破坏分析与关键控制点（BACCP）体系
供应链中各类组织信息安全管理通用工具

Breach analysis and critical control point (BACCP) system —

A general tool for information security management of any

organization in supply chain

草稿版

Draft Version

2023-03-13

13-Mar-23

编制：黄小根

Editor：Sky Huang

Email：Sky.Huang@27001.cn

BACCP 官方网站（Official Website）：http://www.baccp.org.cn

目录

加入 BACCP 微信交流群，请扫码：

若二维码过期，请访问：http://www.baccp.org.cn/34.shtml。

知识产权声明

《破坏分析与关键控制点（BACCP）体系——供应链中各类组织信息安全管理通用工具》（后面简称为“本文”）编写和发布的目的是希望推动信息安全管理学科的发展和创新，以及沉淀相关知识。

本文在编写过程中参考了 ISO 9001、ISO 22000、HACCP 以及 ISO/IEC 27001 等相关标准，所涉及的相关知识产权属于相关机构或个人所有。本人不会将本文用于商业用途，仅限用于信息安全管理学科的钻研和交流。本人将会保留本文相关创新成果涉及的知产产权。

为此，不建议任何个人或组织将本文的相关内容用于商业用途，如果涉及侵犯知识产权，相关后果由其本人或组织承担，相关侵权责任均与我无关。

电子邮箱：Sky.Huang@27001.cn。

黄小根

2023-03-13

前言

本文是通过管理借鉴、经验积累和思路创新对现有信息安全管理体系思维进行整体重构和优化，并采用 ISO/IEC 合并导则附录 SL 中定义的高层结构编写而成的。

本文编写过程中参考了 ISO 9001、ISO 22000、HACCP 以及 ISO/IEC 27001 等管理标准。

与 ISO/IEC 27001 相比，本文内容的主要变化如下：

a) 本文只有正文部分，没有附录部分。

b) 变更了“信息安全管理体系”相关内容（见 4.4）；

c) 变更了“领导作用和承诺”相关内容（见 5.1）；

d) 增加了“以顾客为关注焦点”相关内容（见 5.1.2）；

e) 变更了“信息安全方针”相关内容（见 5.2）；

f) 变更了“组织的角色、职责和权限”相关内容（见 5.3.1）；

g) 增加了“信息安全小组组长”相关内容（见 5.3.2）；

h) 变更了“应对风险和机遇的措施”相关内容（见 6.1）；

i) 增加了“变更的策划”相关内容（见 6.3）；

j) 变更了“资源”相关内容（见 7.1.1、7.1.2、7.1.3 和 7.1.4）；

k) 增加了“外部开发的信息安全管理体系（BACCP）要素”相关内容（见 7.1.5）；

l) 增加了“外部提供的过程、产品和（或）服务的控制”相关内容（见 7.1.6）；

m) 增加了“组织的信息安全知识”相关内容（见 7.1.7）；

n) 变更了“意识”相关内容（见 7.3）；

o) 变更了“沟通”相关内容（见 7.4）；

p) 变更了“运行”所有内容（见 8），通过创新引入了信息安全风险识别、评价和管控工具（BACCP）；

q) 变更了“持续改进”相关内容（见 10.2）；

r) 增加了“信息安全管理体系（BACCP）的更新”相关内容（见 10.3）。

引言

0.1 总则

采用信息安全管理体系（BACCP）作为组织的一项战略，将会有助于组织提升其信息安全管理的整体绩效。组织实施信息安全管理体系（BACCP）带来的潜在益处有：

a) 持续提供满足顾客和适用法律法规相关信息安全要求的产品和服务的能力；

b) 处理与目标相关的信息安全风险；

c) 可作为 ISO/IEC 27001 实施和落地的工具。

本文采用过程方法（见 0.3），该方法包括策划—实施—检查—处置（PDCA）循环（见 0.3.2）和基于风险的思维（见 0.3.3）。

该过程方法使组织能够对过程及其相互作用进行策划。

PDCA 循环使组织能够确保过程得到充分的资源和管理，确定改进机会并采取行动。

基于风险的思维使组织能够确定可能导致其过程和信息安全管理体系（BACCP）偏离策划结果的各种因素，并采取控制措施以防止或最大限度地降低不利影响。

在本文件中，使用以下助动词：

— “应”表示要求；

— “宜”表示建议；

— “可”表示允许；

— “能”表示可能或能够。

“注”为理解和澄清本文相关要求提供指导。

0.2 BACCP 原则

信息安全与组织业务进行时所涉及的信息资产受破坏的状况相关。由于供应链的任何环节均可能发生信息资产破坏，所以非常有必要对供应链中各个环节进行适当控制。通过供应链中所有参与方共同努力确保信息安全。本文规定了信息安全管理体系（BACCP）要求。该体系结合了下列普遍认同的关键要

素：

— 相互沟通；

— 体系管理；

— 前提方案；

— 破坏分析和关键控制点（BACCP，借鉴了 HACCP）原理。

此外，本文也是基于 ISO 管理体系通用原则。这些管理原则是：

— 以顾客为关注焦点；

— 领导作用；

— 全员参与；

— 过程方法；

— 改进；

— 循环决策；

— 关系管理。

0.3 过程方法

0.3.1 总则

本文倡导在建立、实施信息安全管理体系（BACCP）时采用过程方法，以保障产品和服务提供过程中的信息安全。过程方法包括按照组织信息安全方针和战略方向，对各过程及其相互作用进行系统的规定和管理，从而实现预期结果。可以通过使用 PDCA 以及始终基于风险的思维对过程和整个体系进行管理，旨在利用机遇和防止发生不良结果。

识别组织在供应链的作用及所处的位置是必要的，以确保其与整个供应链中的相关方有效的互动沟通。

0.3.2 PDCA 循环

PDCA 循环简要描述如下：

— 策划（Plan）：建立体系的目标及其过程，提供实现结果所需的资源，并识别和应对风险和基于；

— 实施（Do）：执行所做的策划；

— 检查（Check）：监视和测量（适用时）过程及其涉及的重要信息资产，分析和评价来自监视、测量和验证活动的信息和数据，并报告结果；

— 处置（Act）：必要时，采取措施提高绩效。

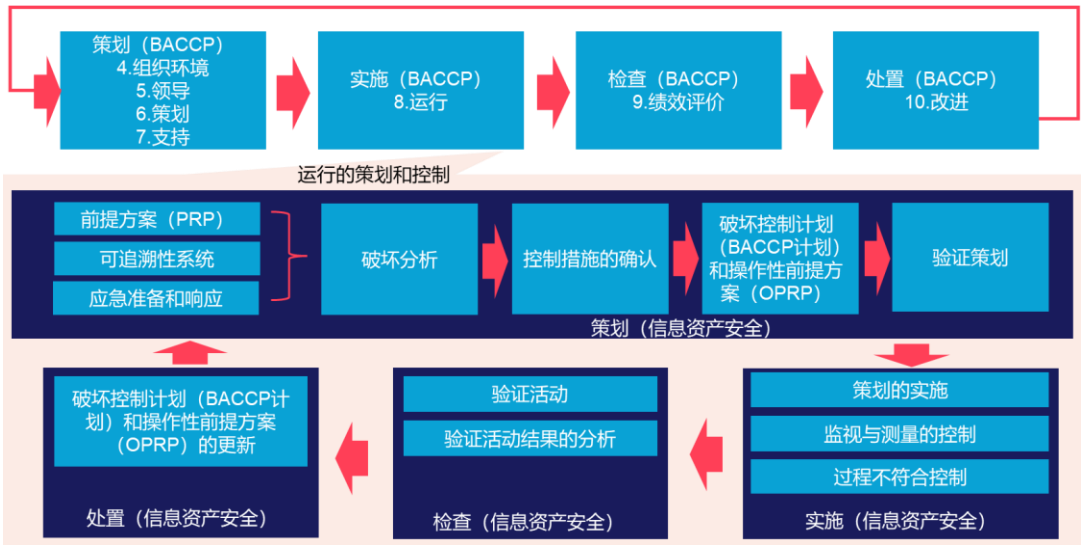

图 1 PDCA 双循环

在本文中，如图 1 所示，基于 PDCA 循环的过程方法包括了两个层次的概念。第一个层次涵盖了整个信息安全管理体系（BACCP）框架（条款 4-7、条款 9 和条款 10）。另一个层次（运行的策划和控制）涵盖了如条款 8 所述的在信息安全管理体系（BACCP）中的运行过程。两个层次之间的沟通是必不可少的。

