事件响应和安全小组股份有限公司论坛

(FIRST.Org)

2016 春 16

安全事件响应小组（SIRT）服务框架

版本 1.0

引言 6
服务 1 事件管理 8
功能 1.1 **事件处理** 8
子功能 1.1.1 **信息收集** 8
子功能 1.1.2 **响应** 9
子功能 1.1.3 **协调** 9
子功能 1.1.4 **事件跟踪** 9
功能 1.2 脆弱点、配置和资产管理 9
子功能 1.2.1 **脆弱点发现研究** 10
子功能 1.2.2 **脆弱点报告** 10
子功能 1.2.3 **脆弱点协调** 10
子功能 1.2.4 **脆弱点根本原因纠正** 10
服务 2 分析 11
功能 2.1 **事件分析** 11
子功能 2.1.1 **事件确认** 11
子功能 2.1.2 **影响分析** 11
子功能 2.1.3 **汲取的教训** 11
功能 2.2 **人工分析** 12
子功能 2.2.1 **表面分析.** 12
子功能 2.2.2 **逆向工程** 13
子功能 2.2.3 **运行时分析** 13
子功能 2.2.4 **比较分析** 14
功能 2.3 **媒介分析** 14
功能 2.4 **脆弱点/利用分析** 15
子功能 2.4.1 技术的（恶意软件）脆弱点/利用分析 15
子功能 2.4.2 **根本原因分析** 15
子功能 2.4.3 **纠正分析** 15
子功能 2.4.4 **减轻分析** 15
服务 3 信息保障 16
功能 3.1 **风险/符合性评估** ..... **Error! Bookmark not defined.**

子功能 3.1.1 **关键资产/数据清单** ..... **Error! Bookmark not defined.**
子功能 3.1.2 **确认评估标准** ..... **Error! Bookmark not defined.**
子功能 3.1.3 **实施评估** ..... **Error! Bookmark not defined.**
子功能 3.1.4 **结果和建议** 17
子功能 3.1.5 **跟踪** 17
子功能 3.1.6 **测试** 18
功能 3.2 **补丁管理** 18
功能 3.3 **运行策略管理** 18
功能 3.4 **风险分析/业务连续性灾难恢复建议** 19
功能 3.5 **安全性建议** 19
服务 4 形势认识 20
功能 4.1 **传感器/度量工作** 20
子功能 4.1.1 **要求形成** 20
子功能 4.1.2 **必需数据的鉴别** 20
子功能 4.1.3 **数据获取方法** 21
子功能 4.1.4 **传感器管理** 21
子功能 4.1.5 **结果管理**. 21
功能 4.2 **融合/相关** 21
子功能 4.2.1 **确定融合算法** 21
子功能 4.2.2 **融合算法** ..... **Error! Bookmark not defined.**
功能 4.3 安全情报的形成和监管 ..... **Error! Bookmark not defined.**
子功能 4.3.1 **来源识别和清单**. ..... **Error! Bookmark not defined.**
子功能 4.3.2 **来源内容收集和编目**. ..... **Error! Bookmark not defined.**
功能 4.4 **数据和知识管理** ..... **Error! Bookmark not defined.**
功能 4.5 **组织的度量** ..... **Error! Bookmark not defined.**
服务 5 外展服务/通信 ..... **Error! Bookmark not defined.**
功能 5.1 **网络安全策略咨询** ..... **Error! Bookmark not defined.**
子功能 5.1.1 内部的 ..... **Error! Bookmark not defined.**
子功能 5.1.2 外部的 ..... **Error! Bookmark not defined.**
功能 5.2 **关系管理** ..... **Error! Bookmark not defined.**

子功能 5.2.1 **对等关系管理** ..... **Error! Bookmark not defined.**
子功能 5.2.2 **顾客关系管理** ..... **Error! Bookmark not defined.**
子功能 5.2.3 **通信管理** 27
子功能 5.2.4 **安全通信管理** ..... **Error! Bookmark not defined.**
子功能 5.2.5 **会议/专题研讨会** 27
子功能 5.2.6 **利益相关者约定/关系** 27
功能 5.3 **安全意识提高** 27
功能 5.4 **品牌推广/营销** 27
功能 5.5 **信息共享和发布** 27
子功能 5.5.1 **公共服务通知** 28
子功能 5.5.2 **信息发布:** 28
服务 6 能力建设 29
功能 6.1 **培训和教育** 29
子功能 6.1.1 **知识、技能和能力要求收集** ..... **Error! Bookmark not defined.**
子功能 6.1.2 **教育和培训材料的发展** ..... **Error! Bookmark not defined.**
子功能 6.1.3 **内容分发** ..... **Error! Bookmark not defined.**
子功能 6.1.4 **指导** ..... **Error! Bookmark not defined.**
子功能 6.1.5 **职业发展** ..... **Error! Bookmark not defined.**
子功能 6.1.6 **技能发展** ..... **Error! Bookmark not defined.**
子功能 6.1.7 **开展训练** ..... **Error! Bookmark not defined.**
功能 6.2 **组织训练** ..... **Error! Bookmark not defined.**
子功能 6.2.1 **要求** ..... **Error! Bookmark not defined.**
子功能 6.2.2 **情况和环境发展** ..... **Error! Bookmark not defined.**
子功能 6.2.3 **参与训练** ..... **Error! Bookmark not defined.**
子功能 6.2.4 **汲取教训的鉴别** ..... **Error! Bookmark not defined.**
功能 6.3 **用于顾客支持的系统和工具** ..... **Error! Bookmark not defined.**
功能 6.4 **利益相关者服务支持** ..... **Error! Bookmark not defined.**
子功能 6.4.1 **基础设施设计和建造** ..... **Error! Bookmark not defined.**
子功能 6.4.2 **基础设施采购** 35
子功能 6.4.3 **基础设施工具评估** 32

子功能 6.4.4 **基础设施资源分配** ..... **Error! Bookmark not defined.**
服务 7 研究/发展 ..... **Error! Bookmark not defined.**
功能 7.1 **脆弱点发现/分析/纠正/根本原因分析方法的发展** ..... **Error! Bookmark not defined.**
功能 7.2 **收集/融合/关联安全情报过程的发展** ..... **Error! Bookmark not defined.**
功能 7.3 **工具的发展** ..... **Error! Bookmark not defined.**
词汇表 38
附件 – 服务体系结构 41

SIRT 服务框架

引言

以下是安全事件响应小组（SIRT）组织为了满足其顾客的需要，可能会考虑实现的一个服务列表，以及解决实施能力上差距的机制。该列表旨在保存由 SIRT 完成的传统服务，以及最近已经出现并且随着其发展正在被现有的小组和组织承担的服务。本文档是一个应包含 SIRT 服务框架的服务列表。

下面的每一项服务均被分解成支持 SIRT 的该服务性能的主功能和子功能，以支持其更广泛的使命。请注意尽管它们在这里表示为唯一的，但许多功能和子功能可用于实现多个服务和/或功能的交付，可以是相互依赖的。虽然本文档认识到存在着这些关系，但在本阶段不试图去定义这些相互关系。

将来，服务会根据服务区内的类似服务而进行分组，起初，本文档集中在三种事件响应小组类型：国家的 CSIRT；部门的 CSIRT（关键的基础设施）；企业（组织的）CSIRT。本服务框架的后续版本还将增加另外两种类型：产品安全事件响应小组（PSIRT）；地区性/多方的事件响应。将来的附带文件将会提供每一种类型的例子，以及从建立一个基础课程来看典型的服务区/服务/功能。为了开发培训模块，还出版了概述每项子功能的任务、子任务以及行动的补充文档。与其他各方也正在就成熟度进行协调，以确保全世界努力达成一致。

