consolidated as CSIRT in order to enhance and expand the emergency response structure.

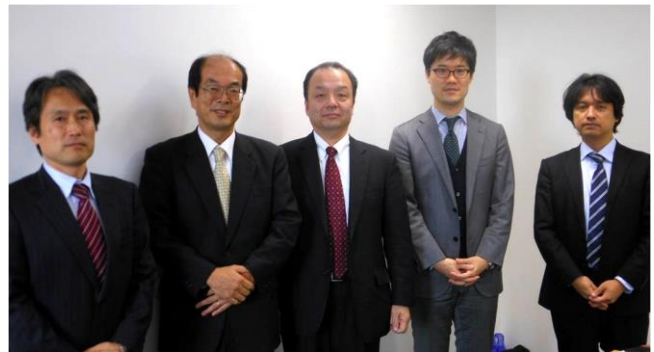


Fig. 1 T-SIRT representative: Toshihiko Tsuka (center)
 Point of contact: Tatsuya Kitamura (second from left)
 Other T-SIRT members

3.8.2. STRUCTURE AND AUTHORITY OF THE CSIRT

T-SIRT is an internal distributed CSIRT that is made up of members of the Information Planning Department, Corporate Planning Office and Taisei Information System (TAIS), a Group company that specializes in information systems. The IT section

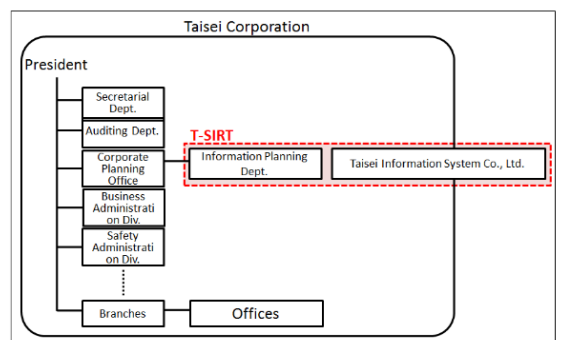


Fig. 2 T-SIRT Structure Chart

chief of the Information Planning Department is in charge of T-SIRT, whose members consist of team leaders of each group. T-SIRT focuses on preparing documents to eliminate any ambiguity over authority and scope of responsibility, which tend to become an issue in internal distributed CSIRTs.

At Taisei Corporation, there is an existing risk management structure, and T-SIRT activities are operated within an existing work flow. T-SIRT develops work procedures and rules for handling equipment, and provides guidance and cooperation on security-related matters within the company and to Group companies. In the event of a critical incident, the Manager of Information Planning Department is summoned as a member of the emergency response structure (CRO*⁸ administrative office). T-SIRT provides technical assistance and serves as a point of contact as part of this response structure.

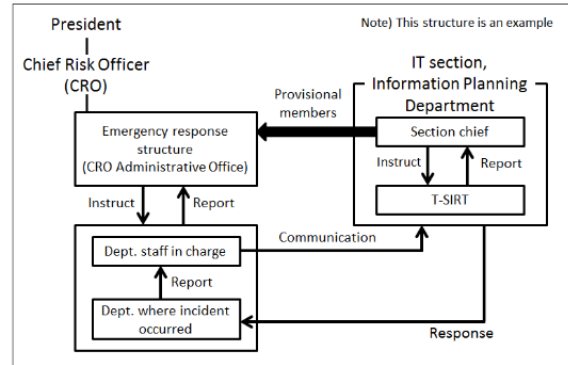


Fig. 3 Structure for Responding to Critical Incidents

3.8.3. OUTPUTS OF CSIRT ACTIVITIES

3.8.3.1. ACTIVITY REPORT TO MANAGEMENT

Activities are reported on weekly and annual bases. In weekly reports, information is shared with the Manager of Corporate Planning Office. In annual reports, security incidents such as lost PCs and the details of loss and damage, new information security measures, and employee education are summarized and reported to the Manager of Corporate Planning Officer and the Manager of General Affairs Department. The Manager of General Affairs Department supervises the risk management structure of Taisei Corporation.

3.8.3.2. DOCUMENTS ISSUED TOWARD AUDIENCES INSIDE AND OUTSIDE THE COMPANY

Annual reports for the management and security alerts for all employees are issued. In security alerts for all employees, incident cases that all employees should be mindful of are introduced, and technical details such as vulnerability information are not included.