0.3.3 基于风险的思维

0.3.3.1 总则

基于风险的思维对于实现信息安全管理体系（BACCP）的有效性至关重要。在本文中，应用基于风险的思维的两个层次，即组织（见 0.3.3.2）和运行（见 0.3.3.3），这与 0.3.2 中所述过程方法相一致。

0.3.3.2 组织风险管理

风险是不确定性的影响，不确定性可能有正面的影响，也可能有负面的影响。在组织风险管理环境下，风险的正面影响可能提供机遇，但并非所有正面影响均可提供机遇。

为符合本文的要求，组织需策划和实施应对组织（条款 6）的措施。应对风险措施为提高信息安全管理体系（BACCP）的有效性，获得改进结果以及防止不利影响奠定基础。

0.3.3.3 破坏分析 — 运行过程

BACCP（借鉴了 HACCP）的逻辑步骤可以认为是必要的措施，以防止破坏或将破坏降低到可接受水平，以确保在业务开展时重要信息资产是安全的（条

款 8）。

BACCP 应用过程中的决策应基于科学，以防止主观偏见和文件化。文件应该包括决策过程中的任何关键假设。

0.4 与其他管理体系标准的兼容

本文采用了 ISO 高层结构（HLS）。高层结构的目的是提高与 ISO 管理体系标准的一致性。本文使组织能够使用过程方法，结合 PDCA 循环和基于风险的思维，将信息安全管理体系（BACCP）方法与其他管理体系标准和支持性标准的要求进行协调或整合。

本文可以作为信息安全管理体系的核心和框架，其列出了整个供应链组织的具体信息安全管理体系要求，且覆盖了信息安全、网络安全、数据安全、工控安全、隐私保护和各类行业信息安全相关的标准和法规要求，并为其预留了接口。

1 范围

本文规定了信息安全管理体系（BACCP）的要求，以确保供应链中的各类组织：

a) 策划、实施、运行、保持和更新信息安全管理体系（BACCP），以便在提供产品和服务过程中，保障重要信息资产的安全；

b) 证实其符合适用的信息安全法律法规要求；

c) 评价双方商定的顾客信息安全要求，并证明其符合此类要求；

d) 与供应链中的相关方在信息安全方面进行有效沟通；

e) 确保符合其声明的信息安全方针；

f) 证实其符合其他相关方的要求；

g) 进行符合性自我评价，或自我声明；

h) 作为 ISO/IEC 27001 实施的优化和补充。

本文所有要求都是通用的，适用于供应链中各种类型、各种规模和复杂程度的所有组织。

本文允许任何组织在其信息安全管理体系（BACCP）范围内实施外部制定的要素，如外包。

可使用内部和（或）外部资源，满足本文的要求。

2 规范性引用文件

本文没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文。

注：ISO 与 IEC 的标准化领域词汇和数据库可参见以下网址：

— ISO 线上浏览平台：http://www.iso.org/obp；

— IEC 电工百科：http://www.electropedia.org/。

3.1 可接受水平 acceptable level

组织（3.30）提供产品和服务过程中相关信息资产（3.16）不得超过的信息安全破坏（3.22）水平。

3.2 行动准则 action criterion

用于监视（3.26）操作性前提方案（3.29）的可测量或可观察的准则。

注：制定行动准则，用以确定操作性前提方案（3.29）是否在控制范围内，并区分什么是可接受（符合或达到准则，指操作性前提方案按预期运行）和不可接受（不符合或未达到准则，指操作性前提方案未按预期运行）。

