SSE-CMM的过程域

主要内容：11个过程域

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

过程域的通用格式

- PA 01—过程域标题
  - 概述 — 过程域的概要介绍
  - 目标 — 实施该过程域所期望达到的目标
  - 基本实施列表 — 说明每个基本实施的序号和名称
  - 过程域注解 — 任何有关该过程域的其它解释。
- BP 01.01— 基本实施名
  - 描述性的名字 — 对该基本实施的单句描述
  - 描述 — 该基本实施的概括
  - 工作结果示例 — 列出所有可能的输出
  - 注解 — 任何有关该基本实施的其他解释。
- BP 01.02…

关键概念

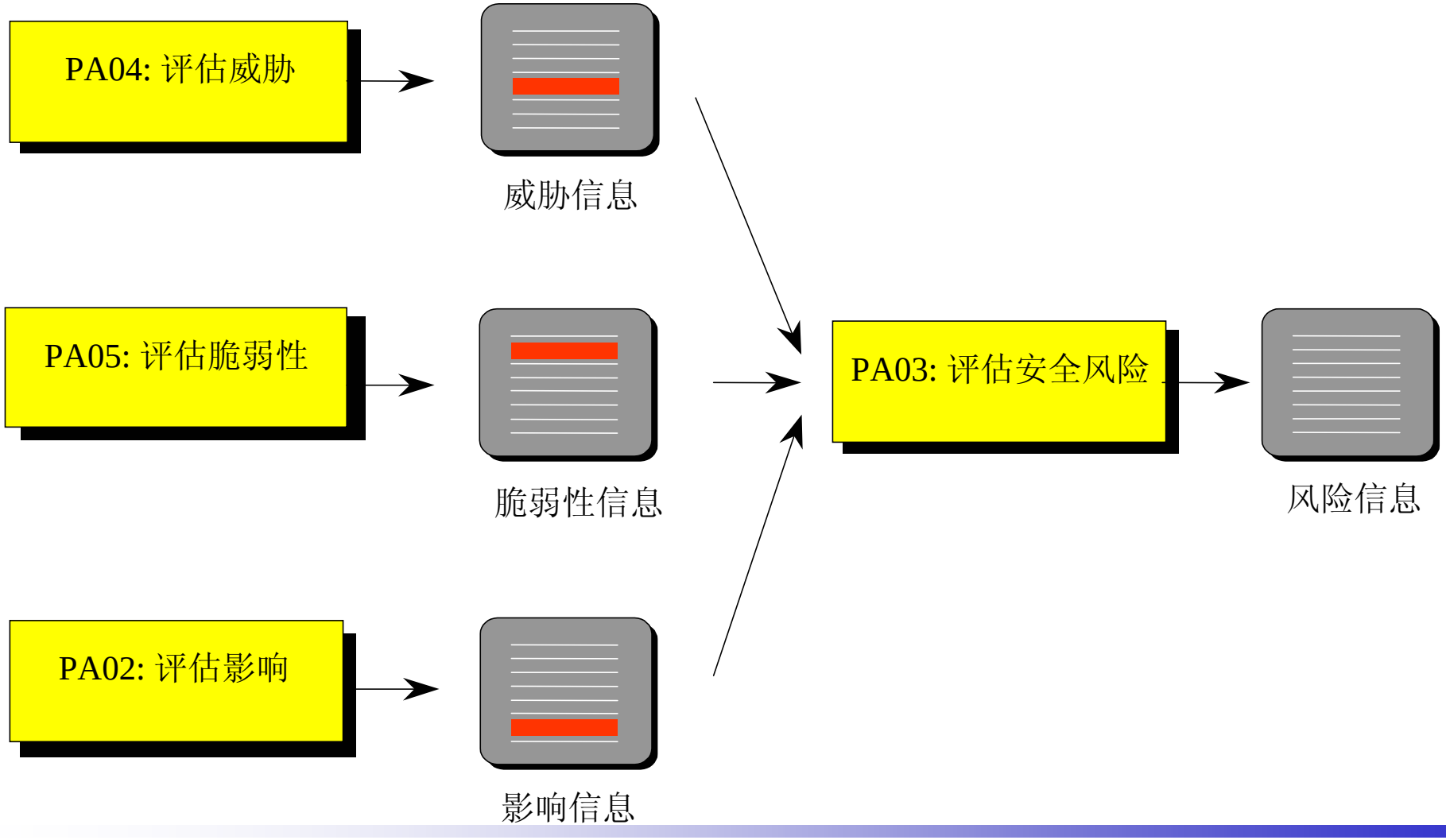
- 工作结果/产品：是指在执行任何过程中产生出的所有文档、报告、文件、数据等。

SSE-CMM不是为每一个过程域列出各自工作结果/产品，而是按特定的基本实施列出其“典型的工作产品”，其目的在于对所需的基本实施范围可做进一步定义。列举的工作结果/产品只是说明性的，目的在于反映组织机构和产品的范围。这些典型的工作结果/产品不是“强制”的产品。