3.8.3.3. METRICS FOR EVALUATING CSIRT ACTIVITIES

Although currently no quantitative metrics are set for evaluating T-SIRT activities, the management regards them in a generally favorable light, thanks in part to regular activity reports and daily information security

*⁸ CRO: Stands for Chief Risk Officer.

activities. Meanwhile, T-SIRT has been asking all employees to exercise caution in educational and awareness-raising opportunities, and as a result, the number of security incidents such as lost PCs and visiting websites unrelated to work has declined. This is considered one of the achievements of T-SIRT.

3.8.4. EDUCATION/TRAINING OF CSIRT MEMBERS

3.8.4.1. INCIDENT HANDLING EXERCISES

T-SIRT members take hands-on exercises provided by security vendors at least once a year. They also actively participate in exercise programs given by JPCERT/CC, TRANSITS Workshops*⁹ hosted by the NCA, and other events.

3.8.4.2. QUANTITATIVE METRICS FOR TECHNICAL SKILLS

No quantitative metrics exist for evaluating the technical skills of T-SIRT members. TAIS has a system for encouraging and evaluating the acquisition of official certifications.

3.8.4.3. HUMAN RESOURCES DEVELOPMENT

T-SIRT members participate in external training to increase their skills. Career paths are also prepared for the members.

3.8.5. REVIEW PERIOD OF STRUCTURE, SERVICES AND MANAGEMENT FUNCTIONS OF THE CSIRT

3.8.5.1. SERVICE RECIPIENTS AND SERVICES PROVIDED

T-SIRT optimizes the scope of services provided each year, considers an improvement plan, and puts necessary investments on the Information Planning Department's budget.

3.8.5.2. SECURITY POLICIES AND OTHER DOCUMENTS

Security policies and other documents are prepared by offices of the Information Planning Department. T-SIRT proposes revision of security policies and develops individual procedures such as incident response manuals based on security policies.

*⁹ TRANSITS Workshop: A workshop designed to provide training with the aim of promoting the establishment of CSIRTs and increasing the ability of existing CSIRTs to respond to incidents.

3.8.5.3. COMMUNICATION FLOW

Taisei Corporation always keeps its emergency communication flow and telephone directory up-to-date, and this communication flow is used to manage the flow of communication from T-SIRT when an incident occurs. Therefore, it is unlikely that members will not know whom to contact. The Public Relations Office, General Affairs Department, and internal telephone exchange are also notified of rules for escalation from outside parties.

3.8.5.4. INCIDENT MANAGEMENT

Although TAIS has a database for managing failure response, T-SIRT does not use any special management tools. The need for special-purpose management tools is urgently felt. Currently, for example, spreadsheet software is used to manage vulnerability response.

3.8.6. SUMMARY

Taisei Corporation uses IT to streamline operations, and it aims for proactive security measures from a management perspective with a view to business continuity (BCP, BCM, BIA). Therefore, it believes exchange of information with external organizations regarding IT and information security should be relatively easy. Accordingly, it actively participates in opportunities to exchange information with outside parties such as the NCA. Learning about the activities of external organizations provides opportunities to acquire knowledge and also exchange opinions about any concerns, which in turn helps CSIRT members to keep up and increase motivation.

3.9. INTERVIEW WITH YMC-CSIRT

YMC-CSIRT	
Organization Name	Yamaha Motor Co., Ltd.
Line of Business	Manufacturing business
CSIRT Structure	
Organizational Model	Internal distributed CSIRT
Number of Staff	8
Affiliation	Information Systems Department
Activities Budget	The budget is included in the Information System Department's activities expenses
Main Service Recipients	Yamaha Motor Co., Ltd. and its group companies around the world



3.9.1. OVERVIEW OF THE ORGANIZATION

Yamaha Motor is a major manufacturing company that manufactures and sells motorcycles, marine products such as boats and outboards, recreational vehicles such as snowmobiles, and various products both in Japan and abroad.



Fig. 1 YMC-CSIRT point of contact: Taku Harako (far right) and other YMC-CSIRT members

Yamaha Motor Corporation Computer Security Incident Response Team (YMC-CSIRT) handles incidents related to websites and systems for the Yamaha Motor Group companies around the world, in addition to collecting information and issuing alerts.