3.3 审核 audit

为获得审核证据并对其进行客观的评价，以确定满足审核准则的程度所进行的系统的、独立的并形成文件的过程（3.35）。

注 1：审核可以是内部（第一方）审核，或外部（第二方或第三方）审核，也可以是结合审核（结合两种或多种领域）。

注 2：内部审核由组织自己或代表组织的外部方进行。

注 3：“审核证据”和“审核准则”见 ISO 19011。

注 4：信息安全管理、质量管理或环境管理可作为相关领域。

3.4 能力 competence

能够应用知识和技能实现预期结果的本领。

3.5 符合 conformity

满足要求（3.37）。

3.6 持续改进 continual improvement

提高绩效（3.32）的循环活动。

3.7 控制措施 control measure

防止显著信息安全破坏（3.22）或将其降低到可接受水平（3.1）所必须的行动或活动。

注 1：参见显著信息安全破坏（3.39）。

注 2：根据破坏分析确定控制措施。

3.8 纠正 correction

为消除已发现的不符合（3.27）所采取的措施。

注：纠正包括潜在不安全的重要信息资产的处理，因此可以连同纠正措施（3.9）一起实施。

3.9 纠正措施 corrective action

为消除不符合（3.27）的原因并防止再发生所采取的措施。

注 1：一个不符合可以有若干个原因。

注 2：纠正措施包括原因分析。

3.10 关键控制点（CCP/CCPs） critical control point

在应用控制措施（3.7）防止或将显著信息安全破坏（3.39）降低到可接受水平的过程（3.35）中的某一步骤，该步骤设定关

键限值（3.11）并通过测量（3.25）能够进行纠正（3.8）。

3.11 关键限值 critical limit

区分可接受和不可接受的可测量值。

注 1：关键限值的设定用于确定关键控制点（CCP）（3.10）是否受控。当超出或不满足关键限值时，受影响的重要信息资产应被作为潜在不安全的重要信息资产进行处理。

3.12 文件化信息 documented information

组织（3.30）需要控制和保持的信息及其载体。

注 1：文件化信息可以任何格式和载体存在，并可来自任何来源。

注 2：文件化信息可涉及：

— 管理体系（3.24），包括相关过程（3.35）；

— 为组织运行产生的信息（一组文件）；

— 结果实现的证据（记录）。

3.13 有效性 effectiveness

实现策划的活动并得到策划结果的程度。

3.14 流程图 flow diagram

以图解的方式系统地表达过程中各环节之间的顺序及相互作用。

3.15 信息安全 information security

对信息资产（3.16）的保密性（3.18）、完整性（3.20）和可用性（3.19）的保持（不被破坏）。

3.16 信息资产 information asset

与信息有关的资产（3.17）。

3.17 资产 asset

对组织（3.30）有任何价值的东西。

3.18 保密性 confidentiality

信息对未授权的个人、实体或过程（3.35）不可用或不泄露的特性。

3.19 可用性 availability

根据授权实体的要求可访问和可使用的特性。

3.20 完整性 integrity

准确和完备的特性。

3.21 安全属性 security attribute

信息资产（3.16）的保密性（3.18）、完整性（3.20）和可用性（3.19）。

注：也可包括诸如真实性、可核查性、抗抵赖和可靠性等其他属性。

3.22 信息安全破坏 information security breach

组织内外环境中对信息资产（3.16）的安全属性（3.21）有潜在破坏的各类因素。

注：术语“破坏”不应和“风险”（3.38）混淆。对信息安全而言，“风险”是信息资产遭受于特定破坏时，对组织不良影响的概率与影响的严重程度之间构成的函数。

3.23 相关方 interested party

可影响决策或活动，也被决策或活动所影响，或自认为受决策或活动影响的个人或组织（3.30）。

3.24 管理体系 management system

组织（3.30）建立方针（3.33）和目标（3.28）以及实现这些

目标的过程（3.35）的相互关联或相互作用的一组要素。

注 1：一个管理体系可以针对单一的领域或几个领域。

注 2：体系要素包括组织的结构、岗位和职责、策划和运行。

注 3：管理体系的范围可能包括整个组织，组织中可被明确识别的职能或可被明确识别的部门，以及跨组织的单一职能或多个职能。

注 4：相关领域，例如，质量管理体系和环境管理体系。

3.25 测量 measurement

确定数值的过程（3.35）。

3.26 监视 monitoring

确定体系、过程（3.35）或活动的状态。

注 1：确定状态可能需要检查、监督或密切观察。

注 2：对于信息安全，监视是指为评价某一过程是否按预期运行，进行策划并实施的一系列观察或测量活动。

注 3：本文对术语确认（3.43）、监视（3.26）和验证（3.44）进行了区分：

— 在活动前进行确认，并提供预期结果实现能力有关的信息；

— 在活动期间进行监视，并提供规定时间范围内活动有关的信息；

— 在活动后进行验证，并提供符合确认有关的信息。

3.27 不符合 nonconformity

未满足要求（3.37）。

3.28 目标 objective

要实现的结果。

注 1：目标可以是战略的、战术的或操作层面的。

注 2：目标可以涉及不同的领域（如财务的、职业健康与安全的、和环境的目标），并可应用于不同的层次（如：战略的、组织整体的、项目的、产品和过程（3.35）的）。

注 3：可以采用其他的方式表述目标，例如：采用预期的结果、活动的目的

或运行准则作为信息安全管理体系（BACCP）的目标，或使用其他有类似含意的词（如：目的、终点或标的）。

注 4：对于信息安全管理体系（BACCP），组织制定的目标与信息安全方针保持一致，以实现特定的结果。

3.29 操作性前提方案（OPRP/OPRPs） operational prerequisite program

用于防止或将显著信息安全破坏（3.39）降低到可接受水平（3.1）的控制措施（3.7）或控制措施组合，其通过行动准则（3.2）和测量（3.25）或观察能够有效控制过程（3.35）和（或）信息资产（3.17）。

3.30 组织 organization

为实现目标（3.28），由职责、权限和相互关系构成自身职能的一个人或一组人。

注：组织的概念包括，但不限于代理商、公司、集团、商行、企事业单位、行政机构、合营公司、慈善机构或研究机构，或上述组织的部分或组合，无论是否为法人组织，公有的或私有的。

3.31 外包（动词） outsource

安排外部组织（3.30）承担组织的部分职能或过程（3.35）。

3.32 绩效 performance

可测量的结果。

注 1：绩效可能涉及定量的或定性的结果。

注 2：绩效可能涉及活动、过程（3.35）、产品（3.36）、服务、体系或组织（3.30）的管理。

3.33 方针 policy

由最高管理者（3.40）正式发布的组织（3.30）的宗旨和方

向。

3.34 前提方案（PRP/PRPs） prerequisite program

在组织（3.30）内和整个供应链中，为保持信息安全所必需的基本条件和活动。

注：所需的前提方案取决于组织在供应链中的位置和组织的类型，前提方案的制定可以参照相关信息安全标准、法规和工具：如 ISO/IEC 27001、TISAX、ISO/SAE 21434、NIST 网络安全框架、GDPR、CCPA、ISO/IEC 27701、ISO 26262 和 S-SDLC。

3.35 过程 process

将输入转换成输出的相互关联或相互作用的一组活动。

3.36 产品 product

输出，即过程（3.36）的结果。

注：产品可以是服务。

3.37 要求 requirement

明示的、通常隐含的或必须履行的需求或期望。

注 1：“通常隐含”是指组织和相关方的惯例或一般做法，所考虑的需求或期望是不言而喻的。

注 2：规定要求是经明示的要求，如：在文件化信息（3.12）中阐明。

3.38 风险 risk

不确定性的影响。

注 1：影响是指偏离预期，可以是正面的或负面的。

注 2：不确定性是一种对某个事件，或是事件的局部的结果或可能性缺乏理解或知识方面的信息的情形。

3.39 显著信息安全破坏 significant information security breach

通过破坏评价确定的，需要通过控制措施（3.7）进行控制的信息安全破坏（3.22）。

3.40 最高管理者 top management

在最高层指挥和控制组织（3.30）的一个人或一组人。

注 1：最高管理者在组织内有授权和提供资源的权力。

注 2：如果管理体系（3.30）的范围仅覆盖组织的一部分，在这种情况下，最高管理者是指管理和控制组织的这部分的一个人或一组人。

3.41 可追溯性 traceability

在实现产品和服务的特定步骤追踪某一对象的历史、应用情况、移动、变更和所处位置的能力。

注：对象可以是产品（3.36）、材料、装置、设备、服务、软件等信息资产。

3.42 更新 update

为确保应用最新信息而进行的即时和（或）有计划的活动。

3.43 确认 validation

通过获取证据以证实控制措施（3.7）（或控制措施组合）能够有效控制显著信息安全破坏（3.39）。

注 1：在策划控制措施组合时，或当实施的控制措施发生变更时，进行确认。

注 2：本文对术语确认（3.43）、监视（3.26）和验证（3.44）进行了区分：

— 在活动前进行确认，并提供预期结果实现能力有关的信息；

— 在活动期间进行监视，并提供规定时间范围内活动有关的信息；

— 在活动后进行验证，并提供合格确认有关的信息。

3.44 验证 verification

通过提供客观证据对规定要求（3.37）已得到满足的认定。

注：本文对术语确认（3.43）、监视（3.26）和验证（3.44）进行了区分：

— 在活动前进行确认，并提供预期结果实现能力有关的信息；

— 在活动期间进行监视，并提供规定时间范围内活动有关的信息；

— 在活动后进行验证，并提供合格确认有关的信息。

4 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨相关并影响其实现其信息安全管理体系（BACCP）预期结果的能力的各种外部和内部因素。

组织应对这些外部和内部因素的相关信息进行确认、评审和更新。

注 1：这些因素可能包括需要考虑的正面和负面要素或条件。

注 2：通过考虑外部和内部因素以有助于理解环境，包括但不限于各种法律法规、技术、竞争、市场、文化、社会和经济环境、网络安全、数据安全、隐私保护、知识产权、黑客攻击、电信诈骗、知识和组织绩效，无论是国际的、国内的、地区的或是当地的。