目的

CSIRT **服**务框架定义了 CSIRT 为**服**务**其**顾客**而**实现的一组服务和功能。**其目的是**对于 CSIRT **做什么通**过使用**全球社会公**认的术语和方法，**促**进 CSIRT **互操作性**、**全球化能力**发**展活**动以及教育和培训。

历史

CERT/CC CSIRT 服务列表已在多个情况下使用，作为对 CSIRT 及其相应服务的一种一致的并且可比较的描述。在最近对现有的 CSIRT 服务列表的评估中，确定的是尽管该 CERT/CC 列表被广泛地使用并作了适应性修改，但它已经过时了，缺少表示现代 CSIRT 使命的关键组成部分。关注于实现 CSIRT 全球化发展和成熟度的 FIRST，认识到这是制定一个全面的 CSIRT 教育课程发展的关键部分。给定 FIRST 成员的地理和功能范围，可以确定的是对于明确地获取和表示由 CSIRT 提供的服务，其聚集的社区将是一个适合的来源。还可以确定的是对于 PSIRT 服务需要采取类似的方法，这些方法将编入本服务框架将来的版本中。

定义

由于需要在本文档中使用，我们定义了某些术语的使用。注意到服务区域、服务和功能是以不同的详细程度确认正在做**什么**，而任务和行动则是以不同的详细程度确认正在**怎样**做。任务和行动在附带文件中出版，能够/将会被更加频繁地更新：

- **服务区** — 与公共方面有关的群服务，它们有助于按顶层分类来组织服务，从而便于理解。（在 2.0 版本中，该区域将会得到进一步的发展）。
- **服务** — 代表或者为了事件响应小组的顾客，朝着特定结果的一组可认知的相关行动，用于实现该服务的功能列表。
- **功能** — 完成特定服务的目标或任务的一种手段，可以作为功能的一部分来执行的任务列表。
- **任务** — 完成该任务必须执行的系列行动。
- **行动** — 怎样以变化的详细程度/成熟度完成某事的列表。
- **能力** — 可能作为组织的任务和职责的一部分而执行的可度量的活动。对于 SIRT 服务框架来说，能力可以定义为更广 泛的服务，也可以定义 为必备的功能、子功能、任务或者行动。
- **容量 —** 组织在达到某种形式的资源耗尽之前，能够履行特殊能力的并发进程的数量。
- **成熟度 —** 组织在其使命和授权范围内如何有效地履行特殊的能力，是行动或任务或者功能或服务集能够达到的熟练程度。

事件响应小组类型

- **国家的 CSIRT（计算机安全事件响应小组）—** 国家的 CSIRT 指的是由国家当局设立的、提供国家级网络安全事件协调的一个实体，其顾客通常包括所有的政府部门和机构、执法和民间社会，通常它还是与其它国家的国家 CSIRT 以及地区的和国际的参与者进行交互的权威机构。
- **关键基础设施/部门的 CSIRT —** 负责监视、管理和响应与特定部门（例如能源、电信、金融）有关的网络安全事件。
- **企业 （组织的）CSIRT —** 企业 CSIRT 通常指负责监视、管理和处理影响特定组织内部 ICT 基础设施和服务的网络安全事件的小组。
- **地区性的 / 多方的 CSIRT —** 地区性的/多方的 CSIRT 指的是负责监视、管理和响应与特定地区或多个组织有关的网络安全事件的小组或者矩阵式小组。

– **产品安全事件响应小组（PSIRT）—** 产品 SIRT 是商业实体（典型的某一个厂家）内部的、管理与该组织商品化的产品或服务有关的安全脆弱点信息的接收、调查以及内部或公开报告的一个小组。

服务1　　事件管理

功能 1.1 **事件处理**：与网络事件管理有关的服务，包括向委托人发出警告，协调与事件响应、减轻和恢复有关的活动。事件处理取决于分析活动，分析活动的规定见“分析”小节。

子功能 1.1.1 **信息收集**：与事情和事件有关信息的吸纳、分类、存储等相关服务，包括：

- **事件报告集**：来自委托人和第三方的（例如其它的安全小组或者商业情报订阅）、关于恶意的或者可疑的事情和事件报告的报告集，不论是人工的、自动化的还是机器可读的格式。
- **数字数据收集**：可能会但不保证有助于了解事件活动的数字数据的收集和分类（例如磁盘镜像、文件、网络日志/流量）。
- **其它数据类型（非数字的）**：非数字数据（物理的签到单、体系结构图、商业模型、地点评估数据、策略、企业风险框架等）的收集和分类。
- **构件收集**：用于吸纳、分类、存储、跟踪被认为是敌手活动残余痕迹的构件的业务和技术过程。
- **证据收集**：收集可能用于执法活动的信息和数据的业务，通常包括获取关于来源、收集方法以及所有者和监管信息的元数据。

子功能 1.1.2 **响应**：与减少事件影响以及努力恢复顾客内部业务功能有关的服务。

- **遏制**：通过短期的战术行动（例如，阻塞或者过滤业务）停止直接的损害并且限制恶意活动的范围；也可以包括重新获得对系统的控制。
- **减轻**：通过根除、实施变通的方法或者实施更深入和全面的遏制策略，防止进一步的损害。
- **修理**：实现在受到影响的领域、基础设施或网络中改正并防止这类活动再次出现所必需的改变，这包括通过策略改变以及补充培训和教育来加强组织的防御状态和运行准备。

- **恢复**：恢复受影响系统的完整性，将受到影响的数据、系统和网络复原到没有恶化的运行状态。

子功能 1.1.3 **协调**：CSIRT 内部和外部的信息共享和劝告活动，这主要出现在当 CSIRT 依赖于在其直接控制之外的企业和资源的时候，为了完成减轻事件影响所必需的行动。通过提供双边的或多边的协调，CSIRT 参与信息的交换，使那些资源有能力检测、保护或纠正敌手正在开展的活动，或者帮助其他人这样做。

子功能 1.1.4 **事件跟踪**：记录关于为解决事件所采取行动的信息，包括收集的关键信息、开展的分析、采取的纠正和减轻措施、终止和决定。

功能 1.2 **脆弱点、配置和资产管理**：与了解和纠正脆弱点、配置问题以及资产存量有关的服务。

子功能 1.2.1 **脆弱点发现研究**：通过研究和试验（即模糊测试和逆向工程）识别新的脆弱点。

子功能 1.2.2 **脆弱点报告**：用于吸纳、分类、存储和跟踪脆弱点报告的业务和技术过程。

子功能 1.2.3 **脆弱点协调**：为了影响修理工作并且限制来自脆弱点利用的潜在影响，通报某一个脆弱点的适当构成。

子功能 1.2.4 **脆弱点根本原因纠正**：实施纠正一个确认的脆弱点所必需的正式纠正行动。典型地，由产品供货商完成。

服务2　　分析

功能 2.1 **事件分析**：识别并描述与事情或事件相关信息特征的有关服务，例如范围、受影响方、有关的系统、时间表（发现、发生、报告）、状态（正在进行的对比已经结束的）。

[注：通过其它的、更加集中的分析任务，例如构件、配置错误、脆弱点、网络或者取证信息的分析，出现了对事件的更加深入的分析。]

子功能 2.1.1 **事件确认**：确切地证实报告的事件事实上发生了并且对有关的系统具有某些影响。

目的：提供技术上的证据，说明事件是一个安全性事件、网络或者硬件错误，并且确认对信息资产的机密性、可用性和/或完整性的潜在安全影响和损害。

结果：**确定一个**报告的事件**是否真的是一个需要**处理的事件，**或者能否将**该报告记录**在有关的系**统中并且终结，**而不需要采取**进一步的行动。获得已经让**委托人**认为安全**事件的确已**经发生的事件细节，**并且确定是否存在**恶意目的或者有不同的原因–**例如配置**错误或者硬件故障。