11个过程域

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

与风险过程相关的过程域



11个过程域

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

PA 02 评估影响

- **概述** —评估影响的目的在于识别系统可能受到的影响，并评估这些影响发生的可能性。影响可能是有形的，例如税收或财政罚款的丢失，或可能是无形的，例如声誉和信誉的损失。
- **目标** —确定并描述风险可能对系统带来的安全影响

PA 02 评估影响 （续）

– 基本实施列表 —

- BP 02.01 标识、分析系统的运行、业务或任务功能，并对这些功能的优先级进行排序
- BP 02.02 对支持系统的关键性运行能力或安全目标的系统资产进行标识和描述。
- BP 02.03 选择可用于评估的影响度量准则。
- BP 02.04 对评估中使用的度量准则与所需的转换因子（如果需要）之间的关系进行确定。
- BP 02.05 标识和描述影响。
- BP 02.06 监视影响的不断变化。

BP 02.01 对功能进行优先级排序

描述

- 用来对机构的运行、业务或任务功能进行标识、分析和优先级排列，还应考虑到业务战略可能受到的影线。这些行为将会影响和缓解一个机构可能遭受的影响，也会继而对其他过程域中的风险评估工作产生影响。。

工作结果:

- 系统的优先级列表及安全事件可能对系统功能的影响。
- 系统的能力轮廓——描述系统的能力及其对系统目标的重要性。

BP 02.02 标识系统资产

描述

- 标识出系统中为支持系统安全目标或关键功能（运行功能、业务功能或任务功能）所必需的资源和数据。本基本实施可以通过评估各类资产在给定环境中（对安全目标或关键功能提供支持）的重要性来定义出各类资产/

工作结果:

- 产品资产分析——标识出产品资产及其对系统运行的重要意义。
- 系统资产分析——标识出系统资产及其对系统运行的重要意义。

BP 02.03 选择影响的度量规则

描述

- 有很多度量准则可用于衡量事件的影响。在评估之前，应预先确定采用何种度量准则来评估具体系统面临的影响。

工作结果:

- 选择影响的度量准则

BP 02.04 确定不同度量准则之间的关系

描述

- 某些影响可能需要使用不同的度量准则进行评估。因此必须确定不同度量准则之间的关系，以确保在整个影响评估中使用一致性的方法对所有影响进行评估。在某些情况下，还需要将各种度量准则组合起来，以产生唯一的确定性结果。

工作结果:

- 度量准则的关系列表——描述度量准则之间的关系。
- 度量准则的组合规则——描述不同度量准则之间的组合规则。

BP 02.05 标识和描述影响

描述

- 利用BP02.01和 BP02.02中确定的资产和功能信息来确定安全事件的可能影响。对每一项资产来说，这种影响可能包括资产的破坏、泄露、阻断或丢失。功能的影响可能包括拦截，延迟，弱化。
- 一旦创建了相对完整的影响列表，便可以用BP02.03和 BP02.04中确定的度量准则或度量准则的组合来描述影响。其中可能还要参考机构的保险情况、财政年检等。在评估中，要考察其中的不确定性，并与影响相联系。

工作结果:

- 影响列表——列出可能的影响及有关的度量准则。

BP 02.06 监视影响

描述

- 任何位置和状态下的影响都是动态变化的。新的影响可以变成互为关联。因此，需要监视现有影响并有规律的检查可能的新影响。本基本实施与BP 08.02中的通用性监视活动紧密相连。

工作结果:

- 影响监视报告——描述对影响的监视结果。
- 影响变化报告——描述影响的变化情况。

11个过程域

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

PA 04 评估威胁

- **概述**—评估威胁过程域的目的在于标识安全威胁及其性质和特征
- **目标**—对系统安全的威胁进行标识和描述。

PA 04 评估威胁 （续）

– 基本实施列表 —

- BP 04.01 标识由自然因素所引起的威胁。
- BP 04.02 标识由人为因素所引起的威胁，无意或有意的。
- BP 04.03 标识在一特定环境中的测量单元和适用范围。
- BP 04.04 评估由人为因素引起的威胁主体的能力和动机。
- BP 04.05 评估威胁事件出现的可能性。
- BP 04.06 监视威胁以及威胁特征的变化