4.2 理解相关方的需求和期望

为确保组织有能力稳定提供符合信息安全相关的适用法律法规要求和顾客要求的产品和服务，组织应确定：

a) 与信息安全管理体系（BACCP）有关的相关方；

b) 与信息安全管理体系（BACCP）相关方的相关要求。

组织应识别、评审和更新这些有关相关方及其要求的信息。

注:相关方的要求可包括法律、法规要求和合同义务。

4.3 确定信息安全管理体系（BACCP）的范围

组织应确定信息安全管理体系（BACCP）的边界和适用性，

以确定其范围。

范围应包括能对其产品和服务提供过程中的信息安全产生影响的活动、过程和服务。

在确定此范围时，组织应考虑：

a) 4.1 中提及的各种外部和内部因素；

b) 4.2 中提及的要求；

c) 产品和服务。

组织的信息安全管理体系（BACCP）范围应可获取并保持文件化信息。

4.4 信息安全管理体系（BACCP）

4.4.1 组织应按本文的要求建立、实施、保持和持续改进信息安全管理体系（BACCP），包括信息安全管理体系（BACCP）所需的过程及其相互作用。

组织应确定信息安全管理体系（BACCP）所需的过程及其在整个组织中的应用，组织应：

a) 确定这些过程所需的输入和期望的输出；

b) 确定这些过程的顺序和相互作用；

c) 确定和应用所需的准则和方法（包括监视、测量和相关的绩效指标），以确保这些过程的有效运行和控制；

d) 确定这些过程所需的资源并确保其可用性；

e) 规定这些过程的职责和权限；

f) 应对按照 6.1 的要求确定的风险和机会；

g) 评价这些过程并实施所需的变更，以确保这些过程实现预期的结果；

h) 改进过程和信息安全管理体系（BACCP）。

4.4.2 在必要的程度上，组织应：

a) 保持形成文件的信息以支持过程运行；

b) 保留确认其过程按策划进行的形成文件的信息。

5 领导

5.1 领导作用和承诺

5.1.1 总则

最高管理者应通过以下方面证实其对信息安全管理体系（BACCP）的领导作用和承诺：

a) 对信息安全管理体系（BACCP）的有效性承担责任；

b) 确保信息安全方针和信息安全目标得到建立，并与组织环境和战略方向保持一致；

c) 确保将信息安全管理体系（BACCP）要求融入组织的业务过程；

d) 促进过程方法和基于风险的思维的应用；

e) 确保获得信息安全管理体系（BACCP）所需的资源；

f) 传达有效的信息安全管理以及符合信息安全管理体系（BACCP）要求的重要性；

g) 确保实现信息安全管理体系（BACCP）的预期结果；

h) 鼓励、指导和支持员工为信息安全管理体系（BACCP）的有效性做出贡献；

i) 推动持续改进；

j) 支持其他相关管理角色,以证实他们的领导按角色应用于其责任范围。

注：本文中的“业务”从广义上解释为对于组织的存在而言具有核心价值的活动，组织可以是公有的、私有的、盈利或非盈利的。

5.1.2 以顾客为关注焦点

最高管理者应通过确保以下方面，证实其以顾客为关注焦点的领导作用和承诺：

a) 确定、理解并持续满足顾客信息安全相关的要求以及信息安全相关适用的法律法规要求；

b) 确定和应对风险和机遇，这些风险和机遇可能影响产品和服务提供过程中的信息安全的保障以及增强顾客满意的能力；

c) 始终致力于增强顾客满意。

5.2 信息安全方针

5.2.1 制定信息安全方针

最高管理者应制定、实施和保持信息安全方针，信息安全方针应：

a) 适应组织的宗旨和环境并支持其战略方向；

b) 为建立和评审信息安全目标提供框架；

c) 包括满足适用的信息安全要求的承诺，包括法律法规要求以及与信息安全相关的共同商定的顾客要求；

d) 解决内部和外部的沟通；

e) 包括持续改进信息安全管理体系（BACCP）的承诺;

f) 解决确保与信息安全相关的能力需求。

5.2.2 沟通信息安全方针

信息安全方针应：

a) 可获取并保持成文信息；

b) 在组织内得到沟通、理解和应用；

c) 适宜时，可为有关相关方所获取。

5.3 组织的角色、职责和权限

5.3.1 最高管理者应确保组织相关岗位的职责、权限得到分配、沟通和理解。

最高管理者应分配职责和权限，以：

a) 确保信息安全管理体系（BACCP）符合本文的要求；

b) 向最高管理者报告信息安全管理体系（BACCP）的绩效；

c) 确保在整个组织提高以顾客为关注焦点的意识；

d) 确保过程实现其预期的输出；

e) 任命信息安全小组和信息安全小组组长；

f) 授予指定人员明确的职责和权限，以采取措施并予以记录。

5.3.2 信息安全小组组长应负责：

a) 确保建立、实施、保持和更新信息安全管理体系（BACCP）；

b) 管理和组织信息安全小组工作；

c) 确保信息安全小组的相关培训和能力（见 7.2）；

d) 向最高管理者报告信息安全管理体系（BACCP）的有效性和适宜性。

5.3.3 所有人员都有责任向指定人员报告信息安全管理体系（BACCP）的有关问题。

6 策划

6.1 应对风险和机遇的措施

6.1.1 策划信息安全管理体系（BACCP），组织应考虑到 4.1 所描述的因素和 4.2、4.3 所提及的要求，确定需要应对的风险和机遇，以：

a) 确保信息安全管理体系（BACCP）能够实现其预期效果；

b) 增强有利影响；

c) 预防或减少不利影响；

d) 实现改进。

注：在本文的范围内，风险和机遇仅限于与信息安全管理体系（BACCP）绩效和有效性相关的事件及其后果。

6.1.2 组织应策划：

a) 应对这些风险和机遇的措施；

b) 如何：

1) 在信息安全管理体系（BACCP）过程中整合并实施这些措施；

2) 评价这些措施的有效性。

6.1.3 应对风险和机遇的措施应与以下方面相适应：

a) 信息安全要求的影响；

b) 产品和服务提供过程中顾客相关信息安全要求的影响；

c) 相关方信息安全要求的影响。

注 1：应对风险和机遇的措施可包括规避风险、为寻求机遇承担风险、消除风险源、改变可能性或后果，分担风险或通过信息决策接受风险的存在。

注 2：机遇可能导致采用新实践（过程的修改），使用新技术和其他可取之处，以应对组织或顾客的信息安全要求。

6.2 信息安全目标及其实现的策划

6.2.1 组织应对信息安全管理体系（BACCP）所需的相关职能、层次和过程设定信息安全目标。

信息安全目标应：

a) 与信息安全方针保持一致；

b) 可测量（如可行）；

c) 考虑适用的信息安全要求，包括法律法规和顾客要求；

d) 予以监视和验证；

e) 予以沟通；

f) 适时更新。

组织应保留有关信息安全目标的形成文件的信息。

6.2.2 策划如何实现信息安全目标时，组织应确定：

a) 要做什么；

b) 需要什么资源；

c) 由谁负责；

d) 何时完成；

e) 如何评价结果。

6.3 变更的策划

当组织确定需要对信息安全管理体系（BACCP）进行变更（包括人员更改）时，变更应经策划和沟通，并系统地实施（见 4.4）。

组织应考虑到：

a) 变更的目的及潜在的后果；

b) 信息安全管理体系（BACCP）持续完整性；

c) 有效实施变更的资源的可获得性；

d) 责任和权限的分配或再分配。

7 支持

7.1 资源

7.1.1 总则

组织应确定并提供所需的资源，以建立、实施、保持、更新和持续改进信息安全管理体系（BACCP）。

组织应考虑：

a) 现有内部资源的能力和局限；

b) 外部供方获得的资源的需求。

7.1.2 人员

组织应确保运行和保持有效的信息安全管理体系（BACCP）所需的人员是胜任的（见 7.2）。

当使用外部专家帮助建立、实施、运行或评审信息安全管理体系（BACCP）时，则应以文件化信息的形式，保留明确外部专家的能力、职责和权限的协议或合同证据。

7.1.3 基础设施

组织应提供资源，以确定、建立和保持符合信息安全管理体系（BACCP）要求所需的基础设施。

注：基础设施可包括：建筑物和相关设施、设备（包含硬件和软件）、信息和通信技术等。

7.1.4 工作环境

组织应确定、提供和保持相关资源，用于建立、管理和保持符合信息安全管理体系（BACCP）要求所需的工作环境。

注：适宜的环境可能是人文因素和与物理因素的结合，例如：

a) 社会因素（如无歧视、和谐稳定、无对抗）；

b) 心理因素（如舒缓心理压力、预防过度疲劳、保护个人情感）；

c) 物理因素（如温度、热量、湿度、照明、空气流通、卫生、噪声等）。

由于所提供的产品和服务不同，这些因素可能存在显著差异。

7.1.5 外部开发的信息安全管理体系（BACCP）要素

当组织通过使用外部开发的信息安全管理体系（BACCP）要素（包括前提方案、破坏分析和破坏控制计划（见 8.5.4））来建立、保持、更新和持续改进其信息安全管理体系（BACCP）时，组织应确保所提供的要素：

a) 根据本文的要求开发；

b) 适用于组织场地、过程、所提供的产品和（或）服务；

c) 经过信息安全小组特别调整，以适应组织的过程、所提供的产品和（或）服务；

d) 根据本文的要求实施、保持和更新；

e) 作为成文信息予以保留。

7.1.6 外部提供的过程、产品和（或）服务的控制

组织应：

a) 建立并实施对外部供方提供的过程、产品和（或）服务进行评价、选择、绩效监视以及再评价的准则；

b) 确保与外部供方充分沟通要求；

c) 确保外部提供的过程、产品和（或）服务不会对组织持续地满足信息安全管理体系（BACCP）要求的能力产生不利影响；

d) 对于这些活动和由评价与再评价导致的任何必要的措施，组织应保留文件化的信息。

7.1.7 组织的信息安全知识

组织应确定信息安全管理体系（BACCP）运行过程所需的信息安全知识，以确保在产品和（或）服务提供过程中，相关信息资产的安全可得到适当的保障。这些信息安全知识应予以保持，并在需要的范围内可得到。

