



Version 2.1

TLP:WHITE

2019 □ 11 □

□ □ □ □ □ □ □ □ □ □ □ □ **CSIRT** □

□ □ □ □

□ □ **2.1**





□ □

<b>1</b>	□ □	<b>7</b>
<b>2</b>	□ □ □ □ □	<b>7</b>
<b>3</b>	<b>CSIRT</b> □ <b>PSIRT</b> □ □ □ □ □	<b>9</b>
<b>4</b>	<b>CSIRT</b> □ □ □ □ □ □	<b>9</b>
<b>5</b>	□ □ □ □ □ □ □ □ □ □ □ □	<b>12</b>
<b>5.1</b>	□ □ □ □ □ □ □ □	<b>13</b>
5.1.1	□ □ □ □ □ □ □ □ □ □ □ □	13
5.1.2	□ □ □ □ □ □ □ □ □ □	13
5.1.3	□ □ □ □ □ □ □ □ □ □	14
<b>5.2</b>	□ □ □ □ □ □ □ □	<b>14</b>
5.2.1	□ □ □ □ □	14
5.2.2	□ □ □ □ □	14
<b>6</b>	□ □ □ □ □ □ □ □ □ □ □ □ □ □	<b>15</b>
<b>6.1</b>	□ □ □ □ □ □ □ □ □ □ □ □ □ □	<b>15</b>
6.1.1	□ □ □ □ □ □ □ □ □ □ □ □ □ □	16
6.1.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □	17
<b>6.2</b>	□ □ □ □ □ □ □ □ □ □ □ □	<b>17</b>
6.2.1	□ □	18
6.2.2	□ □ □ □ □ □ □ □	18
6.2.3	□ □ □ □ □ □ □ □ □ □ □ □	19
6.2.4	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	19
6.2.5	□ □ □ □ □ □ □ □ □ □ □ □	19
<b>6.3</b>	□ □ □ □ □ □ □ □ □ □ □ □ □ □	<b>20</b>
6.3.1	□ □ □ □ □ □ □ □ □ □ □ □ □ □	21
6.3.2	□ □ □ □ □ □ □ □ □ □ □ □	21
6.3.3	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	22
6.3.4	□ □ □ □ □ □ □ □ □ □ □ □	22
<b>6.4</b>	□ □ □ □ □ □ □ □ □ □ □ □	<b>23</b>
6.4.1	□ □ □ □ □ □ □ □ □ □ □ □ □ □	24
6.4.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	24
6.4.3	□ □ □ □ □ □ □ □ □ □ □ □	25



6.4.4	□ □ □ □ □ □ □ □ □ □ □ □ □ □	25
<b>6.5</b>	□ □ □ □ □ □ □ □ □ □ □ □	<b>26</b>
6.5.1	□ □ □ □ □	26
6.5.2	□ □ □ □ □ □ □ □	27
6.5.3	□ □ □ □ □ □ □ □ □ □	27
6.5.4	□ □ □ □ □ □ □ □	28
6.5.5	□ □ □ □ □ □	28
6.5.6	□ □ □ □ □ □ □ □	28
<b>6.6</b>	□ □ □ □ □ □ □ □ □ □	<b>29</b>
6.6.1	□ □ □ □ □ □ □ □ □ □ □ □ □ □	29
6.6.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □	29
6.6.3	□ □ □ □ □ □ □ □ □ □ □ □ □ □	30
<b>7</b>	□ □ □ □ □ □ □ □ □ □	<b>30</b>
<b>7.1</b>	□ □ □ □ □ □ □ □ / □ □	<b>31</b>
7.1.1	□ □ □ □ □ □ □ □ □ □ □ □ □ □	31
7.1.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □	32
7.1.3	□ □ □ □ □ □ □ □ □ □	32
<b>7.2</b>	□ □ □ □ □ □ □ □ □ □ □ □	<b>32</b>
7.2.1	□ □ □ □ □ □ □ □ □ □ □ □ □ □	33
7.2.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	33
<b>7.3</b>	□ □ □ □ □ □ □ □ □ □	<b>34</b>
7.3.1	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	34
7.3.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	34
7.3.3	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	35
<b>7.4</b>	□ □ □ □ □ □ □ □ □ □	<b>35</b>
7.4.1	□ □ □ □ □ □ □ □ / □ □ □ □	35
7.4.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	36
<b>7.5</b>	□ □ □ □ □ □ □ □ □ □	<b>36</b>
7.5.1	□ □	36
7.5.2	□ □ □ □ □ □ □ □ / □ □ □ / □ □ □ □	37
7.5.3	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	37
<b>7.6</b>	□ □ □ □ □ □ □ □ □ □	<b>37</b>
7.6.1	□ □ □ □ □ □ □ □ / □ □ □ □ □ □	38
7.6.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	38
<b>8</b>	□ □ □ □ □ □ □ □ □ □	<b>39</b>
<b>8.1</b>	□ □ □ □ □ □ □ □ □ □	<b>39</b>