子功能 2.1.2 **影响分析**：识别并描述对相关系统所支持的业务功能的影响。

目的：确认事件的规模和范围，包括受到影响的部分基础设施、服务、数据，以及部门或者组织。可以在此分析的基础上实施通用的纠正方法。

结果：**确定事件已**经产生的或者可能产生的（**潜在的**）损害，**不**仅确认技术方面，**而且确**认所有的媒介覆盖范围、**信任或者信誉**损失，**以及所有的名誉**损害。

子功能 2.1.3 **汲取的教训**：事后的回顾确认对于过程、策略、程序、资源和工具的改进，以便有助于减轻和防止将来的危害。

目的：确定什么出了问题，实施预防的措施，通过公布和展示来共享安全社区应汲取的教训。

结果：**被**认为是对**受影响**组织的相关部门内部的信息系统、过程和程序的可能更改的**系列建**议。

功能 2.2 **构件分析**：与了解构件（例如，恶意软件、漏洞利用、垃圾邮件、配置文件）的能力和目的及其发送、检测和抵消有关的服务。

目的：**作**为事件处理过程的一部分，**可能会在受影响的系**统或恶意软件分发站点发现数字**的构件**。**构件可能是入侵者攻**击的残余，**例如**，**脚本**、**文件**、镜像、**配置文件**、**工具**、**工具**输出、**日志等**。**开展构件分析是**为了**找出入侵者如何使用**该**构件**，**例如**进入组织的系统**和网**络，**或者确**认入侵者曾经在该**系**统**内做了什么**。**构件分析力求确**认**构件自己或者和其它构件一起是如何工作的**。这**可以通**过各种类型的活动来获得，**包括**：**表面分析**、**逆向工程**、**运行**时**分析和比**较分析。**每个活**动均**会提供关于构件的更多信息**。**分析方法包含但不限于**对**构件**类型和特征的识别、**与已知的构件**进行**比**较、观**察构件在运行**环境下的执行以**及反**汇编并解释二进制**构件**。为了评估危害，**提出减**轻**构件危害的解决方案**，**并且向委托人和其他研究者提供信息**，**分析人**员**通**过分析**构件**，试图**重**现**并确定入侵者做了什么**。

结果：**了解恢复的数字构件的特性**连同**它与其它构件**、**攻**击和被利用的脆弱点**之**间**的关系**。**通**过了解入侵者为损害系统和网络以及实施恶意活动所使用的战术、**技**术和程序，**确**认减轻所分析**构件的危害的解决方案**。

子功能 2.2.1 **表面分析**：识别并描述关于构件的基本信息和元数据（例如，文件类型、字符串输出、加密的哈希、文件大小、文件名称）；连同审阅关于构件的所有公开的或秘密的源信息。

目的：**作**为收集基础信息的第一步，**表面分析比**较从该**构件收集的信息和从其它公开的**、**秘密的构件和/或**签名库**中收集的信息**。**收集并分析所有已知的信息**（**即可能的危害**、**功能和减**轻）。**取决于开展分析的目**标，**可能需要作**进一步的分析。

结果：确认**数字构件的特征和/或**签名，**以及所有已**经的关于该构件的信息，**包括**恶意、**影响和减**轻。[1]（这样的信息能够用于决定下一步措施。）

子功能 2.2.2 **逆向工程：**对构件的深入分析，以确定其完整的功能，与它可能运行于其中的环境无关。

目的：**提供**对于恶意软件**构件的更加深入的分析**，**包括确**认隐藏的活动和触发命令。**通**过揭示所有的源码或者将二进制反汇编**成**汇编语言并解释它，**逆向工程使分析人**员**能**够**挖掘**过去**所有的模糊**处理和编译（对于二进制）**并且确**认组成恶意软**件的程序**、**脚本或代**码。**揭示所有的机器**语言**能使**恶意软件能够执行的功能和行动**曝光**。**逆向工程是在表面分析和运行**时**分析不能提供所需要的全部信息**时开展的更加深入的分析。

结果：获得数字**构件的全部功能来了解它是如何工作的**、**如何被触**发的，**可以利用的相关系**统弱点，**它的全部影响以及潜在的危害**。**因此**，**形成减**轻**构件危害的解决方案**，**并且适当**时建立一个新的签名**用于与其它的**样本进行比较。

子功能 2.2.3 **运行时分析：**当在实际或模拟环境下（例如，沙箱、虚拟环境、硬件或软件仿真器）运行样本时，通过观察来了解构件的能力。

目的：**了解构件的运行**，**采用模**拟环境捕获主机、**网**络流量和执**行**输出的变化。**基本的前提是**设法在一个尽可能接近于现实的情况下观察**运行中的构件**。

结果：**通**过观察数字构件在执行期间的行为来获得对其工作的额外认识，**来确定受影响的宿主系**统的变化、**与其它系**统的交互以及最后的网络流量，**从而更好地了解系**统**的危害和影响**，**建立新的构件**签名并且确定**减**轻**措施**。（**注**，**由于不是所有的构件代**码部分均可能被触发，**因此运行**时分析并不能看见**所有的功能**。**运行**时只能让分析人员看见恶意软件在测试情况下做**了什么**，**而不是它完全能**够做什么。）

子功能 2.2.4 **比较分析：**关注于确认公共功能或目的的分析，包括对已编目过的构件的系列分析。

目的：**探究一个构件与其它构件的关系**，**它可以确**认在代码或者做法、**目**标、**意**图和**作者方面的相似性**，这些相似性可以用于**得到攻**击的范围（**即**，**有一个更大的目**标，类似的代码以前已经使用过，**等等**）。**比**较分析技术可以包括**精确匹配比**较或代码相**似性比**较。**比**较分析提供了**构件或其**类似的版本如何被使用以及如何随**着**时间变化**的更**宽阔视角，**有助于理解**恶意软件或者恶意构件类型的评估。

结果：**得到与其它构件的共同点或关系**，**以便确**认**可能会提供**对**于数字构件功能**、**影响和减**轻的**附加了解或理解的**趋势或者相似性。

功能 2.3 **媒介分析：**为了更好地了解如何防止、检测和/或减轻类似的或者有关的事件，与来自系统的相关数据、网络、数字存储和可移动媒介的分析有关的服务，这些服务可以为法律、取证、符合性审查或其它历史的信息复审提供信息。

目的：**收集并分析来自媒介的**证据，**例如硬**盘、**移**动设备、**可移**动存储、**云存**储，**或者其它的形式包括**纸张或视频。**如果分析的**结果要**出**现在**法律或者遵从性背景下**，**将需要以依法的合理方式收集信息**，这会保护证据的完整性和监管链。证据可能包括构件，**例如**遗留**的**恶意软件；**文件**、**寄存器和其它系**统部件状态的变化；**网**络流量捕获或者存储器内的其**它日志文件**、**信息**。**注意到媒介分析正期望**寻找发生了什么**的**证据以及可选的该活动的起因；**它不同于构件分析**，**构件分析期望了解一个构件及其关系**。**然而**，**构件分析技**术**可以用作媒介分析技**术和方法的一部分。**在网**络事件之外**也可以**调用这些服务，**但是将它**们**作**为人力资源问题或者其它法律的或组织的调查的一部分。