为应对不断变化的需求和发展趋势，组织应考虑现有的信息安全知识，确定如何获取更多必要的信息安全知识，并进行更新。

注 1：组织的信息安全知识是从其信息安全管理体系（BACCP）运行过程中获得的特定知识，是实现组织信息安全目标所使用的共享信息。

注 2：组织的信息安全知识可基于内部来源（例如从经历中获得的知识、从失败和成功项目中得到的经验教训）和外部来源（例如标准、学术交流、专业会议、从顾客或外部供方收集的知识）。

7.2 能力

组织应：

a) 确定在其控制范围内的人员（包括外部供方人员）所需具备的能力，这些人员从事的工作影响其信息安全绩效和信息安全安全管理体系（BACCP）有效性；

b) 基于适当的教育、培训和（或）经验，确保这些人员（包括信息安全小组和负责破坏控制计划操作的人员）是胜任的；

c) 确保信息安全小组具备多学科的知识和建立与实施信息安全管理体系（BACCP）的经验（这些知识和经验包括但

不限于组织的信息安全管理体系（BACCP）范围内的产品、服务、过程、信息资产和信息安全破坏）；

d) 适用时，采取措施以获得所需的能力，并评价措施的有效性；

e) 保留适当的文件化信息，作为人员能力的证据。

注：适用措施可包括对在职人员进行培训、辅导或重新分配工作，或者招聘具备能力的人员，或借助外部具备能力的人员（如外包人员、外部顾问等）。

7.3 意识

组织应确保在其控制范围内的相关人员知晓：

a) 信息安全方针；

b) 与其工作相关的信息安全目标；

c) 他们对信息安全管理体系（BACCP）有效性的贡献，包括改进信息安全绩效的益处；

d) 不符合信息安全管理体系（BACCP）要求的后果。

7.4 沟通

7.4.1 总则

组织应确定与信息安全管理体系（BACCP）相关的内部和外部沟通，包括：

a) 沟通什么；

b) 何时沟通；

c) 与谁沟通；

d) 如何沟通；

e) 谁来沟通。

组织应确保所有影响信息安全的人员理解有效沟通的要求。

7.4.2 外部沟通

组织应确保对外沟通充分的信息，并且可供信息安全相关方获得。

组织应建立、实施和保持与下列各方的有效沟通：

a) 外部供方和承包方；

b) 顾客和（或）消费者；

c) 立法和监管部门；

d) 对信息安全管理体系（BACCP）的有效性或更新具有影响或将受其影响的其他组织。

指定人员应具有规定的职责和权限，以开展有关信息安全有关信息的外部沟通。适当时，通过外部沟通获得的信息应作为管理评审（见 9.3）和信息安全管理体系（BACCP）更新（见 4.4 和 10.3）的输入。