8.1.1	□ □ □ □ □ □ □ □ □ □ □ □	40
8.1.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	40
8.1.3	□ □ □ □ □	41
8.1.4	□ □ □ □ □ □ □ □ □ □	41
<b>8.2</b>	<b>□ □ □ □ □ □ □ □</b>	<b>42</b>
8.2.1	□ □ □ □ □ □ □ □	42
8.2.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □ / □ □ □ □	42
8.2.3	□ □ □ □ □ □ □ □ □ □ □ □ □ □	43
8.2.4	□ □ □ □ □ □ □ □	43
<b>8.3</b>	<b>□ □ □ □ □</b>	<b>43</b>
8.3.1	□ □ □ □ □ □ □ □ □ □ □ □	44
8.3.2	□ □ □ □ □ □ □ □ □ □	44
8.3.3	□ □ □ □ □ □	44
8.3.4	□ □ □ □ □ □ / □ □ □ / □ □ □ □ □ □	44
8.3.5	□ □ □ □ □ □ □ □ □ □ □ □	45
8.3.6	□ □ □ □ □ □	45
<b>9</b>	<b>□ □ □ □ □ □ □ □ □ □</b>	<b>46</b>
<b>9.1</b>	<b>□ □ □ □ □ □ □ □</b>	<b>46</b>
9.1.1	□ □ □ □ □ □ □ □ □ □ □ □	46
9.1.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □	47
9.1.3	□ □ □ □ □ □ □ □ □ □	47
9.1.4	□ □ □ □ □ □	47
<b>9.2</b>	<b>□ □ □ □ □ □ □ □ □ □</b>	<b>47</b>
9.2.1	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	48
9.2.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □	48
9.2.3	□ □ □ □ □ □ □ □ □ □	48
9.2.4	□ □ □ □ □ □ □ □	49
9.2.5	□ □ □ CSIRT □ □ □ □ □ □ □ □	49
<b>9.3</b>	<b>□ □ □ □ □ □</b>	<b>49</b>
9.3.1	□ □ □ □ □ □ □ □ □ □	50
9.3.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □	50
9.3.3	□ □ □ □ □ □ □ □ □ □	50
9.3.4	□ □ □ □ □ □ □ □ □ □	51
9.3.5	□ □ □ □ □ □ □ □ □ □ □ □	51
<b>9.4</b>	<b>□ □ □ □ □ □ □ □ □ □ □ □</b>	<b>51</b>
9.4.1	□ □ □ □ □ □ □ □ □ □ □ □	52
9.4.2	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	52