结果：**提供**结果1)**存量信息**资产（**即知**识产权或者**已**发现的其它敏感**信息**）；2)**提供可能**显**示与**该事件有关的所有媒介资产的增加、**更改和**删除**的事件**时间**表**，连同谁**或者什么**执行**了那些活**动，**如果可能的**话，**所有的事件是如何**联系在一起的以便解释该事件的范围和影**响**。

功能 2.4 **脆弱点/利用分析：**提供对已经成为网络事件一个因素的脆弱点的更深入了解的服务。

子功能 2.4.1 **技术的（恶意软件）脆弱点/利用分析：**了解可能被利用发起一个事件的弱点以及敌手利用该弱点时所采取的谍报技术。

目的：告知顾客所有已知的脆弱点（攻击程序的通常进入点），因此，系统能够相对于漏洞利用保持最新状态和受控，使任何的负面影响最小化。

结果：完全掌握脆弱点以及恶意程序将使用这个脆弱点实施其渗透/**利用系**统的方**式**。

子功能 2.4.2 **根本原因分析：**了解让攻击得以发生的“设计”或“实现”缺陷。

目的：确认根本原因和折衷点，有助于彻底地根除问题。

结果：对允许脆弱点存在的环境以及攻击者因此能够在该环境下利用该脆弱点有着明**确的**认识。

子功能 2.4.3 **纠正分析：**了解纠正使攻击成为可能的潜在缺陷以及防止将来这类攻击所必需的步骤。

目的：确认实现折衷、修补脆弱点，改变程序或设计、复审第三方的纠正等问题，并识别在纠正步骤中引入的所有新的脆弱点。

结果：制定一个计划改进过程、**基**础设施和设计，**从而**终止**特定的攻**击向量并防止将**来**这种攻击。

子功能 2.4.4 **减轻分析：**在不一定纠正攻击或脆弱点引入的潜在缺陷的情况下，为了确定减轻（防止）该攻击或脆弱点所产生风险的手段而进行的分析。

服务3　　信息保障

功能 3.1 **风险/符合性评估：**与评估风险或者符合性评估活动有关的服务。这可能包括实际的评估行为，以便支持对评估的结果进行评价。典型地支持符合性要求时（例如 ISO 27XXX、COBIT）开展该评估。

目的：改进对时机和威胁的识别；改进控制；改进防损和事件管理，连同信息安全性和其它相关功能。

结果：一贯的应用于关键资产和数据的信息风险评估和管理过程；输入到风险评估；选择相关的风险处理选项，以便包含适当情况下的事件管理和取证。

子功能 3.1.1 **关键资产/数据清单：**确定对于完成组织的使命必不可少的关键资产和数据，这些资产和数据可能未必属于该组织（例如，云提供商或者外部数据集），包括确认他们的位置、所有者、信息敏感度、使命功能及其当前的状态/水平。

目的：在可能需要事件管理以便让组织与相关的行业一起完成其使命的情况下，定期地确认那些资产和数据。

结果：定期地更新被组织用于风险评估的关键资产和数据的清单、列表或数据库。

子功能 3.1.2 **确认评估标准：**通过开展风险等级/状态评估，获得组织的风险策略和已经枚举的/确认的标准。建议供企业风险管理者和 CISO 考虑的用于评估或基准测试的准则。标准的例子可能包含但不限于巴塞尔 II、COBIT、 ITIL 、认证和鉴定。

目的：有助于选择一个供组织内部使用的、经过批准的信息风险评估方法， 并提供更广泛的、组织层级的风险评估和管理。

结果：一个选择的、供跨组织使用的信息风险评估方法；对于所做的选择，执行层的支持和接受；适当情况下，要求使用所选择的风险评估方法的组织策略；经过同意的度量、模板和输出；经过同意的用于信息风险评估的过程和程序；经过同意的将信息风险评估结果融入到组织级风险管理和决策之中的机制。

子功能 3.1.3 **执行评估：**有助于开展审查并参与评估，以确保风险和安全要求得到满足/解决。

目的：对于所选择的关键资产或数据，采用经批准的方法、以尽可能彻底的方法来完成信息风险评估。

结果：**关于所**选择的关键资产或数据**的一份完整的信息**风险评估。

子功能 3.1.4 **结果和建议：**形成并提供调查结果、报告和/或建议（例如，报告书写，使用公布信息中的任务）。

目的：有助于完整地记录一个已完成的风险评估的结果，并且作为该评估的结果，枚举应采取的行动以及应考虑的建议。

结果：**一份**经过授权、签署的报告，详述**了关**键资产或数据，**随后的**风险评估过程，风险评估中使用的数据，结果、**建**议、**行**动、计划和**分**发的时间表。

子功能 3.1.5 **跟踪：**帮助 CISO 和/或风险管理者跟踪评估的状态以及随后的建议执行情况。

目的：确保所有的计划、行动和建议均被跟进，并且在用文件记录的时间表内完成。

结果：**定期地**审查计划和时间表；**已完成行**动的列表；**如果行**动没有按时完成，则修**改**时间表；报告相对于计划和时间表的进展情况。

子功能 3.1.6 **测试：**对符合风险程度的主动测试，可以包括渗透性测试、脆弱点扫描和评估、应用测试、审计和验证等。

目的：测试所选择和执行的风险处理是合适的，被正确地执行，并提供了预期的风险减轻。

结果：**一份具有**预期结果的用**文件**记录的测试计划；**用文件**记录的测试和结果；**与**预期结果**的比**较；纠正**离开**预期值的**任何偏差的行**动和时间表。

功能 3.2 **补丁管理：**帮助顾客具备管理清单识别、要修补的系统、补丁安装的部署和验证所必需能力的服务。

目的：对于产品和系统，有助于补丁的识别、获取、安装和验证，并从事件管理的观点提供对补丁的效用和影响的评估。

结果：组织对所需**要**补丁的认识和了解；**了解要由服**务提供商应**用的**补丁；**了解**补丁对**信息**风险的影响；**了解**对事件管理的**影响**。

功能 3.3 **运行策略管理：**制定、维护、制度化和强制执行组织的运行概念以及其它策略的服务。

目的：通过提供公平的、基于事实的建议，考虑到时机以及所讨论的问题，可能采纳该建议的环境以及任何限制该应用的资源，作为委托人或行业关于业务连续性和灾难恢复的一个值得信赖的顾问。

结果：**包含**业务连续性和灾难恢复的业务**决定**；视为值得信赖顾问的事件管理；时间和地**点合适**时，**涉及**业务决定的事件管理小组的成员。

功能 3.4 **风险分析/业务连续性灾难恢复建议：**向顾客提供的与基于确认风险的组织恢复活动有关的服务。这可能包括各种风险管理活动，从开展实际的评估到提供评估结果评价和减轻方面的分析支持。

目的：通过提供公平的、基于事实的建议，考虑到时机以及所讨论的问题，可能采纳该建议的环境以及任何限制该应用的资源，作为委托人或行业关于信息安全和事件管理的一个值得信赖的顾问。