3.9.2. STRUCTURE AND AUTHORITY OF THE CSIRT

YMC-CSIRT was established in November 2013. Its members are those in charge of infrastructure operation and engineers of the Process & IT Division,

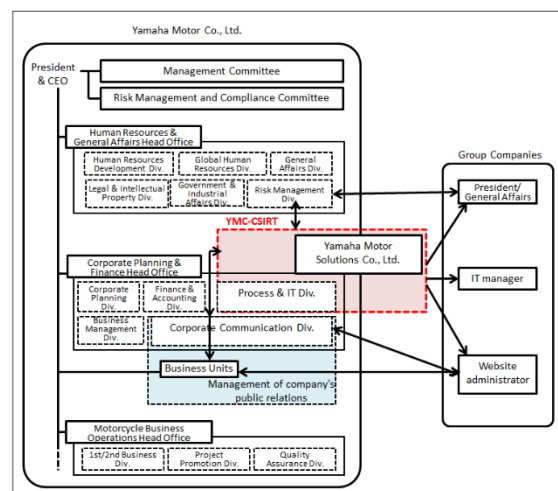


Fig. 2 YMC-CSIRT structure chart

Corporate Planning & Finance Head Office. Only one person is a full-time member of YMC-CSIRT; the other members serve concurrent duties for the Process & IT Division.

Yamaha Motor's Risk Management Division was established in about 2007 to provide internal control and risk management. YMC-CSIRT is also closely related to the Risk Management Division.

While the Risk Management Division has discretion to determine policies on how to respond to incidents, authority with regards to IT risks is vested in YMC-CSIRT. Security alerts and other countermeasure information are issued by YMC-CSIRT.

3.9.3. OUTPUTS OF CSIRT ACTIVITIES

3.9.3.1. ACTIVITY REPORT TO MANAGEMENT

The Risk Management Division reports information such as the number of incidents that occurred to the management. Incident information related to the products of over 100 Group companies are reported to the Risk Management Division, and YMC-CSIRT serves as the point of contact.

3.9.3.2. DOCUMENTS ISSUED TOWARD AUDIENCES INSIDE AND OUTSIDE THE COMPANY

There are no documents that are periodically issued toward audiences inside or outside the company.

3.9.3.3. METRICS FOR EVALUATING CSIRT ACTIVITIES

Targets such as an upper limit for the number of incidents are set as metrics for evaluating the activities of YMC-CSIRT. Whether the targets can be achieved depends on the trend of attack which varies significantly each year, so the evaluation of activities is not directly tied to budget requests.

3.9.4. EDUCATION/TRAINING OF CSIRT MEMBERS

3.9.4.1. INCIDENT HANDLING EXERCISES

YMC-CSIRT created a flow for responding to incidents in 2015. Currently, incident response and confirmation are performed according to this flow. As of now, incident handling exercises are not conducted.

3.9.4.2. QUANTITATIVE METRICS FOR TECHNICAL SKILLS

YMC-CSIRT does not yet have a system for evaluating the members' technical skills or recommending the acquisition of certification.

3.9.4.3. HUMAN RESOURCES DEVELOPMENT

YMC-CSIRT does not have education schemes or training systems such as clearly defined skill maps and career paths. However, human resources development is positioned as one of the issues to be tackled in the next three years. It plans to develop security experts with basic knowledge about IT including operating systems, and personnel who can handle internal coordination.

3.9.5. REVIEW PERIOD OF STRUCTURE, SERVICES AND MANAGEMENT FUNCTIONS OF THE CSIRT

3.9.5.1. SERVICE RECIPIENTS AND SERVICES PROVIDED

Process & IT Division reviews the details and recipients of services provided by YMC-CSIRT on an ongoing basis. YMC-CSIRT initially provided only services related to the company's websites. However, it currently actively handles information systems within the company, widening the scope of its services. Going forward, it will also consider expanding the range CSIRT services and adding PSIRT functions.

3.9.5.2. SECURITY POLICIES AND OTHER DOCUMENTS

Security policies and other documents are reviewed by the Risk Management Division. However, information security guidelines are created by YMC-CSIRT in order to keep them consistent with its handling of incidents.

3.9.5.3. COMMUNICATION FLOW

There is a companywide system for sharing the latest communication flow.

3.9.5.4. INCIDENT MANAGEMENT TOOLS

An incident management tool is introduced so that the status of response can be shared as needed. As a means of communication regarding incidents, a bulletin system is used in addition to email. Further, a system such as chat tool is used for optimizing information sharing even when the members are away from their desks.