9.4.3 □ □ □ □ □ □ □ □ 52

9.4.4 □ □ □ □ □ □ □ □ 52

□ □ **1** □ □ □ □ **54**

□ □ **2** □ □ □ □ □ □ □ □ **ERROR! BOOKMARK NOT DEFINED.**

□ □ **3** □ □ □ □ □ □ □ □ **55**

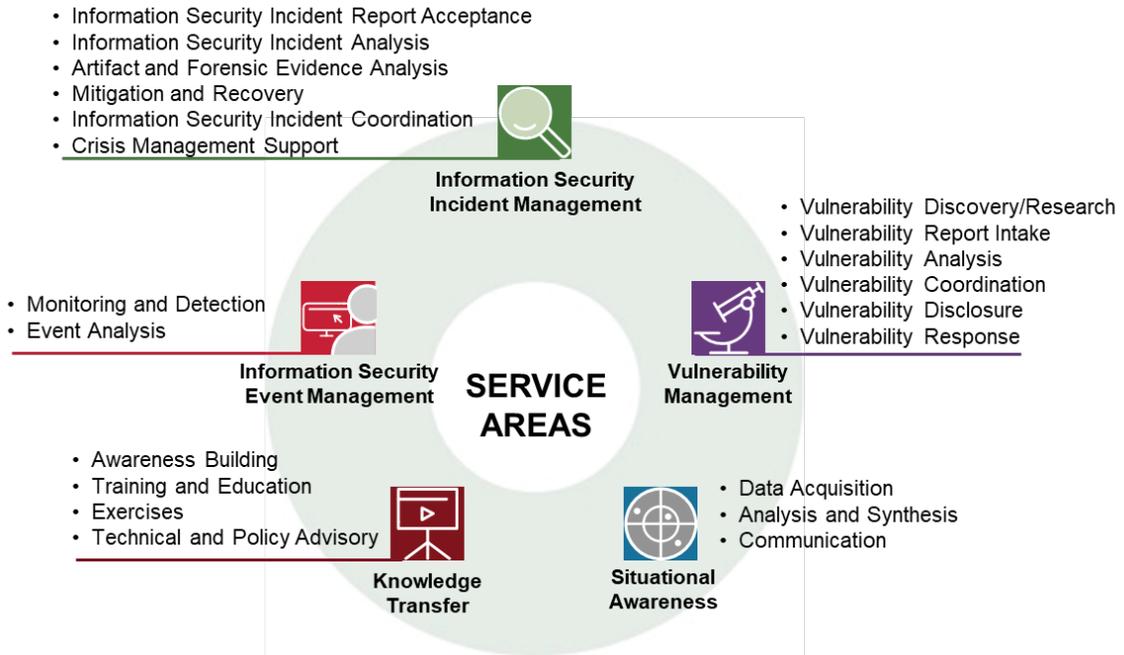
□ □ **4** □ □ □ □ **CSIRT** □ □ □ □ □ □ □ □ □ □ □ □ □ □ **60**











□ □ □ □ □

Service areas □ □ □ □

Information Security Event Management □ □ □ □ □ □ □ □

Monitoring and detection □ □ □ □ □

Event analysis □ □ □ □ □

Information Security Incident Management □ □ □ □ □ □ □ □

Information security incident report acceptance □ □ □ □ □ □ □ □ □ □

Information security incident analysis □ □ □ □ □ □ □ □

Artifact and forensic evidence analysis □ □ □ □ □ □ □ □ □ □

Mitigation and recovery □ □ □ □ □

Information security incident coordination □ □ □ □ □ □ □ □

Crisis management support □ □ □ □ □ □ □

Vulnerability Management □ □ □ □ □









CSIRT “ ” CSIRT

CSIRT

5

- Error! Bookmark not defined.
- Error! Bookmark not defined.

### 6.1.1

ISAC CSIRT / / / / /

- CSIRT
- 

<sup>5</sup> CSIRT /





- [Redacted]
- [Redacted]  
[Redacted]  
[Redacted] / [Redacted]
- [Redacted]  
[Redacted]  
[Redacted]
- [Redacted]  
[Redacted]
- [Redacted]  
[Redacted]

### 6.2.3 [Redacted]

[Redacted]

[Redacted] CSIRT  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]

### 6.2.4 [Redacted]

[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]

[Redacted] CSIRT [Redacted]  
[Redacted] CSIRT [Redacted]  
[Redacted]

### 6.2.5 [Redacted]

[Redacted]  
[Redacted]









### 6.4.1 [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted] CSIRT [Redacted] “ [Redacted] ” [Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

### 6.4.2 [Redacted]

[Redacted] / [Redacted]

[Redacted]

[Redacted]



[Redacted text block]

[Redacted text block]

[Redacted text block]

- [Redacted list item]

### 6.4.3 [Redacted section header]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]

### 6.4.4 [Redacted section header]

[Redacted text block]



   CSIRT   

### 6.5

CSIRT   

          CSIRT   

- 
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- 
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

#### 6.5.1

      CSIRT    CSIRT







Placeholder text for the first paragraph.

Placeholder text for the second paragraph.

### 6.6.3 Placeholder text

Placeholder text for the first line of section 6.6.3.

Placeholder text for the second line of section 6.6.3, including the word CSIRT.