外部沟通的证据应作为文件化信息予以保留。

7.4.3 内部沟通

组织应制定、实施和保持有效的机制，以就影响信息安全的

事项进行沟通。

为保持信息安全管理体系（BACCP）的有效性，组织应确保信息安全小组及时获得变更的信息，包括以下方面：

a) 组织的业务过程；

b) 信息资产和重要信息资产；

c) 组织各业务过程主要风险及处置措施；

d) 工作场所、设施位置和周围环境；

e) 能力和（或）职责及权限分配；

f) 适用的法律法规要求；

g) 与信息安全破坏和控制措施有关的知识；

h) 组织遵守的顾客、行业和其他要求；

i) 内部员工个人信息；

j) 来自外部相关方的有关问询和沟通；

k) 表明与业务过程有关的信息安全破坏的抱怨和警示；

l) 影响信息安全的其他条件。

信息安全小组应确保信息安全管理体系（BACCP）的更新（见4.4 和 10.3）包括上述信息。

最高管理者应确保将相关信息作为管理评审的输入（见 9.3）。

7.5 文件化信息

7.5.1 总则

组织的信息安全管理体系（BACCP）应包括：

a) 本文要求的文件化信息；

b) 组织所确定的、为确保信息安全管理体系（BACCP）有效性所需的文件化信息；

c) 立法、监管部门和顾客要求的文件化信息和信息安全要求。

注：对于不同组织，信息安全管理体系（BACCP）文件化信息的多少与详略程度可以不同，取决于：

— 组织的规模，以及活动、过程、产品和服务的类型；

— 过程及其相互作用的复杂程度；

— 人员的能力。

7.5.2 创建和更新

在创建和更新文件化信息时，组织应确保适当的：

a) 标识和说明（如标题、日期、作者、索引编号）；

b) 形式（如语言、软件版本、图表）和载体（如纸质的、电子的）；

c) 评审和批准，以保持适宜性和充分性。

7.5.3 文件化信息的控制

7.5.3.1 应控制信息安全管理体系（BACCP）和本文要求的文件化信息，以确保：

a) 在需要的场合和时机，均可获得并适用；

b) 予以妥善保护（如防止泄密、不当使用或缺失）。

7.5.3.2 为控制文件化信息，适用时，组织应进行下列活

动：

a) 分发、访问、检索和使用；

b) 存储和防护，包括保持可读性；

c) 更改控制（如版本控制）；

d) 保留和处置。

对于组织确定的策划和运行信息安全管理体系（BACCP）所必需的来自外部的文件化信息，组织应进行适当识别，并予以控制。

对所保留的、作为符合性证据的文件化信息应予以保护，防止非预期的更改。

注：对文件化信息的“访问”可能意味着仅允许查阅，或者意味着允许查阅并授权修改。

8 运行

8.1 运行策划和控制

组织应通过采取以下措施策划、实施、控制、保持并更新满足实现组织业务目标的相关信息安全要求所需的过程，并实施 6.1 中确定的措施：

a) 建立过程准则；

b) 按照准则实施过程控制；

c) 在必要程度上，保持文件化信息，以证实过程已经按策划进行。

组织应控制策划的变更，评审非预期变更的后果，必要时，采取措施减轻不利影响。

组织应确保外包过程受控（见 7.1.6）。

8.2 前提方案（PRP）

8.2.1 组织应建立、实施、保持和更新前提方案（PRPs），以助于预防和（或）减少组织业务实现过程中的信息资产的安全属性的破坏。

8.2.2 前提方案（PRPs）应：

a) 与组织及其信息安全有关的环境相适宜；

b) 与组织运行的规模和类型、以及其所实现的业务的性质相适宜；

c) 前提方案（PRPs）应在组织提供的产品和（或）服务所涉及的所有过程中实施；

d) 获得信息安全小组的批准。

8.2.3 选择和（或）制定前提方案（PRPs）时，组织应确保已识别适用的信息安全法律法规及共同商定的顾客信息安全要求。

组织宜考虑：

a) 适用的信息安全技术规范；

b) 适用的标准、操作规范和指南。

8.2.4 建立前提方案（PRPs）时，组织应考虑：

a) 建筑物和相关设施的构造与布局；

b) 物理区域和环境；

c) 通信、水、能源和其他支持性设施的供给；

d) 业务过程；

e) 重要信息资产及其信息安全的保障；

f) 供应商的信息安全管理；

g) 适用的法律法规和顾客的信息安全要求；

h) 重要信息资产安全属性被破坏的预防措施；

i) 员工信息安全意识；

j) 其他（适用的其他方面）。

应规定前提方案（PRPs）的选择、建立、适用的监视以及验证过程中的文件化信息。

8.3 可追溯性系统

组织应建立信息安全管理追溯系统，在实现组织业务的各环节建立清晰的记录，以确保出现信息安全事故时能清晰定位和追溯。

8.4 应急准备和响应

8.4.1 总则

最高管理者应确保对能影响信息安全的潜在紧急情况和事

故的程序已有效实施，并应与组织在供应链中的作用相适宜。

应建立和保持管理这些情况和事故的文件化信息。

8.4.2 紧急情况和事故的处置

组织应：

a) 采取以下措施应对实际的紧急情况和事故：

1) 确保已识别适用的法律法规要求；

2) 内部沟通；

3) 外部沟通（如供应商、顾客、有关当局、媒体）；

b) 采取措施减轻紧急情况的后果，并与紧急情况或事故的严重程度以及潜在的信息安全影响相适宜；

c) 适宜时，定期测试程序；

d) 在发生任何事故、紧急情况或进行测试后，评审并在必要时更新文件化信息。

8.5 破坏控制

8.5.1 实施破坏分析的预备步骤

8.5.1.1 总则

为了进行破坏分析，信息安全小组应收集、保持并更新预备的文件化信息。应包括但不限于：

a) 适用的法律法规及顾客信息安全要求；

b) 组织的产品和（或）服务、过程、以及相关信息资产；

c) 与信息安全管理体系（BACCP）相关的信息安全破坏。

8.5.1.2 信息资产的特性

组织应确保已识别所有信息资产所适用的法律法规的信息安全要求。

组织应保持所有信息资产的文件化信息，其详略程度足以进行破坏分析（见 8.5.2），适宜时，描述内容包括以下方面：

a) 各业务过程所涉及的信息资产和重要信息资产；

b) 信息资产的安全属性评价；

c) 信息资产的关键安全属性；

d) 关键安全属性的潜在破坏因素。

e) 适宜的有关信息安全的准则或规范。

8.5.1.3 预期用途

应考虑重要信息资产合理的预期处理以及可能发生的非预期错误处置和误用，并以文件化信息形式进行保持，其详略程度应足以实施破坏分析（见 8.5.2）。

8.5.1.4 流程图和过程描述

8.5.1.4.1 流程图的准备

信息安全小组应建立、保持并更新作为文件化信息的流程图，流程图应包含信息安全管理体系（BACCP）所覆盖产品（服务）或产品（服务）类别和过程。

流程图以图表形式说明过程。在进行破坏分析时应将流程图用作评价信息安全破坏可能发生、增加、减少或引入的基

础。

流程图应清晰、准确和足够详尽，其详略程度应足以实施破坏分析。适宜时，流程图应包括以下方面：

a) 流程的顺序和相互关系；

b) 所有外包过程；

c) 重要信息资产的引入点；

d) 重要信息资产的流转路线；

e) 重要信息资产的销毁点。

8.5.1.4.2 流程图的现场确认

信息安全小组应在现场确认流程图的准确性，适宜时，更新流程图并作为文件化信息保留。

8.5.1.4.3 过程和工作环境的描述

信息安全小组应描述以下方面，其详略程度足以实施破坏分析：

a) 物理区域布局，包括关键区域、一般区域和交界区域；

b) 重要信息资产以及其流向；

c) 现有前提方案（PRPs）、控制措施（适用时）和（或）其实施的严格程度，或可能影响信息安全的程序；

d) 可能影响控制措施的选择和严格程度的外部要求（如立法、监管部门和顾客）。

适宜时，应更新描述并作为文件化信息保持。

8.5.2 破坏分析

8.5.2.1 总则

信息安全小组应根据预备信息实施破坏分析，以确定需要控制的破坏。控制程度应确保信息安全，适宜时，应使用控制措施组合。

8.5.2.2 破坏识别和可接受水平的确定

8.5.2.2.1 组织应识别并记录与产品（服务）类型、过程类别和工作环境相关的所有合理预期发生的信息安全破坏。

识别应基于以下方面：

a) 根据 8.5.1 收集的预备信息和数据；

b) 经验；

c) 内部和外部信息，尽可能包括国内外信息安全热点事件、科学技术和其他历史数据；

d) 来自供应链，与终产品、中间产品和消费时信息安全相关的信息安全破坏信息；

e) 适用的法律法规和顾客信息安全要求。

宜对破坏进行充分详细的考虑，以便进行破坏评价以及选择适宜的控制措施。

8.5.2.2.2 组织应识别每种信息安全破坏可能存在、引入、增加或持续存在的步骤（节点）。

识别破坏时，组织应考虑：

a) 供应链中前后阶段环节；

b) 流程图中所有步骤（节点）；

c) 重要信息资产及工作环境。

8.5.2.2.3 只要可能，组织应确定重要信息资产中识别的每种信息安全破坏的可接受水平。

确定可接受水平时，组织应：

a) 确保已识别适用的法律法规和顾客信息安全要求；

b) 考虑重要信息资产的预期用途；

c) 考虑任何其他相关信息。

组织应保持关于可接受水平的确定以及可接受水平的合理性依据的文件化信息。

8.5.2.3 破坏评价

组织应对每种已识别的信息安全破坏进行破坏评价，以确定其预防或降低到可接受水平是否必要。

组织应就以下几方面评价每种信息安全破坏：

a) 在采取控制措施前，其发生在重要信息资产的可能性；

b) 其预期用途带来破坏的严重程度（见 8.5.1.3）。

组织应识别任何显著信息安全破坏。

应描述所采用的方法，并且应保持破坏评价结果的文件化信息。

8.5.2.4 控制措施的选择和分类

8.5.2.4.1 组织应基于破坏评价，选择适宜的控制措施或控制措施组合，以便能够将识别的显著信息安全破坏得到预防或

降低至规定的可接受水平。

组织应将所选择的控制措施分类为操作性前提方（OPRPs）或关键控制点（CCPs）进行管理。

应采用系统性方法进行分类。对于每种控制措施的选择，应评价以下方面：

a) 其作用失效的可能性；

b) 若其作用失效，后果的严重程度；该评价应包括：

1) 对已识别的显著信息安全破坏的影响；

2) 相对其他控制措施的位置；

3) 是否有针对性的建立控制措施并用于将降低破坏至可接受水平；

4) 是单一措施或控制措施组合的一部分。

8.5.2.4.2 此外，对于每项控制措施，系统性方法应包括对以下方面的可行性评价：

a) 建立可测量的关键限值和（或）可测量（可观察）的行动准则；

b) 进行监视，以发现任何未能保持在关键限值和（或）可测量（可观察）的行动准则内的失效情况；

c) 一旦失效，及时的纠正。

应保持决策过程及控制措施选择和分类的结果的文件化信息。

可能影响控制措施的选择和严格程度的外部要求（例如法

律法规和顾客要求）也应作为文件化信息予以保持。

8.5.3 控制措施和控制措施组合的确认

信息安全小组应确认所选择的控制措施能够实现对显著信息安全破坏的预期控制。应在破坏控制计划（见 8.5.4）中的控制措施和控制措施组合实施之前以及变更后（见 7.4.2、7.4.3、10.2 和 10.3）进行确认。