结果：**包括信息安全和事件管理的**业务决定；视为值得信赖顾问的事件管理；时间和地点**合适**时，**涉及**业务决定的事件管理小组的成员。

功能 3.5 **安全性建议：**向委托人或行业提供关于适当的安全操作或功能的执行和实现方面建议的服务。

服务4　　形势认识

目的：形势认识是让组织了解其运行环境的活动集合。形势认识包括对可能影响组织使命的关键因素的鉴别，监视那些因素并且使用该知识来告知决策及其它的行动。

结果：**以及**时和安全的方式**提供在**组织周围的、**可能会影响**组织工作**能力的事件和活动的必要**认**知**。

功能 4.1 **传感器/度量工作**：关注于系统的开发、部署和运行以及确认调查活动的分析方法的服务。

目的：建立向组织提供形势认识所必需的信息收集基础设施和过程。

结果：为形势认识提供信息的**运行信息收集基**础设施（**即**传感器）。

子功能 4.1.1 **要求形成：**了解顾客的需求，并确保权限在 CSIRT 能够操作的范围内。

目的：要求形成过程确认该组织的形势认识需求，然后将那些要求映射成达到那些目标所需要的信息类型。

结果：从信息的观点，**了解**组织及其顾客**需要的**认识程度，**此外**，**确保**该组织已经具**有收集信息的必需的政策和法律批准**。

子功能 4.1.2 **必需数据的鉴别：**确定满足要求所需要的数据。

目的：传感器会以各种各样的形式出现，从自动化系统到人类，这些信息（数据）源用于为组织建立形势认识画面，“必需数据的鉴别”过程将形势认识要求映射为可能的信息源（即传感器）。

结果：支持组织的形势认识要求所需的数据鉴别。**某些数据源可能已**经存在，**而其它的数据源可能需要建造和/或**获取。

子功能 4.1.3 **数据获取方法：**确定用于收集必需数据的方法、工具、技能和技术。

目的：该过程确认了用于收集、处理和存储被收集的信息（数据）的方法。

结果：确定关于信息将如何被收集、存储、过程和杀毒的具体细节。

子功能 4.1.4 **传感器管理**：维护并持续改进与规定的要求有关的传输器性能。

目的：维护并监视传感器以确保合适的功能和准确度。

结果：实现传感器管理和生命周期的维持规划。

子功能 4.1.5 **结果管理**：对由传感器获得的信息和度量结果进行分类和分发。通常，通过仪表板提供，供组织内部不同的级别查看。

功能 4.2 **融合/相关**：实施多数据源的分析和包含的服务。获取信息的订阅，不论其来源，将它们融入到形势的总体认识中（形势认识）。

目的 确认事件、指示器和行动者之间新的关系，使对安全事件的减轻或响应得到改进。

结果：利用新的威胁信息，将它与组织知识库中已有的可用信息相结合，该过程的最终结果将是一个改进的信息集，使 CSIRT 能够以更加高效和准确的方式做出决定。

子功能 4.2.1 **确定融合算法**：确定用于分析（融合）信息的方法和技巧（算法）或技术。

目的 作为事件处理的一部分，CSIRT 保持一个良好的关于由各种来源接收到信息的运行视图是很重要的。融合实现了以这样一种方式管理信息，使 CSIRT 能够迅速地注意到接收的新信息，将该信息完全地融入到背景中并且在事件处理过程中加以利用。

结果：开发一个内部过程，能够吸纳新信息及其在已有信息情况下的评估，以及成功地利用在事件情况下 CSIRT 可获得的最终信息。

子功能 4.2.2 **融合分析：**使用知识管理系统中的数据来分析（融合）数据源，从而确认数据中间的共同点和关系。

目的 作为事件处理的一部分，CSIRT 将需要持续保持对于某一特殊事件对组织造成威胁的了解。为了做到这一点，需要对事件本身以及战术上的演进、被敌手利用的技能和程序有着最新的了解，需要持续地收集信息，相对于已有的信息对它进行评估。子功能 4.2.2 将利用子功能 4.2.1 中选择的融合算法对从外部源获得的威胁信息进行分析。

结果：**了解收集到的新威**胁信息**相**对于**已有事件的影响**，让组织对敌手在 TTP **方面的任何**变化有着充分的准备，**或者使**组织能够持续地更新其减轻和响应技术以便更好地处理相关事件。

功能 4.3 **安全情报的形成和监管：**为了形成和管理第三方来源的安全情报，向内部或者外部委托人提供的服务。安全情报可以定义为提供运行情报或威胁情报的安全和威胁信息，服务可能包含但不限于分析、形成、分发和管理安全情报，包括威胁指示器、威胁检测逻辑例如反恶意软件的规则和签名，敌手的战术、技术和程序。这些服务取决于信息交换活动，信息交换活动的规定见第 5.6 节“外展服务/通信”。

目的：来自外部实体的信息对于获得形势的充分认识至关重要，CSIRT 需要大量高质量的、与其工作有关的信息，但获取它所需的成本和工作量意味着工作必须集中在选择的信息源集合上。

结果：**吸**纳**多个高**质量的**涵盖** CSIRT **工作所有相关**领域的数据订阅-**主要通**过完全自动化的过程-**采用数据管理系**统（**功能** 4.4）。**另一个**结果**也是**检测**由外部源**获得的信息流中的异常**和**变化趋势**的**过程。

子功能 4.3.1 **来源鉴别和清单：**对信息源进行持续的鉴别、维护，并将其并入知识管理和分析过程。

目的：从外部源获得相关的、高质量的信息来实施有效的事件响应，并主动提高形势认识（通常，该组织的安全状况）。内部收集到的外部源补充数据：事件报告（功能 1.1）、脆弱点报告（功能 1.2）和 CSIRT 操作的传感器输出（功能 4.1）。

结果：从内部的、外部的和开源和/或商业源获取高质量、相关的安全信息。所有收集到的信息均存储在数据管理系统中（功能 4.4）。

子功能 4.3.2 **来源内容收集和编目：**获取威胁信息源材料，这些源可能是内部的、外部的、开源的和或者按服务收费的。

目的：评定收集到信息的质量。观察由外部源获取的数据的特征（包括数量）的变化，以便检测异常和/或新的趋势。

结果：包含来源质量评定的文件。自动化或半自动地处理由外部源获取信息的总特征的主要变化。

功能 4.4 **数据和知识管理：**提供给委托人的支持获取、发展、共享和有效利用组织知识的服务，包括数据标记（例如，STIX、TAXII、IODEF、TLP）、指示器数据库和恶意软件/脆弱点目录。

目的：委托人需要一定质量水平和适合于其需要的时间表的网络安全数据和知识。网络安全数据包括拟用于系统处理的信息，以便支持安全的自动操作。网络安全知识包括供人类网络安全分析人员/操作人员使用的信息。此外，其它的CSIRT服务和功能需要以网络安全数据和知识作为输入。假设大部分信息跨多个服务和功能被重复地使用，这样的信息最好作为一个总的CSIRT资源来进行管理。

结果：将所要求质量的网络安全数据和知识及时地提供给委托人，其它的CSIRT服务和功能能够容易地获取他们需要从该CSIRT内部单一来源获得的数据和知识。

- **数据表示管理：**将如何表示和交换数据标准化（例如 STIX、TAXII、IODEF、RID 等。）
- **数据存储管理：**存储管理系统的设计、实现和维护。
- **数据消化：**用于输入、验证和存储 信息的过程和系统。
- **数据提取：**用于提取信息的过程、策略和技术方法。
- **工具评估：**对用于数据管理、分析和协作的工具进行评估和集成。

功能 4.5 **组织的度量：**集中于组织性能目标的鉴别、建立、收集和完成分析的服务，连同度量组织的效率。

目的：计算机安全事件响应小组（CSIRT）和事件管理组织当前正在为确定他们怎样成功地满足其管理网络安全事件的使命而努力，随着小组在操作持久性方面变得更加成熟，他们正在问一个问题“我做得真的有多好？”小组正在寻找评估其工作的方法，不仅确认过程、技术和方法中的优点和弱点，而且相对于其它类似的小组对他们自己进行基准测试。他们正在寻找定量的证据和度量，来显示他们在预防、检测、分析和响应网络事情和事件方面是否有效。该功能集中在识别CSIRT小组尤其是利益相关者为了评估其工作并且显示价值，需要回答什么管理问题（信息）；建立收集测量结果的机制，以便提供所需要的度量，然后收集、分析并呈现结果。