3.9.6. SUMMARY

YMC-CSIRT has been able to smoothly operate from the high cooperativeness of the organization and high consciousness of collaboration, such as being able to discuss at early stage before reporting as an

incident from each business establishment. When the headquarters function is located in a local city, it tends to create a digital divide with those operating in a major city. To prevent this, YMC-CSIRT tries to improve literacy on information security by vigorously collecting cases and best practices of other organizations through NCA and other channels. In the security filed, it takes an approach of mutual cooperation, not competition, with other organizations by sharing best practices and working to change negative elements into positive ones.

4. MATTERS THAT SHOULD BE DEFINED AT THE TIME OF ESTABLISHMENT

Based on the results of the survey and interviews with these CSIRTs, the following six items were identified as matters that organizations should define if they decide to establish internal CSIRTs.

1. Scope of services provided by CSIRTs
2. Authority granted to CSIRTs
3. Deployment and members of CSIRTs
4. Point(s) of contact (PoC)
5. Reporting structure to effectively communicate the effects of CSIRT activities within the company
6. Periodic review of CSIRT activities

These will be introduced in order.

4.1. SCOPE OF SERVICES PROVIDED BY CSIRTs

Business activities, scale, departmental makeup, and anticipated risks differ according to the organization. For this reason, when establishing a CSIRT, the following items must first be considered.

- Services to be provided by the CSIRT, service level, service targets, and risk tolerance
- Scope of responsibility of the CSIRT, resources allocated to the CSIRT, and SLA*¹⁰
- Documented security policies of the organization and their approval by the management

As seen in the results of survey question 2.2.12, about 60% of the organizations had documented service definitions. The results of survey question 2.2.13 showed that over 80% of the organizations had documented security policies that were approved by the management.

The CSIRT Starter Kit*¹¹ provided by the NCA categorizes services offered by CSIRTs roughly into the following three types: reactive services, proactive services, and security quality control services. First, it is necessary to consider the situation that the organization is in, and then decide whether to provide all these services or only one or two of these.

Of the three categories of services, the services provided by many of the CSIRTs are as follows, according to the questionnaire:

*¹⁰ SLA: Stands for Service Level Agreement, and refers to an assurance of service quality and agreement on service level (definition, scope, details, goals to be achieved, etc.) concluded between the service provider and its users

*¹¹ CSIRT Starter Kit: <http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf>

- Reactive services
 - "Incident handling," "alerts," and other services to respond timely in the event of an incident

- Proactive services
 - "Intrusion detection" and other services to monitor for attack activities in normal times

- Security quality control services
 - "Educational activities," "security alerts," and other services to raise awareness about security within the organization
 - "Training" and other services aimed at increasing skills for incident response, etc.

The fact that these services are provided by many of the CSIRTs indicates that they serve the role of protecting their organization and reducing any possible damage. For these services, the risk management structure of the existing organization often provides a similar system, making them relatively easy to introduce. It is important to first launch these activities as the CSIRT's services, and then review and adjust the scope of services as appropriate to make it more suitable for the organization.

4.2. AUTHORITY GRANTED TO CSIRTs

In responding to security incidents, it is necessary as an organization to make appropriate decisions timely. To this end, the department or person responsible for decision-making should be determined in advance. CSIRTs are in a position to provide assistance to such departments or persons. The type of authority required for investigating and providing information for decision-making should be clearly defined.

For example, when a system needs to be suspended for risk avoidance in the event of an incident, the results of survey question 2.2.8 were as follows:

- CSIRT is granted authority to suspend the system: 12%
- CSIRT is not granted authority to suspend the system but can give guidance: 85%
- CSIRT is not granted authority to suspend the system, nor can it give guidance: 3%

The interview results show that CSIRTs do not necessarily need to have such powerful authority as the authority to suspend systems to function effectively as CSIRTs.

In addition, the results of survey question 2.2.12 show that about 60% of the organizations have documented definitions of the authority of the CSIRTs and incidents. Since CSIRTs often perform investigations in concert with other departments, having documented rules that define the authority on the extent to which investigations may be performed and decisions made within the organization ensures that

CSIRTs can provide the defined services smoothly and appropriately when an incident occurs.

4.3. DEPLOYMENT AND MEMBERS OF CSIRTs

If members of CSIRTs are thoroughly familiar with the systems within the organization and also knowledgeable about security, they will be able to respond quickly and appropriately when an incident occurs. Therefore, by deploying CSIRTs in departments that facilitate investigations, etc., in the event of an incident, and assigning suitable members, companies can ensure their CSIRTs can operate effectively.