当确认结果表明控制措施无法实现预期控制时，信息安全小组应对控制措施和（或）控制措施组合进行修改和重新评价。

信息安全小组应保持控制措施的确认方法和能力证据以达到预期控制，并形成文件化信息。

8.5.4 破坏控制计划（BACCP / OPRP 计划）

8.5.4.1 总则

组织应建立、实施和保持破坏控制计划。破坏控制计划应作为文件化信息予以保持，并应包括作为控制措施的每个关键控制点（CCPs）或操作性前提方案（OPRPs）的如下信息：

a) 由该关键控制点（CCP）或操作性前提方案（OPRP）控制的信息安全破坏；

b) 关键控制点（CCPs）的关键限值或操作性前提方案（OPRPs）的行动准则；

c) 监视程序；

d) 当不满足关键限值或行动准则时，应采取的纠正；

e) 职责和权限；

f) 监视的记录。

8.5.4.2 关键限值和行动准则的确定

应规定关键控制点（CCPs）的关键限值和操作性前提方案（OPRPs）的行动准则。应保持关键限值和行动准则确定理由的文件化信息。

关键控制点（CCPs）的关键限值应是可测量的。符合关键限值应确保不超过可接受水平。

操作性前提方案（OPRPs）的行动准则应是可测量的或可观察的。符合行动准则应该有助于确保不超过可接受水平。

8.5.4.3 关键控制点（CCPs）和操作性前提方案（OPRPs）的监视系统

应在每个关键控制点（CCPs），为控制措施或控制措施组合建立监视系统，以发现任何偏离关键限值的情况。系统应包括所有针对关键限值的、有计划的测量。

应在每个操作性前提方案（OPRPs）中，为控制措施或控制措施组合建立监视系统，以发现任何不符合行动准则的情况。

每个关键控制点（CCPs）和每个操作性前提方案（OPRPs）的监视系统应由文件化信息构成，包括以下内容：

a) 在适当的时间范围内提供结果的测量或观察；

b) 使用的监测方法或工具；

c) 适用的校准方法，或用于验证操作性前提方案（OPRPs）的可靠测量或观察的等效方法（见 8.7）；

d) 监视频次；

e) 监视结果；

f) 与监视有关的职责和权限；

g) 与监视结果评价有关的职责和权限。

每个关键控制点的监视方法和频率应能够及时发现偏离关键限值的情况，以便及时识别、评价和处置潜在不安全的重要信息资产（见 8.9.4）。

每个操作性前提方案（OPRPs）的监测方法和频率应与失效的可能性和后果的严重程度应相适宜。

当基于观察的主观信息（例如目视检查）监视操作性前提方案（OPRPs）时，应通过说明书或技术规范对该方法提供支持。

8.5.4.4 不满足关键限值或行动准则时采取的措施

组织应规定在不满足关键限值或行动准则时应采取的纠正（见 8.9.2）和纠正措施（见 8.9.3），并应确保以下方面：

a) 潜在不安全的重要信息资产的处置（见 8.9.4）

b) 识别不符合的原因；

c) 关键控制点（CCPs）或操作性前提方案（OPRPs）控制的参数恢复至关键限值或行动准则范围内；

d) 防止再次发生。

组织应按照 8.9.2 进行纠正，按照 8.9.3 采取纠正措施。

8.5.4.5 破坏控制计划（BACCP 计划）的实施

组织应实施和保持破坏控制计划（BACCP 计划），并保留实施证据的文件化信息。

8.6 前提方案（PRP）和破坏控制计划（BACCP 计划）的信息更新

在建立破坏控制计划（BACCP 计划）后，必要时，组织应更新以下信息：

a) 重要信息资产及其关键安全属性；

b) 关键安全属性的常见威胁和脆弱性；

c) 重要信息资产预期用途；

d) 流程图、过程和过程环境的描述；

组织应确保破坏控制计划（BACCP 计划）和（或）前提方案（PRPs）及时更新。

8.7 监视和测量的控制

组织应提供证据表明所采用的特定监视、测量方法和设备适合于与前提方案（PRPs）和破坏控制计划（BACCP 计划）有关的监视和测量活动。

使用的监测和测量设备应：

a) 使用前按规定的时间间隔进行校准或验证；

b) 必要时，进行调整或再调整；

c) 得到识别，以确定其校准状态；

d) 防止可能使测量结果无效的调整；

e) 免受损坏和失效。

应保留校准和验证结果的文件化信息。所有设备的校准应可溯源至国际或国家的测量标准；当不存在上述标准时，应保留校准或验证依据的文件化信息。

当发现设备或过程环境不符合要求时，组织应对以往测量结果的有效性进行评价。组织应对该设备或过程环境以及任何受不符合影响的重要信息资产采取适当的措施。

评价和相应措施的文件化信息应予以保持。

信息安全安全管理体系（BACCP）中用于监视和测量的软件，应在使用前由组织、软件供应商或第三方进行验证。组织应保持有关验证活动的文件化信息，并及时更新软件。

当发生变更（包括对市售软件的软件配置或修改）时，都应在实施前进行授权、形成文件并确认。

8.8 与前提方案（PRP）和破坏控制计划（BACCP 计划）有关的验证

8.8.1 验证

组织应建立、实施和保持验证活动。验证策划应规定验证

活动的目的、方法、频次和职责。

验证活动应确定：

a) 前提方案（PRPs）得以实施且有效；

b) 破坏控制计划（BACCP 计划）得以实施且有效；

c) 破坏水平在确定的可接受水平之内；

d) 破坏分析的输入已更新；

e) 组织确定的其他措施得以实施和有效。

组织应确保验证活动和监视活动由不同人员实施。

验证结果的文件化信息应予以保留并进行沟通。

当验证是基于重要信息资产样品或过程样品的测试，且测试样品显示不符合信息安全破坏的可接受水平（见 8.5.2.2）时，组织应将受影的重要信息资产作为潜在不安全的重要信息资产（见 8.9.4）处置，并按照 8.9.3 采取纠正措施。

8.8.2 验证活动结果的分析

信息安全小组应对验证结果进行分析，并作为信息安全管理体系（BACCP）绩效评价的输入（见 9.1.2）。

8.9 过程的不符合项控制

8.9.1 总则

组织应该确保关键控制点（CCPs）和操作性前提方案（OPRPs）监视所获得的数据，由具备能力并有权启动纠正和纠

正措施的指定人员进行评价。

8.9.2 纠正

8.9.2.1 当不满足关键控制点（CCPs）的关键限值和（或）操作性前提方案（OPRPs）的行动准则时，组织应对受影响的重要信息资产进行识别，并有对其适宜的控制。