结果：**提供必需的**认识和经验证据**来演示一个事件管理**组织**在**满足**和**执行其使命**方面有多好**；**同**时确认差距以便改进。**使用**该信息**促**进决策并提高性能和责任感。

服务5　外展服务/通信

功能 5.1 **网络安全策略咨询：**支持网络安全策略的制定和采用的服务，通过提供主题专家意见来告知决策者，从而积极地形成 CSIRT 及其顾客和其他利益相关者的环境。

子功能 5.1.1 **内部的**

- **策略和法律咨询：**传送与组织和委托人授权、托管有关的策略和法律蕴涵输入。
- **编写策略：**涉及或影响组织或委托人的工作和授权的创作策略。

子功能 5.1.2 **外部的**

- **提供策略输入：**提供关于技术和安全策略问题的建议，这可能会影响组织及其委托人或其它合作伙伴。
- **影响策略：**提供官方信息或者主题专家意见来指导策略、规则或法律的修订，可能包含但不限于在立法的、科学的或其它团体前面的证实；撰写意见书、白皮书或者文章；博客或者社交媒体；会见利益相关者等。
- **标准或最佳方法的发展：**有助于行业、全球、区域和国家的标准或最佳方法组织（IETF、ISO、FIRST）的工作，实现过程/最佳方法的标准化，从而使兼容性、互操作性、安全性、可重复性或质量最大化。

功能 5.2 **关系管理：**关注于建立和维护该组织关系的服务。

子功能 5.2.1 **对等关系管理：**发展并维护与组织之间的关系，这些组织可能会执行 CSIRT 的使命，这可能会涉及确保组织之间或跨组织的互操作性，或者促进组织之间或跨组织的协作。

子功能 5.2.2 **顾客关系管理：**发展和实现用于确认、区分、了解、管理、跟踪和评估委托人和利益相关者的实践、策略和技术。

子功能 5.2.3 **通信管理：**管理用于分发通知、警报、警告、数据订阅和其它的发布物或信息共享的列表。

子功能 5.2.4 **安全通信管理：**管理用于电子邮件、网络、即时通信或者话音通信的安全通信机制。

子功能 5.2.5 **会议/专题研讨会：**给 CSIRT 及其顾客提供机会，让他们花时间共同讨论所面临的威胁和挑战，加强信任关系，交换联系人，共享最佳方法或者汲取的教训。

子功能 5.2.6 **利益相关者约定/关系：**包括与部门/纵向组织的协作，保持与内部和外部的利益相关者的正式联络点，与该组织内部领导层接洽，以便开展组织使命方面的教育，并确保对于安全意识的理解。

功能 5.3 **安全意识提高：**在顾客内部运行的服务，用于提高集体的对于他们所面临威胁以及应采取的减轻由这些威胁产生风险的行动的认识。

功能 5.4 **品牌推广/营销：**确保利益相关者和委托人了解 CSIRT 和 CSIRT 提供的能力，以及他们应怎样与 CSIRT 交互表达其需求的服务。

功能 5.5 **信息共享和发布：**集中在广泛交流的服务，包括组织告知其顾客所支持的操作，例子包括培训、事件、组织策略和程序的注解。

子功能 5.5.1 **公共服务通知：**传播与安全有关的信息，以便改进组织、委托人、部门的认知和实现，或者公共安全实践。

子功能 5.5.2 **信息发布：**

- **要求收集：**确认需要传播什么信息，向谁传播，以什么方式和时间表（范围）传播。注：发布可能会面向有限的受众，或者针对合作伙伴受众的更深入的发布。

673 - **开发**：定义信息产品的格式和用途以满足要求。
674 - **编写**：准确地获取信息，使其能够容易地被预定的受众理解（例如，呈现
675 辩论、事件、脆弱点和恶意软件管理活动的结果）。
676 - **审查**：审查出版物的清晰、准确、语法、拼写、敏感性和遵守信息公开规
677 则，以及得到最后的批准。
678 - **分发**：通过必需的和适合的渠道将信息发送给预定的受众。

679

服务6　　能力建设

目的：构成健壮的事件处理以及响应过程和方法肯定总会涉及能力建设，它是组织的总体性能和有效性的中心。组织需要在了解哪些能力会真正地影响其 CSIRT 和总的业务性能并相应地调整其培训课程方面更为深思熟虑。在 McKinsey 调查中，接近 60%的回答者指出建设组织的能力是其组织位于前三名的优先考虑的事情，然而当轮到指出什么是最需要的时候，只有不到 30%的回答者实际上会将其培训课程集中在建设能增加最多价值并且是性能最优化所需要的能力上。

人们可以将能力定义为组织做得好的、达成了有意义的业务结果的任何事情，组织需要对于他们总的业务和小组性能最为关键的能力，并了解他们之所以关注所选择的能力的原因。文化确实在组织列入优先提供的能力方面起了一定作用。虽然上层管理通常会涉及为组织能力设立风格和愿景，但最成功的是使组织层级的能力对准业务单元或者小组层级的需要和要求。

结果：**了解**、**用文件**记录并执行一个计划，**能**够**利用并度量各种能力建**设时机**的**结果和关系，单个小组成员和总的组织层级的准备情况。**定**义并实践**成**为了总的人力规划一部分的系统化**方法**。

功能 6.1 **培训和教育：**容量意味着处于若干个成熟度水平的多个能力水平。因此，能力是 CSIRT 服务的核心部件。能力建设给 CSIRT 顾客（可能包括组织的职员，但不包括功能项目例如对小组的 HR 培训）提供与网络安全、信息保障和事件响应有关主题的培训和教育。

目的：培训和教育课程通常是朝着规定一个能力建设实体并付诸行动的第一步，这可以通过各种类型的活动来完成，包括培训和教育、用文件记录的必备知识、需要的技能和能力，已形成的教育和培训材料内容分发，指导，职业和技能发展，提供训练和实验室。这些活动中的每一个均会共同地对组织和小组的能力起作用 。

结果：**了解培**训和教育课程的**前景及其在支持** CSIRT **小**组能力建设方面的关系，**能**够了解**并**记录小组的类型和组织的结果，**以及能**够了解所取得进展的 KPI。

子功能 6.1.1 **知识、技能和能力要求收集：**收集知识、技能和能力需求以及顾客关于确定应提供什么培训和教育的权限。

目的：正确地评估、确认和用文件记录CSIRT小组在必备的KSA方面的需求是什么，以便让小组成员做好准备并且能力更强。

711
712 **结果**：**确**认所需要的 KSA **的特征**，CSIRT **小**组藉此**可**满足业务需求的过程，**并与其**
713 **它的**进行比较以求做得**最好**。这将有助于确定该小组**正在以什么**样的**水平工作**，**以及**
714 **是否有机会改**进和哪**里有机会改**进。

715

716 子功能 6.1.2 **教育和培训材料的发展**：创建或者获得教育和培训材料的内容，例如
717 呈现、讲义、演示、模拟等。
718

719 **目的**：教育和培训材料发展被CSIRT小组用于保持对用户的认知，使该小组能随着快
720 速变化的前景和威胁而保持更新，并且促进CSIRT与顾客之间的沟通。
721

722 **结果**：优等质量的 CSIRT **培**训和教育材料；传递**快速**变化的 CSIRT 环境**需求**，**并利**
723 **用各种各**样有效的呈现技术和平台。

724

725 子功能 6.1.3 **内容分发**：将知识和内容传递给“学生”，这可以通过各种方法来实
726 现，例如基于计算机的培训/在线、教师引导、虚拟、会议、展示、实验室
727 等。
728