Placeholder text for the third line of section 6.6.3, including the word CSIRT.

Placeholder text for the fourth line of section 6.6.3, including the word CSIRT.

## 7 Placeholder text

Placeholder text for the first line of section 7.

Placeholder text for the second line of section 7, including the word CSIRT.

Placeholder text for the third line of section 7.

- Error! Bookmark not defined.



CSIRT /

7.1

CSIRT

CSIRT CSIRT 6 CSIRT

CSIRT

- 
- 
- 

PSIRT CSIRT

7.1.1

6 CSIRT





### 7.3 [redacted]

[redacted]

[redacted]

[redacted] CVD<sup>7</sup> [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

#### 7.3.1 [redacted]

[redacted]

[redacted] CSIRT [redacted]

[redacted] CSIRT [redacted]

[redacted]

#### 7.3.2 [redacted]

[redacted]

[redacted] CSIRT [redacted] PSIRT [redacted] PSIRT [redacted]

<sup>7</sup> [redacted] CVD [redacted]





CSIRT CVD CSIRT

CVD

7.5.2

CVSS

7.5.3

CSIRT

7.6

8 CSIRT







- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

### 8.1.3 [Redacted]

[Redacted] / [Redacted] CSIRT [Redacted]

[Redacted]  
[Redacted] CSIRT [Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]

### 8.1.4 [Redacted]

[Redacted] CSIRT [Redacted]

[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted] IP [Redacted]  
[Redacted] / [Redacted]  
[Redacted]  
[Redacted]













9.1.2 [redacted]

[redacted]

[redacted]

[redacted] CSIRT [redacted]

9.1.3 [redacted]

[redacted]

[redacted] CSIRT [redacted]

[redacted] CSIRT [redacted]

9.1.4 [redacted]

[redacted] CSIRT [redacted]

[redacted] CSIRT [redacted] CSIRT [redacted]

[redacted]

9.2 [redacted]

[redacted] CSIRT [redacted] CSIRT [redacted]

[redacted] CSIRT [redacted]

- [redacted]
- [redacted]
- [redacted] CSIRT [redacted]
- [redacted]















## 附件 2：术语和定义

本节定义了 CSIRT 服务框架中使用的某些术语。

**行动 (Action)** - 描述如何在不同的详细程度上完成某件事情。

**通报 (Advisory)**<sup>9</sup> - 用于通知、建议和警告产品漏洞的公告或简报。

**能力 (Capability)** - 可以作为一组织的作用和职责的一部分来开展的一种可度量的活动。对于 FIRST 服务框架而言，能力可以定义为更广泛的服务，也可以定义为必备的功能。

**容量 (Capacity)** - 一组织在达到某种形式的资源耗尽之前，能够履行某种特定能力的并发进程的数量。

**常见漏洞陈列 (Common Vulnerability Exposures) (CVE)**<sup>10</sup> - 条目列表，其中包含一个标识号、一个描述和至少一个有关公开已知漏洞的公共参考。用作参考漏洞的标准标识符。

**常见漏洞评分系统 (Common Vulnerability Scoring System) (CVSS)**<sup>11</sup> - 反映漏洞严重程度的一计分系统。

**常见漏洞枚举 (Common Weakness Enumeration) (CWE)**<sup>12</sup> - 创建的软件弱点类型的正式列表，用作用于描述架构、设计或代码中软件安全弱点的一种通用语言；用作针对这些弱点的软件安全工具的标准衡量尺度；并为弱点识别、缓解和预防工作提供一个通用的基线标准。