Responses to survey questions 2.1.1 (Department(s) that led the establishment) and 2.2.1 (Department(s) where the CSIRT was deployed) show that in many organizations, information system management and security departments tended to lead the establishment of CSIRTs, or be chosen as the departments in which to deploy the CSIRTs. Presumably, this is because departments that maintain systems and equipment and deal with security matters as part of their normal operations were chosen as the place to deploy CSIRTs. However, the departments that host CSIRTs do not necessarily have to be such departments. They can also be deployed in departments that would make it easy to cooperate with other departments in providing the defined services.

Although answers to survey question 3.1 show that 80% of the CSIRTs are made up only of regular employees, not all the members have to be regular employees. We believe there is no problem in hiring support staff from external contractors as members of CSIRTs, as long as they sign a nondisclosure agreement and facilitate CSIRT activities.

4.4. POINT(S) OF CONTACT (PoC)

If vulnerabilities were found in services provided by an organization, or if fraudulent communications were directed toward external networks, security-related reports may be received from external organizations. In order to receive such reports or requests accurately and respond timely, points of contact (PoCs) must be set up within CSIRTs and then made public, and an escalation flow must be established to ensure reported information is directed toward appropriate departments.

For example, results of survey question 2.4.1 show that most organizations have rules for escalation to the management, as well as points of contact:

- Rules for escalation to management are clearly defined and documented: 77%
- Rough standards exist for escalation to management, but there are no clearly defined and documented rules: 20%

- Rules are not defined and are considered on an ad hoc basis: 1.5%
- No response: 1.5%

Results of survey question 2.2.5 indicate that many of the interviewed organizations participate in a framework for information sharing such as the NCA. Some of the respondents have also said that acquiring knowledge and sharing insight help keep up the motivation of CSIRT members.

In addition to receiving information about cyber threats including vulnerabilities and incident-related information, PoCs are expected to play a role in sharing information with other organizations as well.

For this reason, individuals with excellent communication skills are desirable for PoCs. PoCs who are able to communicate effectively can not only collect a wide range of information but also obtain more detailed information about attack methods and their countermeasures. By building relationships of trust both within and outside the organization, PoCs will be able to further broaden their network of information sources through their activities.

4.5. REPORTING STRUCTURE OF CSIRT ACTIVITIES TO EFFECTIVELY BE ACKNOWLEDGED BY THE COMPANY

Reporting and introducing CSIRT activities within the organization help raise awareness of organization members and gain trust in the CSIRT. That in turn will facilitate its activities through increased cooperation from outside, such as more reports coming in about early signs of incidents.

Results of survey question 2.7.1 reveal that about half of the organizations issue periodic reports, many of which are directed toward related departments or general readership within the company.

Further, results of survey question 2.4.9 show that about half of the organizations have a system for periodically reporting CSIRT activities to an information security committee, etc., including the management. One of the organizations interviewed said that it regularly compiles reports on matters related to the industry and the impact of legislation, and submit them to the management as appropriate.

In some organizations, CSIRT activities are only seen as a cost center and not given a fair evaluation. This sometimes makes it difficult to secure enough budget to provide continued services, develop human resources, and make further improvements. Even under such circumstances, reporting the results of its activities and their cost-reducing effects to the management and to audiences both in and outside the company will help gain an understanding of the value of CSIRT activities. This can be done, for example, by:

- Performing risk assessment in advance for incidents that can be anticipated.
- Estimating the amount of time saved in resolving incidents after their occurrence.

- Evaluating the amount of handling costs that were reduced based on risk assessment.

It is important to communicate that CSIRT activities benefit the organization and are an effective investment. By evaluating the activities as quantitatively as possible, the value of the CSIRT can be communicated more effectively to the management and others both in and outside the company. In this survey, there was also an organization that calculates and reports the estimated value of damage that would be caused if incidents were not handled based on evaluation metrics defined by the JNSA*¹².

4.6. PERIODIC REVIEW OF CSIRT ACTIVITIES

There may be cases in which incidents can no longer be handled appropriately with existing definitions of CSIRT services and authority, due to factors such as new trends in cyber attacks, technological developments, and changes in the organization's business activities. To prevent this, it is important to periodically review services and the structure for CSIRT activities.

Results of survey questions 2.6.1, 2.6.2, and 2.6.3 show that many of the CSIRTs review the structure for their activities at least once a year. Interview results reveal that reviews cover various elements including services, structures, and authority. CSIRTs that were established recently said they were satisfied with their current functions and services but they intend to review them in the future.