729 **目的**：内容分发的正式过程将有助于该小组确认一种透明的、关于CSIRT成员如何能
730 够最好地接受其培训的方法。
731

732 **结果**：**一个内容分**发框架，该框架采用**所有可用的方法**、**呈**现、**技**术**学**习、软技能和
733 过程，**使用所有**备选的方法，**包括**实际操作训练、远程 CBT **和**亲自**培**训等。

734

735 子功能 6.1.4 **指导**：通过一个既定的关系向有经验的职员学习，可以包括现场访
736 问、轮换（交流）、由有经验的职员陪着工作以及讨论具体决定和操作的基
737 本原理。
738

739 **目的**：指导课程通常是朝着规定一个能力建设实体并付诸行动的第一步，它能有助于
740 提供一个正式的和非正式的、导师与学员分享教育和技能发展、见识、人生和职业经
741 验（超出了该小组的官方的报告关系和结构的范围）的机制。

结果：**具有增强的保持力、忠**诚度、**置信度和**总体能力来做出合理决定的CSIRT**小**组。

子功能 6.1.5 **职业发展：**帮助职员成功地并且适当地规划和发展其职业，可以包括出席会议、高级培训、交叉培训活动等。

目的：CSIRT小组使用职业发展来发起一个连续不断的过程，巩固与安全职业、独特的工作职责以及总的小组环境相关的新知识、技能和能力。

结果：**得到**职业发展的特征，这样该小组不仅拥有信心，**而且**拥有必备的、**可直接**转**入**实践的知识、**技能和能力**，**并且根据工作任**务和需求进行更新。

子功能 6.1.6 **技能发展：**为组织职员提供用于日常运行功能的工具、过程和程序的训练。

目的：在合适的技能已经得到了确认之后，CSIRT小组需要采取一系列的行动，这将决定他们准备就绪的能力。

结果：**具有所需的技**术、软技能和过程认知**的成熟的且**经过**培**训**的**职员，CSIRT **成**员**随**时可处理日常运行**的挑**战，**支持**该小组及其顾客。

子功能 6.1.7 开展训练：对委托人“学生”准备情况进行测试，测试他们开展培训并履行工作或任务功能的能力。可以是虚拟环境、模拟、现场测试、桌面、假想情况的形式，或者是它们的一个组合。

目的：通过开展练习/训练，CSIRT小组将会增加在组织的CSIR计划有效性及其执行力方面的信心。

结果：让小组**尽可能地做好准**备，**确保** KSA **关**键过程**以及所有工作均成功地共同**执**行**，这还将有助于确定该小组运行的水平，**以及是否有空**间以及哪里有空间改进。

功能 6.2 **组织训练**：组织向委托人提供的、支持网络训练的设计、实施和评估的服务，该网络训练旨在训练和/或评估单个委托人或者将顾客作为一个整体的能力。这些类型的训练可以用于：

- **测试策略和程序**：小组评估是否有充分的策略和适当的程序来应对事件，通常这是纸上的/桌面的训练。
- **测试操作准备情况**：小组评估合适的人是否适当地对事件做出了响应，并且程序是否被正确地执行。典型地，这包括训练程序。

目的：开展训练旨在提高网络安全服务和功能的有效性和效率。该功能及相关的子功能解决的是组织及其委托人的需求，更具体地说，通过模拟网络安全事情/事件，训练可以用于一个或多个目标：

- 演示：举例说明网络安全服务和功能，以及脆弱点、威胁和风险，以便提高意识。
- 培训：给职员讲授新工具、技术和程序。
- 训练：给职员提供一个使用其已经接受了培训的工具、技术和程序的机会。训练对于易逝的技能是必需的，有助于提高并保持效率。
- 评估：分析并了解网络安全服务和功能的有效性和效率水平。
- 证实：对于网络安全服务和功能，确定能否达到特定水平的有效性和/或效率。

结果：网络安全服务和功能的有效性和效率**将会直接得到提高**，**并且将会确**认**用于**进一步**提高的**课程。**取决于**训练的具体目标，还**可能会向利益相关者演示网**络安全，对职员进行**培**训，对服务和功能的效率和有效性进行评估和/**或**证实，还可能确认用于改进将来训练**的**课程。

子功能 6.2.1 **要求**：了解训练的目标，特别地，所有参与者的目标，以确保发展能包含这些期望。

目的：参加训练的目的是提高网络安全服务和功能的有效性和效率。参与的形式可以是以下之一：

- 观察者：职员观察训练的进行，但不是目标受众的一部分，并且不会接受训练事件的挑战，也不会就其行为表现被评估。不直接参与的观察能够在某种程度上有助于提高CSIRT服务和功能的有效性和效率。它还有助于组织将来的训练。
- 训练受众：职员作为目标受众参与训练，并且接受训练事件的挑战，也可能会被评估。

取决于训练的形式，职员可以到训练的场所或者从他们通常的办公室或另一个适合的地点远程地参与。同样，训练可以提供特定的环境或者参与者可以从他们自己的训练环境或者他们通常的工作环境来参与。

结果：网络安全服务和功能有效性和效率方面的提高，**以及确**认**用于**进一步改进的课程，**取决于**训练的具体目标，**也可能会向利益相关者演示网**络安全，对职员进行培训，对服务和功能的效率和有效性进行评估和/**或**证实，**也可以确**认用于改进将来训练**的**课程。

子功能 6.2.2 **情况和环境发展：**发展训练情况以支持顾客目标。

目的：组织训练的目的是通过处理模拟的网络安全事情/事件，给目标受众提供一个提高其服务和功能的效率和有效性的机会。

结果：**特定的目**标受众已经提高了其服务和功能的效率和有效性，**并且已**经确认了**用于其**进一步提高的课程，**用于改**进**将来**训练的课程也已经得到了确认。

子功能 6.2.3 **参加训练：**组织能够以不同的程度参与一次训练，这归因于其成熟度。

- **评估：**评估训练的结果、征求反馈，并且根据对训练的观察来确认教训。
- **观察：**观察第三方的训练。
- **协调：**协调训练。
- **参与：**参加网络训练，参与者能够选择参与的程度，并且获益于训练的结果（例如对他们的参与进行第三方评估）。

子功能 6.2.4 **汲取教训的鉴别：**形成一个事后报告，包括汲取的教训或者来自训练的结果/最佳方法。

功能 6.3 **用于顾客支持的系统和工具：**集中在给顾客的网络安全相关工具和服务的建议、开 发、提供和获得的服务，所有这些系统和工具均与 CSIRT/安全有关，而与一般的信息技术无关；这些系统可能包括报文发送/发出警告的门户网站。

结果：CSIRT 拥有**适当的**过程和系统来确认委托人需求和能力，**并且**获得、**提供或者开**发**支持**这些需求的平台。

功能 6.4 **利益相关者服务支持**：集中在 CSIRT 提供的技术能力的服务，该技术能力有助于建设给利益相关者的 CSIRT 服务的能力、容量和成熟度，这是服务水平的成熟。

目的：在建设和提高 CSIRT 顾客能力的过程之中，特别关注在设计、获取、管理、运行和维护他们的基础设施方面提供帮助。

结果：开发一种系统化方法，用于基础设施需求评估、要求定义、布局设计、获取、符合性验证、维护和升级、操作培训、内部和外部的审计。

子功能 6.4.1 **基础设施设计和建造**：有助于基础设施的设计和建造以便支持顾客要求。

目的：根据全面的需求评估和顾客要求分析，提供对设计方法、相关标准和规范知识的广泛了解，并且强调在设计和建造该基础设施方面的最佳方法。

结果：根据国际的最佳方法并结合相关的标准和规范，在开发和比较基础设施设计方法和备选方案方面的实际经验。

子功能 6.4.2 **基础设施采购**：有助于基础设施的采购，不是有助于加强风险框架成熟度，就是提高最低安全性要求和合同语言标准（例如，要求符合特殊的标准如产品认证）。