**服务对象 (Constituency)** - 可以获取 CSIRT 提供的一组特定服务的特定人群和/或组织。

**情境数据源 (Contextual Data Source)** - 情境数据源旨在为数据点提供情境，例如，身份、资产或信息安全事件。具体示例包括用户数据库、资产清单、IP 否认服务或威胁情报数据。

**协调漏洞披露 (Coordinated vulnerability disclosure)** - 一个用于表示包括协调在内的披露过程的术语。来源：ISO/IEC 29147:2018，术语和定义。

**协调员 (Coordinator)**<sup>13</sup> - 一个可选的参与者，可协助供应商和搜寻者来处置和披露漏洞信息。

**检测用例 (Detection Use Case)** - 有待信息安全事件管理服务区检测的一个特定条件。该术语源于软件工程，但现已广泛用于检测工程。

**禁令 (Embargo)** - 坚持不发布漏洞详情，直至受影响的供应商能够发布安全更新程序或缓解措施以及应变方法来保护客户。

**搜寻者 (Finder)**<sup>14</sup> - 识别产品或在线服务中潜在漏洞的个人或组织。请注意：搜寻者可以是研究人员、报告人、安全公司、黑客、用户、政府或协调员。

<sup>9</sup> ISO/IEC 29147:2014 □□□□ - □□□□ - □□□□ - □□ / □□ 3.1

<sup>10</sup> <https://cve.mitre.org/>

<sup>11</sup> <https://www.first.org/cvss/>

<sup>12</sup> <https://cwe.mitre.org/about/index.html>

<sup>13</sup> ISO/IEC 30111:2013 □□□□ - □□□□ - □□□□ - □□ / □□ 3.1

<sup>14</sup> ISO/IEC 29147:2014 □□□□ - □□□□ - □□□□ - □□ / □□ 3.3

**功能 (Function)** - 旨在实现某特定服务目的的一项或一组活动。其他定义包括：一组相关的行动；<sup>15</sup>执行某项指定的行动或活动、工作、操作。<sup>16</sup>

**信息安全事件 (Information Security Event)** - 在信息技术环境中可观察到的、与安全相关的事件；例如，用户登录或入侵检测 (IDS) 告警。信息安全事件通常会产生某种证据，例如，一条审计记录或日志文件中的一个条目，作为信息安全事件管理服务区的一部分，进行收集和分析这些信息。

**信息安全事故 (Information Security Incident)**<sup>17</sup> - 指示用户、系统、组织和/或网络信息安全某些方面受到损害的、任何不利的信息安全事件 (或信息安全事件集)。信息安全事故的定义在组织与组织之间可能有所不同，但通常至少以下类别是适用的：

- 失去信息保密性
- 损害信息完整性
- 拒绝服务
- 滥用服务、系统或信息
- 系统损坏

攻击，即使因适当的保护而失败，也可以视为信息安全事故。

**关键绩效指标 (Key Performance Indicator) (KPI)**<sup>18</sup> - 一个可度量的值，用于表明公司有效实现关键业务目标的能力。组织在多个层面上使用关键绩效指标来评估其在达成目标方面的成就。

**成熟度 (Maturity)** - 指的是一个组织在其使命和授权范围内如何有效地履行特定能力，它是在执行特定功能或者功能或服务集的过程中能够达到的熟练程度，一个组织的能力将取决于已建立的策略和文档的范围和质量以及执行既定流程的能力。

**开源 (Open Source)** - 允许自由地重新分发和修改的软件作品，其中的源代码是公开可用的，可以自由分发，不歧视任何个人、团体或工作领域，且技术中立。开源软件通常由共同创建和维护它的个人和实体社群来维护。

**产品 (Product)**<sup>19</sup> - 一个为销售或免费提供而实施或开发的系统。

**修复 (或补救) (Remediation (or Remedy))**<sup>20</sup> - 对产品或在线服务进行的更改，以消除或缓解漏洞。修复通常采取二进制文件替换、配置更改或源代码修补和重新编译的形式进行。用于“修复”的不同术语包括补丁、修复、更新、修补和升级。缓解措施也称为应变方法或对策。