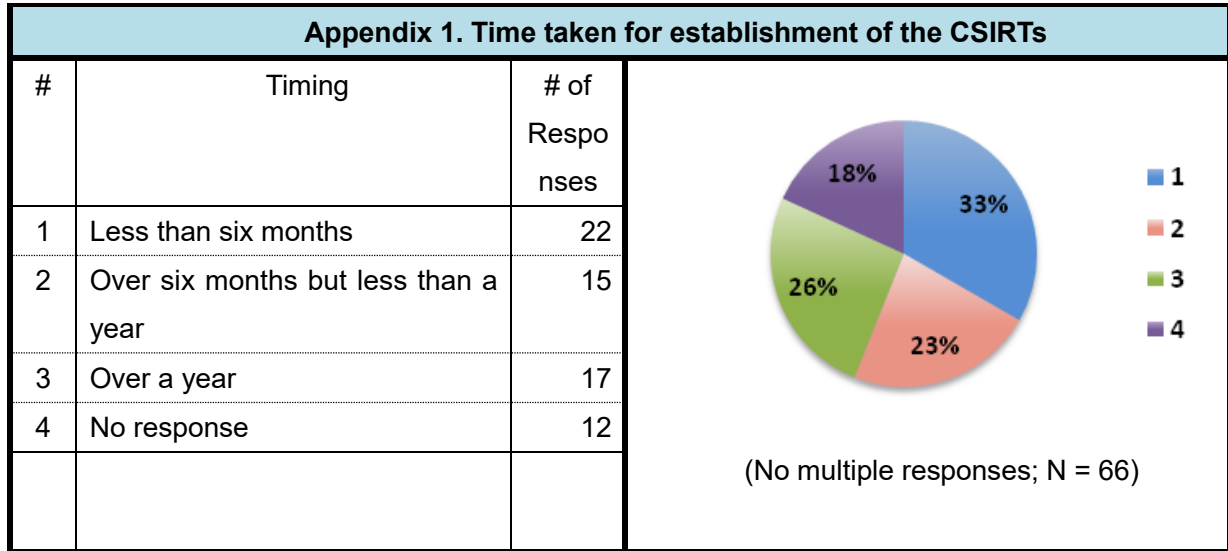
In general, organizations have periodic personnel transfers, and the same applies to CSIRTs as well. When members change, CSIRTs may no longer be able to maintain the same level of services as before. Therefore, it is important to define the members' skill sets and to assign appropriate members in order to maintain the required service level. By quantitatively measuring skill levels, the need to train members, provide an environment for training, and secure the necessary budget can be communicated effectively to the management.

According to the results of survey question 3.4, only a few of the organizations define the necessary skill sets. In the interviews, many organizations responded that they were considering to establish a system for education and training, given the broad range of skills required of CSIRT members, including knowledge about security and their organizations' business activities as well as presentation skills. It appears that many organizations regard quantitative evaluation of skills as a major issue from the perspective of training members as well.

*¹² "Survey Report on Information Security Incidents" (<http://www.jnsa.org/result/incident/>) published by the Japan Network Security Association (JNSA)

APPENDIX 1. TIME TAKEN FOR ESTABLISHMENT OF THE CSIRTs

The time taken for the establishment of the CSIRTs was calculated based on the results of survey questions 2.1.5 and 2.1.6. We found that a majority of the teams established their CSIRTs in less than a year.



Of the 22 organizations that established their CSIRTs in less than six months, 15, or about 70%, were established relatively recently in 2014 or later. This may have been due to a heightened interest in security among the management, helping facilitate coordination. Knowledge about CSIRTs accumulated through the NCA's activities and shared with the management may also have played a part. Organizations are expected to take measures against cyber attacks at an early stage. We advise organizations to properly define necessary matters within the organization and consider the time it takes to document them as they prepare to establish their CSIRTs.

APPENDIX 2. REALATIONSHIP BETWEEN DEPARTMENTS THAT CSIRTs BELONG TO AND SERVICES THEY PROVIDE

We analyzed the correlation between the departments that CSIRTs belong to and the services they provide. In many of the services, no major difference was observed in the ratio between in-house and outsourced operations for providing the services. However, when the departments where CSIRTs are deployed were categorized into the following two types, differences were seen in the ratio for some of the services. It should be noted that this analysis does not include cross-departmental CSIRTs between information system management and security departments.