组织应建立、保持和更新文件化信息，包括：

a) 对受影响的重要信息资产进行识别、评价和纠正的方法，以确保对其进行适宜的处置；

b) 评审所实施纠正的安排。

8.9.2.2 当不满足关键控制点（CCPs）的关键限值时，应识别受影响的重要信息资产并将其作为潜在不安全的重要信息资产的处置（见 8.9.4）。

8.9.2.3 当不符合操作性前提方案（OPRPs）的行动准则时，则应执行以下操作：

a) 确定该失效在信息安全方面造成的后果；

b) 确定失效的原因；

c) 确定受影响的重要信息资产并按照 8.9.4 进行处置。

组织应保留评价结果的文件化信息。

8.9.2.4 描述对不符合过程所采取的纠正措施的文件化信息应予以保留，包括：

a) 不符合的性质；

b) 失效的原因；

c) 不符合结果造成的后果。

8.9.3 纠正措施

当不满足关键控制点（CCPs）的关键限值和（或）操作性前提方案（OPRPs）的行动准则时，应评价采取纠正措施的需求。

组织应建立并保持文件化信息，规定适宜的措施以识别和消除已发现的不符合的原因，防止其再次发生，并在识别不不符合后，使过程恢复受控。

这些措施应包括：

a) 评审顾客和（或）监管检查报告中发现的不合格；

b) 评审监视结果可能表明失控的趋势；

c) 确定不不符合的原因；

d) 确定和实施措施，以确保不符合不再发生；

e) 记录所采取的纠正措施的结果；

f) 验证所采取的纠正措施，以确保其有效。

组织应保留所有纠正措施的文件化信息。

8.9.4 潜在不安全的重要信息资产的处置

组织应采取措施防止潜在不安全的重要信息资产在组织开展业务过程时进行利用和流转，包括流入供应商和顾客端，除

非其能证明如下情况：

a) 相关的信息安全破坏已降至规定的可接受水平；

b) 尽管不合格，但仍能满足相关规定的信息安全破坏的可接受水平。

组织应保留已被识别为潜在不安全的重要信息资产在其控制之中，直至对重要信息资产进行评价并确定处置方式。

当重要信息资产在组织的控制之外，并继而确认为不安全时，组织应通知相关方，（适用时）并启动撤回/召回（见8.9.5）。

对潜在不安全的重要信息资产的控制要求、相关方的响应和处理潜在不安全的重要信息资产的授权应作为文件化信息予以保留。

8.9.5 撤回/召回

组织应指定有能力的人员启动和执行撤回/召回，确保及时撤回/召回被确定为潜在不安全的重要信息资产。

组织应建立并保持文件化信息，以便：

a) 通知相关方（如立法和执法部门、顾客和（或）消费者、供应商）；

b) 处置撤回/召回的重要信息资产；

c) 按采取措施的顺序执行。

应保留撤回/召回的原因、范围和结果的文件化信息，并向

最高管理者报告，作为管理评审的输入（见 9.3）。

组织应通过使用适宜技术验证撤回/召回的实施情况和有效性（如模拟撤回/召回或实际撤回/召回），并保留文件化信息。

9 绩效评价

9.1 监视、测量、分析和评价

9.1.1 总则

组织应确定：

a) 需要被监视和测量的内容，包括信息安全过程和控制；

b) 适用的监视、测量、分析和评价的方法，以确保得到有效的结果；

c) 何时应执行监视和测量；

d) 何时应分析和评价监视和测量的结果；

e) 应该由谁对监视和测量的结果进行分析和评价。

组织应保留适当的文件化信息作为监视和测量结果的证据。

组织应评价信息安全管理体系（BACCP）的绩效和有效性。

9.1.2 分析和评价

组织应对监测和测量产生的适当数据和信息进行分析和评

价，包括与前提方案（PRPs，见 8.2）和破坏控制计划（BACCP 计划，见 8.5.4）、内部审核（见 9.2）和外部审核有关的验证活动的结果。

应该执行分析，以便：

a) 确认系统的整体绩效符合组织制定的计划安排和信息安全管理体系（BACCP）要求；

b) 识别更新或改进信息安全管理体系（BACCP）的需要；

c) 识别潜在不安全的重要信息资产发生率较高的趋势；

d) 建立与被审计区域的地位和重要性有关的内部审计方案的规划信息；

e) 提供纠正和纠正措施有效性的证据。

分析的结果和由此产生的活动应该作为文件化信息保留。结果应报告给最高管理者，并且用作管理评审（见 9.3）和信息安全管理体系（BACCP）更新（见 10.3）的输入。

注：分析数据的方法可以包括统计技术。

9.2 内部审核

9.2.1 组织应按计划的时间间隔进行内部审核，以提供有关信息安全管理体系（BACCP）是否符合以下要求的信息：

a) 符合以下要求：

1) 组织对其信息安全管理体系（BACCP）的内部要求；

2) 本文的要求。

b) 已经得到有效实施和保持。

9.2.2 组织应：

a) 计划、建立、实施和保持一项或多项审核方案，其中包括频率、方法、责任、计划要求和报告，其中应考虑到有关过程的重要性、信息安全管理体系（BACCP）的变化，以及监视、测量和以前审核的结果；

b) 确定每次审核的审核准则和范围；

c) 选择合格的审核员，以确保审核过程的客观性和公正性；

d) 确保将审核结果报告给信息安全小组和相关管理者；

e) 保留文件化信息，作为审核计划实施和审核结果的证据；

f) 在约定的时限内进行必要的纠正，并采取必要的纠正措施；

g) 确定信息安全管理体系（BACCP）是否符合信息安全方针的意图（见 5.2）和信息安全管理体系（BACCP）的目标（见 6.2）。

组织的后续活动应该包括对所采取措施的核实以及报告核实结果。

9.3 管理评审

9.3.1 总则

最高管理者应该按计划的时间间隔审查组织的信息安全管理体系（BACCP），以确保其持续的适宜性、充分性和有效性。

9.3.2 管理评审的输入

管理评审应考虑：

a) 以往管理评审的行动状况；

b) 与信息安全管理体系（BACCP）相关的外部和内部问题的变化，包括组织及其背景的变化（见 4.1）；

c) 有关信息安全管理体系（BACCP）的效能和有效性的信息，包括以下趋势：

1) 系统更新活动的结果（见 4.4 和 10.3）；

2) 监视和测量结果；

3) 分析与前提方案（PRP）和破坏控制计划（BACCP 计划）有关的验证活动的结果（见 8.8.2）；

4) 不合格项和纠正措施；

5) 审核结果（内部和外部）；

6) 检查（例如监管机构，顾客）；

7) 外部供应商的绩效；

8) 审查风险和机遇以及为解决这些问题而采取的行动的

有效性（见 6,1）；

9) 满足信息安全管理体系（BACCP）目标的程度。

d) 资源的充裕性；

e) 发生的任何紧急情况、事故（见 8.4.2）或撤回/召回（见 8.9.5）；

f) 通过外部（见 7.4.2）和内部（见 7.4.3）交流获得的相关信息，包括有关各方的请求和投诉；

g) 持续改进的机会。

数据应以适当的方式呈现，以便使得最高管理者能够将信息与信息安全管理体系（BACCP）的既定目标联系起来。

9.3.3 管理评审的输出

管理评审的结果应包括：

a) 与持续改进机会有关的决定和措施；

b) 任何更新和更改信息安全管理体系（BACCP）的需要，包括资源需求以及对信息安全方针和信息安全管理体系（BACCP）目标的修订。组织应保留文件化信息，作为管理评审结果的证据。

10 改进

10.1 不符合和纠正措施

10.1.1 当发生不符合时，组织应：

a) 对不符合做出应对，并在适用时：

1) 采取措施控制和纠正；

2) 处理相关后果。

b) 通过以下方式评价是否需要采取行动消除不符合的原因，避免其再次发生或在其他地方发生：

1) 评审不符合；

2) 确定不符合的原因；

3) 确定类似的不符合是否存在，或可能发生。

c) 实现任何需要的措施；

d) 评审任何所采取的纠正措施的有效性；

e) 必要时，对信息安全管理体系（BACCP）进行变更。

纠正措施应与不符合所产生的影响相适应。

10.1.2 组织应保留文件化信息，以作为以下证据：

a) 不符合的性质以及随后采取的措施；

b) 纠正措施的结果。

10.2 持续改进

组织应持续改进信息安全管理体系（BACCP）的适宜性、充分性和有效性。

通过沟通（见 7.4）、管理评审（见 9.3）、内部审核（见 9.2）、验证活动结果分析（见 8.8.2）、控制措施和控制措施组合（见 8.5.3）的验证、纠正措施（见 8.9.3）和信息安全管理体系（BACCP）更新（见 10.3），最高管理者应确保组织不断提高信息安全管理体系（BACCP）的有效性。

10.3 信息安全管理体系（BACCP）的更新

最高管理者应确保信息安全管理体系（BACCP）持续更新。为实现这一目标，信息安全小组应按计划的时间间隔评价信息安全管理体系（BACCP）。信息安全小组应考虑是否有必要评审破坏分析（见 8.5.2）、既定的破坏控制计划（BACCP 计划，见 8.5.4）和既定的前提方案（PRPs，见 8.2）。更新活动应基于：

a) 来自外部和内部沟通信息的输入（见 7.4）；

b) 关于信息安全管理体系（BACCP）的适用性、充分性和有效性的其他信息的输入；

c) 验证活动结果分析的输出（见 9.1.2）；

d) 管理评审的输出（见 9.3）。

信息安全管理体系（BACCP）更新活动应作为文件化信息

保留，并作为管理评审的输入进行报告（见 9.3）。

参考标准：

[1] ISO 9001: 2015；

[2] ISO 22000: 2016；

[3] HACCP；

[4] ISO/IEC 27001: 2013。