**负责任的披露 (Responsible Disclosure)** - 一个用于表示以下过程或模型的术语，在该过程或模型中，仅在补救措施 (修补程序或补丁程序) 变得可用的一段时间后才允许披露漏洞。该术语不一定等同“协调的漏洞披露”。

<sup>15</sup> Source: <https://www.merriam-webster.com/dictionary/function>

<sup>16</sup> Source: <https://www.dictionary.com/browse/function>

<sup>17</sup> RFC2350 “ ” “ ” <https://tools.ietf.org/html/rfc2350>

<sup>18</sup> <https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator>

<sup>19</sup> ISO/IEC 29147:2014 - / 3.5

<sup>20</sup> ISO/IEC 29147:2014 - / 3.6

**风险 (Risk)**<sup>21</sup> - “不确定性对目标的影响”。在该定义中，不确定性包括事件（可能发生或可能不发生）以及因含糊或信息缺乏而引起的不确定性。

**风险接受 (Risk Acceptance)**<sup>22</sup> - 指的是一种风险响应策略，项目团队据此来决定确认风险，除非风险发生，否则不采取任何行动。

**风险注册表 (Risk Register)**<sup>23</sup> - 用于记录风险分析结果和风险响应计划的文档。

**服务 (Service)** - 一项服务指的是针对某特定结果的一组可识别的、一致的功能。此类结果可能是服务对象或代表某实体的利益攸关方或为某实体的利益攸关方所预期或要求的。

**服务水平协议 (Service Level Agreement) (SLA)** - 服务提供商（内部的或外部的）与最终用户之间的一个合同，用于定义期望从服务提供商处得到的服务水平。

**利益攸关方 (Stakeholders)**<sup>24</sup> - 定义和修改服务区或服务并确保适当的服务沟通策略的个人或团体，以及可以从提供的服务中受益的团体。

**任务 (Tasks)** - 完成某项特定功能必须执行的行动列表。

**供应商 (Vendor)**<sup>25</sup> - 开发产品或服务或负责其维护的个人或组织。

**漏洞 (Vulnerability)**<sup>26</sup> - 软件、硬件或在线服务中可以被利用的弱点。

---

<sup>21</sup> ISO 31000:2009/ ISO 73:2002 - / 2.1

<sup>22</sup> PMBOK

<sup>23</sup> PMBOK

<sup>24</sup>

<sup>25</sup> ISO/IEC 30111:2013 - / 3.7

<sup>26</sup> ISO/IEC 30111:2013 - / 3.8

## 附件 3 □ □ □ □ □

Alberts, David S., et.al. Understanding information age warfare. In *DOD Command and Control Research Program Publication Series*. ADA395859. Booz Allen & Hamilton, McLean, VA. 2001.  
<https://apps.dtic.mil/docs/citations/ADA395859>

Barford P., et al. (2010) Cyber SA: Situational Awareness for Cyber Defense. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) *Cyber Situational Awareness*. *Advances in Information Security*, vol 46. Springer, 2010. Boston, MA. ISBN 978-1-4419-0140-8\_1  
[https://link.springer.com/chapter/10.1007/978-1-4419-0140-8\\_1](https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_1)

Boyd, John R. *Destruction and Creation*. Goal Systems International. September 3, 1976.  
[http://www.goalsys.com/books/documents/DESTRUCTION\\_AND\\_CREATION.pdf](http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf)

Cartwright, James E. Joint Concept of Operations for Global Information Grid NetOps. *United States Strategic Command*. PDF August 10, 2005. Homeland Security Digital Library. August 10, 2005.  
<https://www.hsdl.org/?view&did=685398>

Committee on National Security Systems Instruction CNSSI 4009. *Committee on National Security Systems Website*. June 23, 2019 [accessed].  
<https://www.cnss.gov/cnss/>

Cybersecurity Situation Awareness. *The MITRE Corporation Website*. June 25, 2019 [accessed].  
<https://www.mitre.org/capabilities/cybersecurity/situation-awareness>

Endsley, Mica R. Toward a theory of situation awareness in dynamic systems. *Human factors* Volume 37. Number 1. March 1995 Pages 32-64.  
<https://journals.sagepub.com/doi/10.1518/001872095779049543>

FIRST *Product Security Incident Response Team (PSIRT) Services Framework*, Version 1.0, 2018. North Carolina: First.org, 2018  
[https://www.first.org/education/FIRST\\_PSIRT\\_Service\\_Framework\\_v1.0](https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0)

FIRST Vulnerability Reporting and Data eXchange SIG (VRDX-SIG). 2013-2015. North Carolina: First.org, 2015  
<https://www.first.org/global/sigs/vrdx/>

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure, Version 1.0, 2017. North Carolina: First.org, 2017  
<https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0>

Hawk, Robert. Situational Awareness in Cyber Security. [blog post]. *Hawk's Posts: Security Essentials from Robert Hawk*. June 11, 2015.  
<https://www.alienvault.com/blogs/security-essentials/situational-awareness-in-cyber-security>

Householder, Allen D.; Wassermann, Garret; Manion, Art; King, Christopher. *The CERT® Guide to Coordinated Vulnerability Disclosure*. CMU/SEI-2017-SR-022. Software Engineering Institute, Carnegie Mellon University. 2017  
<https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330>

Householder, Alan. Vulnerability Discovery for Emerging Networked Systems [blog post]. *Vulnerability discovery techniques*. November 20, 2014.