- Belongs to an information system management department but not to a security department

Average number of members: 11.6

Characteristics seen in the ratio between in-house and outsourced operations for services provided by the CSIRTs:

- Many of the organizations that provide malware analysis services outsource certain operations
- In forensics services the ratio between in-house and outsourced operations is about the same

- Belongs to a security department but not to an information system management department

Average number of members: 13.0

Characteristics seen in the ratio between in-house and outsourced operations for services provided by the CSIRTs:

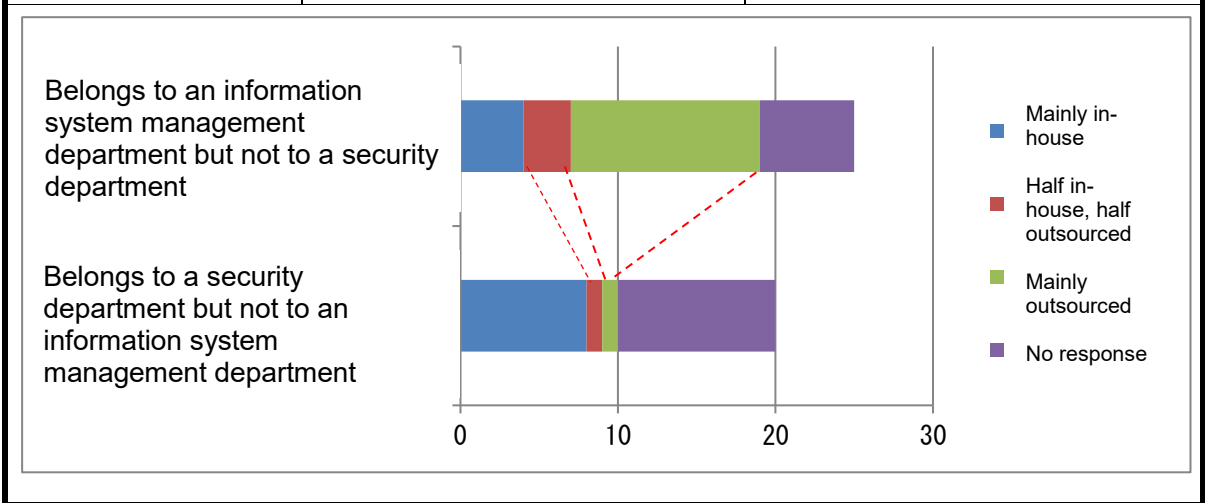
- Many of the organizations that provide malware analysis services handle operations in-house
- In forensics services the ratio of operations that are outsourced is low

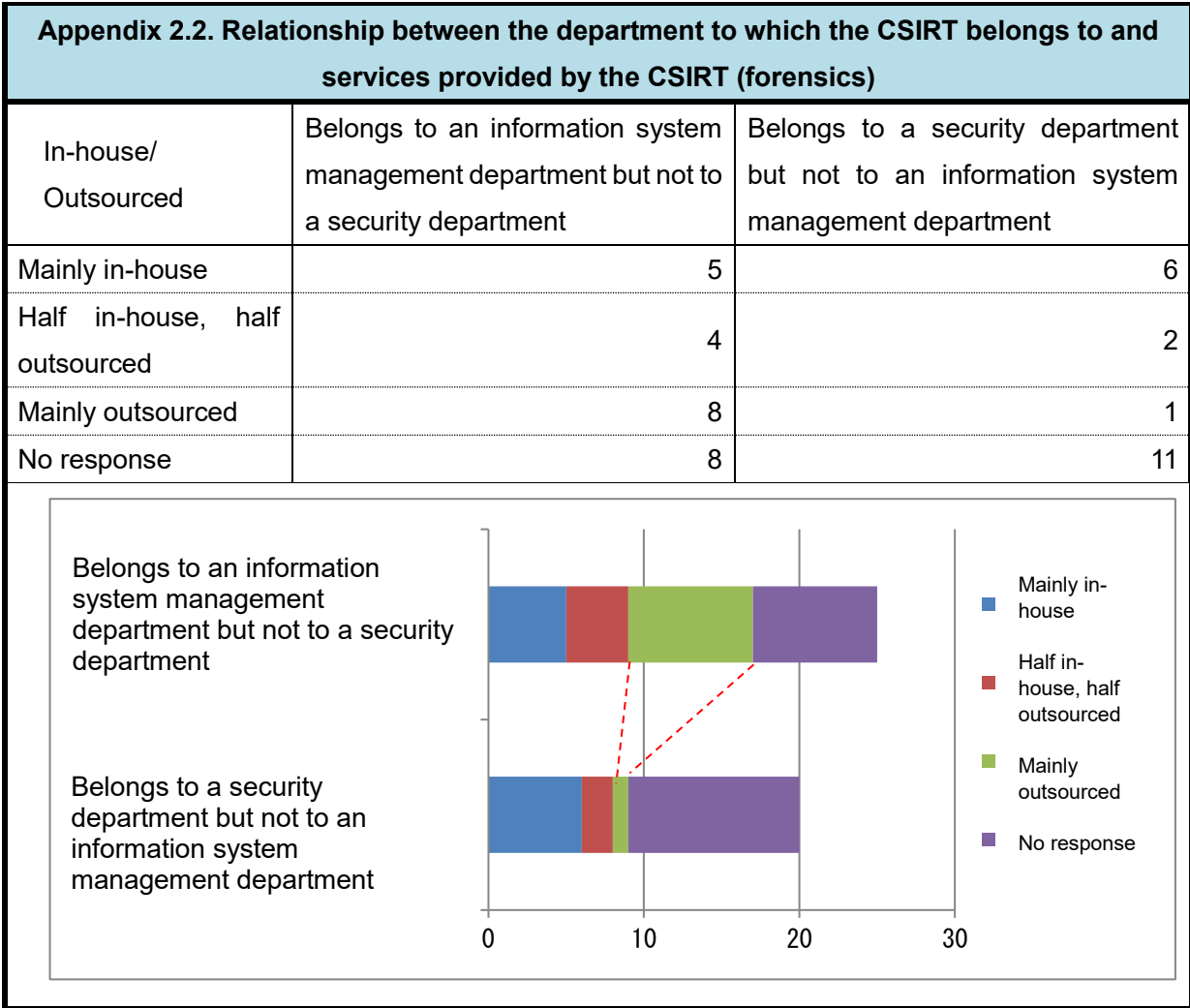
Results of this analysis show that some of the departments where CSIRTs are deployed and the services provided by the CSIRTs have certain characteristics. This may be because the departments to establish the CSIRTs were chosen to provide certain services.