目的：从制度、技术和运行要求的角度，了解制定适用于基础设施采购的职权范围。

结果：了解基础设施采购的过程，同时遵守相关的标准和规范，并且考虑到需要遵循的各种技术措施和合同程序。

子功能 6.4.3 **基础设施工具评估**：代表顾客对工具的评估。

目的：在评估各种工具的功能性和符合性方面提供支持，包括硬件设备、软件和定制应用。

结果：分析工具的性能以及它们对于标准、规范以及预置的职责范围的符合性。

子功能 6.4.4 **基础设施资源分配：**有助于获取需要的基础设施资源。（即硬件提供商、服务提供商等。）

目的：强调取得成功的基础设施资源分配的关键因素，并且基于清晰的职责和责任，提出与解决方案提供者建立可持续的和有效的关系的机制。

结果：得到用于基础设施资源分配的关键性能指示（KPI），**以及适合的可供高效和有效的基**础设施分配的服务水平协议（SLA）。

服务7　　研究/开发

功能 7.1 **脆弱点发现/分析/纠正/根本原因分析方法的发展：**帮助定义、确认新的能力并且改进方法的服务，该方法用于开展与脆弱点相关的服务，或者协调能够证实相同脆弱点的其它组织或业务实践。

目的：某些组织将只通过从外部源获取脆弱点信息来工作，但是有一些组织会拥有发现和分析脆弱点的有机能力的需求/期望。该功能旨在概述某一个组织可能会怎样构架这些脆弱点研究功能。

结果：必要时，**确定**组织为了更好地了解脆弱点**可能会采取的方法**。

功能 7.2 **收集/融合/相关安全情报过程的发展：**定义、确认新能力并且改进开展信息分析和共享相关服务（当它与操作上的和威胁情报有关时）的方法的服务。

目的 为了取得成功，所有的安全情报功能必须能够收集信息，并且能够与第三方共享相关的信息。这种收集通常取决于共享各方之间的人际关系，人际关系达到的信任程度足以实现敏感信息的共享。分析人员必须能够发展这些关系，确认适当的需要共享的信息集合，确认最适合于自动化交换的协议、关系管理和联合调查，并且评估信息源的有效性。

结果：组织拥**有收集、分析**、综合和评估**来自描述信息安全**资产**威**胁的外部源的信息相关**性的适当**过程和程序。该组织具有发展新的来源和共享伙伴**的有机能力**。

功能 7. 3 **工具的发展**：开发、确认新的能力并且共享新工具和使 CSIRT 相关过程自动化执行的方法的服务。

结果：CSIRT **开**发的旨在使 CSIRT **相关任**务自动化的工具是**可**扩展的、**可靠的**，**会**产生确**定性的**结果，**不会降低使用它**们的 CSIRT **的安全状况**。释放分析人员资源用于非例行的任务。

支持资源

FIRST - https://www.first.org

CERT/CC - http://www.cert.org

STIX/TAXII - https://stix.mitre.org

TLP - https://www.us-cert.gov/tlp

IETF - https://www.ietf.org

ISO/IEC 27035 -
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379

词汇表

Application Testing 应用测试 –旨在向利益相关者提供关于被测试的产品或服务的质量信息的调查。

Basel II–第二个巴塞尔协议，该协议是巴塞尔银行监管委员会发布的关于银行法律和规章制度的建议。

Capability 能力 –作为组织的作用和职责的一部分，可能要完成的可度量的活动。对于 CSIRT 服务框架来说，能力可以定义为更广泛的服务，也可定义为必备的功能、子功能或任务。

Capacity 容量 –组织在达到某种形式的资源耗尽之前能够履行特殊能力的并发数量。

CERT/CC –计算机紧急响应小组协调中心。

CISO –首席信息安全官。

Cloud 云–允许使用可上网的设备运行应用软件的分布式计算环境。

COBIT –信息及相关技术的控制目标。

Cryptographic Hash 加密的哈希–被认为几乎不可能反变换的哈希函数，即不可能只从其哈希值重新得到输入的数据。

CSIRT –计算机安全事件响应小组。

External Data Set 外部数据集 –第三方的数据集。

FIRST –事件响应和安全小组论坛。

Function 功能 –实现特定服务的目标或者任务的手段。

Fuzz Testing 模糊测试–软件测试技术，通常是自动的或者半自动的，包括向计算机程序的输入端提供无效的、意外的或者随机的数据。

Hardware / Software Emulator 硬件/软件模拟器–使一个计算机系统（称为主机）行为就像另一个计算机系统一样（称为客户机）的硬件或软件。典型地，使主机系统运行软件或者使用为客户机系统设计的外围设备。

IEC – I 国际电工委员会。

IETF –互联网工程任务组。

940 **IODEF** –事件目标描述交换格式，是一种数据表示法，为计算机安全事件响应小组（CSIRT）通
941 常交换关于计算机安全事件的共享信息提供一个框架。

942 **ISO** –国际标准化组织。

943 **ISO/IEC 27000-系列 (ISO27k)** –在总的信息安全管理系统（ISMS）范围内提供关于信息安全管
944 理、风险和控制的最佳方法建议的信息安全标准，类似于设计用于质量保证（ISO 9000 系列）和
945 环境保护（ISO 14000 系列）的管理系统。

946 **ITIL** –信息技术基础设施库，是关注于使 IT 服务对准商业需求的 IT 服务管理（ITSM）的一系列
947 实践。

948 **Maturity 成熟度** –组织在其使命和授权范围内如何有效地履行某一项特殊的能力。

949 **Open Source 开源**–一种发展模式，通过免费得到产品的设计或者蓝图的使用权促进普遍使用，以
950 及促进该设计或蓝图包括任何人后来对它的改进的普遍再次分发。

951 **Penetration Testing 渗透测试**–对计算机系统的攻击，其目的是查找安全脆弱点，潜在地使用它及
952 其功能和数据。

953 **Reverse Engineering 逆向工程**–从任何人为提取知识或设计信息，或者基于提取的信息复现它或
954 再生任何信息的过程。

955 **RID** –实时网间防御，是将现有的适用于一个完整事件处理解决方案的检测、跟踪、来源识别和
956 减轻机制集成在一起的时候，促进事件处理数据共享的一种网间通信方式。

957 **Sandbox 沙箱** –隔离正在运行程序的一种安全机制。

958 **Service 服务** –代表或者为顾客帮助工作或做工作的行为。

959 **STIX** –结构化威胁信息表示方法，是一种合作社区驱动的工作，定义和制定一种标准化语言来表
960 示结构化的网络威胁信息。

961 **Strings Output 字符串输出**–最后得到的字符序列，为字面常量或者是某种变量。

962 **TAXII** –指示器信息的可信自动交换，是一组服务和报文交换，实施该交换能够实现可采取行动
963 的网络威胁信息跨组织和产品/服务边界的共享。

964 **TLP** –红绿灯协议，用于确保敏感信息与正确的受众共享。

965 **Virtual Environment 虚拟环境**–对特殊的计算机系统的模拟。

966 **Vulnerability Scanning and Assessment 脆弱点扫描和评估**–在计算机系统中用于识别安全弱点的
967 安全技术。

968

附件 – 服务体系结构

如上所述，本框架中采用的服务体系结构包含鉴别为定义“是什么”的三层（服务区、服务和功能）和确认“怎样做”的另外两层（任务和行动）。

简而言之，总体结构如下所示：