<https://insights.sei.cmu.edu/cert/2014/11/-vulnerability-discovery-for-emerging-networked-systems.html>

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability disclosure*. Second Edition. ISO/IEC 29147:2018. Geneva, Switzerland: ISO: IEC. 2018

<https://www.iso.org/standard/72311.html>

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability handling processes*. First Edition. ISO/IEC 30111:2013. Geneva, Switzerland: ISO: IEC. 2013

<https://www.iso.org/standard/53231.html>

Jajodia, Sushil, et al., (Eds.). *Cyber Situational Awareness: Issues and Research*. Part of the Advances in Information Security book series (ADIS, volume 46). 2010. ISBN 978-1-4419-0140-8

<https://link.springer.com/book/10.1007/978-1-4419-0140-8>

Kossakowski, Klaus-Peter. *Information Technology Incident Response Capabilities*. Hamburg: Books on Demand, 2001. ISBN: 9783831100590.

Kossakowski; Klaus-Peter & Stikvoort, Don. *A Trusted CSIRT Introducer in Europe*. Amersfoort, Netherlands: M&I/Stelvio, February, 2000.

<http://www.ti.terena.nl/process/ti-v2.pdf>

Manion, Art & Householder, Alan. *Vulnerability Analysis*. CERT Coordination Center (CERT/CC). May 30, 2019.

<https://vuls.cert.org/>

McGuinness, B. &, Foy, L. A subjective measure of SA: The crew awareness rating scale (cars). In Kaber, D.B.; Endsley, M.R.; p. 286-291. *Proceedings of the First Human Performance, situation awareness and automation conference; user-centered design for the new millennium*. Savannah, Georgia, October 2000.

Salerno, John; Hinman, Michael & Boulware, Douglas. Situation awareness model applied to multiple domains. In *Proceedings of the Defense and Security Conference*, Orlando, FL, March 2005.

<https://www.spiedigitallibrary.org/conference-proceedings-of-spie/5813/0000/A-situation-awareness-model-applied-to-multiple-domains/10.1117/12.603735.full?SSO=1>

Stone, Steve. Data to Decisions for Cyberspace Operations. *The MITRE Corporation Website*. January 2016

<https://www.mitre.org/publications/technical-papers/data-to-decisions-for-cyberspace-operations>

Tadda G.P., Salerno J.S. (2010) Overview of Cyber Situation Awareness. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) *Cyber Situational Awareness*. Advances in Information Security, vol 46. Springer, Boston, MA. 2010. ISBN 978-1-4419-0140-8

[https://link.springer.com/chapter/10.1007/978-1-4419-0140-8\\_2](https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_2)

West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. CMU/SEI-98-HB-001. Software Engineering Institute, Carnegie Mellon University. 1998.

<http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html>

□ □ 4 □ □ □ CSIRT □ □ □ □ □ □ □ □ □ □

Error! Bookmark not defined.

Error! Bookmark not defined.

- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.

Error! Bookmark not defined.

- □ □
- □ □

Error! Bookmark not defined.

Error! Bookmark not defined.

- Error! Bookmark not defined.
- Error! Bookmark not defined.
- □ □ □ □ □ □ □ □ □ □

Error! Bookmark not defined.

- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined. □ □ □ □

Error! Bookmark not defined.

- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.

Error! Bookmark not defined.

- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined. □ □
- Error! Bookmark not defined.

Error! Bookmark not defined.

- □ □

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- □ □ □ □
- **Error! Bookmark not defined.**

**Error! Bookmark not defined.** □ □ **Error! Bookmark not defined.** □ □ □ □ □ □

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

Error! Bookmark not defined.



- Error! Bookmark not defined.

Error! Bookmark not defined.

- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.

Error! Bookmark not defined.

- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.
- □ □

Error! Bookmark not defined.

- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.

Error! Bookmark not defined.

- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.

Error! Bookmark not defined.

- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.
- Error! Bookmark not defined.