For CSIRTs to provide services defined within their organizations, it is effective to choose necessary methods without being concerned about whether operations should be handled in-house or outsourced.

Appendix 2.1. Relationship between the department to which the CSIRT belongs and services provided by the CSIRT (malware analysis)

In-house/ Outsourced	Belongs to an information system management department but not to a security department	Belongs to a security department but not to an information system management department
Mainly in-house	4	8
Half in-house, half outsourced	3	1
Mainly outsourced	12	1
No response	6	10





5. IN CONCLUSION

As stated in the previous chapter, this survey points to six items that should be defined at the time of establishing an internal CSIRT. However, although these items are minimum required conditions for operating an internal CSIRT, it does not necessarily mean that fulfilling these conditions will ensure its activities live up to the expectations of the organization. In order for an internal CSIRT to function effectively, it is extremely important that the team shares information and cooperates with other departments within the organization and/or other CSIRTs, etc., outside the organization. In this chapter, we will share some relevant insights we gained through interviews in this survey.

Some of the CSIRTs we interviewed told us that while they were hampered in their efforts to share information and respond to incidents due to a lack of cooperation and understanding from related departments in the company, they were able to build a solid trust relationship by repeatedly providing training through exercises involving related departments, and expanding the scope of these activities to include a greater part of the organization.

The importance of building trust relationships with the CSIRTs of other organizations was also pointed out by some of those interviewed. They spoke of how participating in the NCA and other community activities, sharing information about cases of incident response within their organizations, and actively exchanging opinions about and sharing insights into CSIRT activities with other organizations provided opportunities to reframe how they interact with their organizations. We believe that willingly sharing information about how improvements were made within one's organization with other organizations help foster a relationship of trust, and promote further exchange of information. Cooperation among CSIRTs will further invigorate CSIRT activities within the entire country and in turn lead to the growth of individual CSIRTs.

For organizations considering launching their own CSIRTs for the first time, it may be too heavy a burden to define all six items mentioned in the previous chapter. However, few organizations were able to define the six items flawlessly from the start. We encourage those organizations new to an internal CSIRT to start small. These definitions do not need to be perfect at first. Referring to the examples of CSIRTs in other organizations should be helpful. Then, through day-to-day operations including exercises and training, sharing of information with their counterparts in other organizations, and also responding to actual incidents, newly established CSIRTs should accumulate technical insights and experience required for a CSIRT, and develop into a trusted and indispensable part of the organization. We hope that this report will serve as a guide in that effort.