BP 04.01 标识自然威胁

描述

- 有自然原因引起的威胁包括地震、海啸和台风等。然而，并非所有的自然威胁都会在所有地方发生。因此，重要的是标识出在一具体地方到底回存在哪一种自然威胁。

工作结果：

- 自然威胁列表——应记录自然威胁的特点和可能性

BP 04.02 标识人为威胁

描述

- 认为原因引起的威胁与自然威胁不一样。它基本有两种类型，偶然原因引起的威胁和故意原因引起的威胁。在某些环境中，因为不涉及到人为威胁，可以在经过分析后取消对人为威胁的考察。

工作结果:

- 威胁概述——描述威胁如何发生作用
- 威胁严重性估计——考察威胁的可能性

BP 04.03 标识威胁的测量单元

描述

- 大量的自然和人为威胁都有其与之相关的测量单元。例：地震的里氏震级。大多数情况下，测量单元的全部尺度并不适用于一次具体的评估。因此，对可能在一个机构中出现的事件，可根据具体情况建立最大和最小测量单元。

工作结果：

- 包含测量单元和位置范围的威胁表

BP 04.04 评估威胁主体的能力

描述

- 确定可能对系统发动攻击的敌人的主观能力和客观能力。主观能力是指一个攻击者所掌握的攻击知识（例：经过的训练和拥有的技能）；客观能力是指一个有能力的敌人实际发动攻击的可能性（例：拥有的资源）

工作结果：

- 对威胁主体的描述——对其能力评估和描述

BP 04.05 评估威胁的可能性

描述

- 对威胁事件发生的可能性进行评估。在评估中需要考虑多种因素，从自然事件的概率到人员的有意或无意行为的概率等均可能需要评估。并不是说这些所有因素都要去计算或测量，但这其中应该有一个一致的度量准则。

工作结果:

- 威胁事件的可能性评估——描述威胁事件的可能性

BP 04.06 监视威胁及其特征

描述

- 任何位置和状态下的威胁都是动态变化的。新的威胁可能出现，现有的威胁也会发生变化。因此，需要有规律的监视现有威胁及特征，并检查可能的新威胁。本基本实施与BP 08.02中的通用性监视活动紧密相连。

工作结果:

- 威胁监视报告——描述对威胁的监视结果。
- 威胁变化报告——描述威胁的变化情况。

11个过程域

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

PA 05 评估脆弱性

- 概述—评估安全脆弱性的目的在于标识和描述系统的安全脆弱性。本过程区包括分析系统资产、定义具体的脆弱性以及对整个系统的脆弱性进行评估。与安全风险和脆弱性评估有关的术语，在许多不同场合的使用是不同的。就本模型的用途而言，“脆弱性”指的是可被利用完成不期望行为的系统的某些特征、安全弱点、漏洞或易被威胁所攻击的系统实施的缺陷。这些脆弱性与任何特定的威胁或攻击的形成并不相干。本过程域的活动在系统生命周期内任何时间都可进行，以支持在已知环境中系统的开发、维护和运行决策。
- 目标—获得对一给定环境中系统安全脆弱性的理解 。

PA 05 评估脆弱性 （续）

– 基本实施列表 —

- BP 05.01 选择对一给定环境中的系统脆弱性进行标识和描述的方法、技术和标准。
- BP 05.02 识别系统安全脆弱性。
- BP 05.03 收集与脆弱性属性有关的数据。
- BP 05.04 评估系统脆弱性并将特定脆弱性及各种特定脆弱性的组合结果进行综合。
- BP 05.05 监视脆弱性的变化及其特征的变化。

BP 05.01 选择脆弱性分析方法

描述

- 包括定义系统的脆弱性分析方法，以对安全脆弱性进行标识和描述，其中还包括脆弱性的分类和优先级排序方案，根据威胁及其可能性、系统的运行功能、安全需求或其他为基础来完成脆弱性的分类和排序。

工作结果：

- 脆弱性分析方法——标识发现并讨论系统安全脆弱性的方法，包括分析、报告和跟踪过程。
- 脆弱性分析格式——描述脆弱性分析结果的格式，以保证分析方法的标准化。
- 攻击方法学及其原理
- 攻击过程
- 渗透研究
- 攻击概要

BP 05.02 标识脆弱性

描述

- 记录系统脆弱性。

工作结果:

- 描述系统的脆弱性列表
- 包括攻击测试结果的渗透性轮廓

BP 05.03 收集脆弱性数据

描述

- 脆弱性有自身的属性。本基本实施旨在收集与这些属性有关的数据。脆弱性被利用的难易程度、脆弱性存在的可能性等数据也应得到标识和收集

工作结果:

- 脆弱性属性表——记录产品或系统的脆弱性的特征。

BP 05.04 综合系统的脆弱性

描述

- 分析那些脆弱性或脆弱性的组合给系统带来的问题。分析中还应确定出该脆弱性的属性特征，例如脆弱性被利用以及被成功攻击的概率，并提出脆弱性的综合分析建议。

工作结果:

- 脆弱性评估报告——包括对系统脆弱性的定量或定性的描述，包括攻击的可能性，成功地可能性以及攻击产生的影响。
- 主动攻击报告——记录攻击的结果以及对结果的分析，包括已发现的脆弱性，被利用的潜在危害以及建议。

BP 05.05 监视脆弱性及其特征

描述

- 任何位置和状态下的脆弱性都是动态变化的。新的脆弱性可以从中产生，现有的脆弱性的特征也会发生变化。因此，需要有规律的监视现有脆弱性及特征，并检查可能的新脆弱性。本基本实施与BP 08.02中的通用性监视活动紧密相连。

工作结果:

- 脆弱性监视报告——描述对脆弱性的监视结果。
- 脆弱性变化报告——描述脆弱性的变化情况。

11个过程域

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

PA03 评估安全风险

- **概述**—评估安全风险的目的在于标识出一给定环境中某一系统的安全风险。这一过程域将基于机构的功能和资产在面对威胁所表现出的脆弱性的理解而确定系统的安全风险。该工作特别涉及到对安全事件“暴露”的可能性进行标识和评估。“暴露”一词指的是可能对系统造成重大伤害的威胁、脆弱性和影响的组合。在系统生命周期的任何时候都可进行这一系列活动，以便支持对已知环境中的系统的开发、维护和运行作出决策。

- **目标**—
  - 获得对在一给定环境中系统运行风险的理解。
  - 按照已定义的原则和方法对风险问题进行优先级排序。

PA03 评估安全风险（续）

– 基本实施列表 —

- BP 03.01 选择用于分析、评估和比较给定环境中系统安全风险所依据的方法、技术和准则。
- BP 03.02 标识威胁/脆弱性/影响三组合（暴露）。
- BP 03.03 评估与每个暴露相关的风险。
- BP 03.04 评估与风险相关的总体不确定性。
- BP 03.05 排列风险的优先顺序。
- BP 03.06 监视风险及其特征的不断变化。

BP 03.01 选择风险分析方法

描述

- 定义用于标识一给定环境中系统安全风险的方法，以对安全风险进行分析、评估和比较。它还包括一个对风险进行分类和分级的方案。该方案将以来与威胁、系统的运行功能、已获知的系统脆弱性、潜在损失、安全需求或其他相关事项。

工作结果:

- 风险评估方法——描述对风险进行识别和描述的方法。
- 风险评估格式——描述对风险进行归档和跟踪的格式，还包括基本描述，重要性和相关性等内容。

BP 03.02 标识暴露

描述

- 标识威胁/脆弱性/影响的三组合（暴露）。标识暴露的目的在于认识这些威胁和脆弱点的利害关系，进而标识威胁和脆弱性造成的影响。这些暴露是选择系统保护措施时必须考虑的

工作结果:

- 系统暴露列表——描述系统所有的暴露。

BP 03.03 评估暴露的风险

描述

- 标识出每一个暴露的可能性。

工作结果:

- 暴露风险列表——计算出的风险列表。
- 暴露优先级表格——对计算出的风险进行优先级排序

BP 03.04 评估总体的不确定性

描述

- 每种风险都有与之相关的不确定性。总体的风险不确定性是在BP04.05评估威胁的可能性， BP05.03收集脆弱性数据， BP02.05标识和描述影响中标识的不确定性的累积。本实施过程与PA06建立保证论据联系紧密，因为保证能用于改变——很多时候是减低——不确定性。

工作结果:

- 与不确定性有关的暴露风险——风险列表中列出的风险应考虑了对不确定性的测量。

BP 03.05 排列风险优先级

描述

- 已经标识的风险应该基于机构的优先安排、风险出现的可能性、与这些因素相关的不确定性以及可用的财力而进行排序。风险可以被减轻，规避，转嫁或接受，也可以使用这些措施的组合。

工作结果:

- 风险优先级列表——列出风险的优先级
- 安全措施需求列表——列出可能有助于减轻风险的安全措施
- 优先级原理——描述优先级的排序原理

BP 03.06 监视风险及其特征

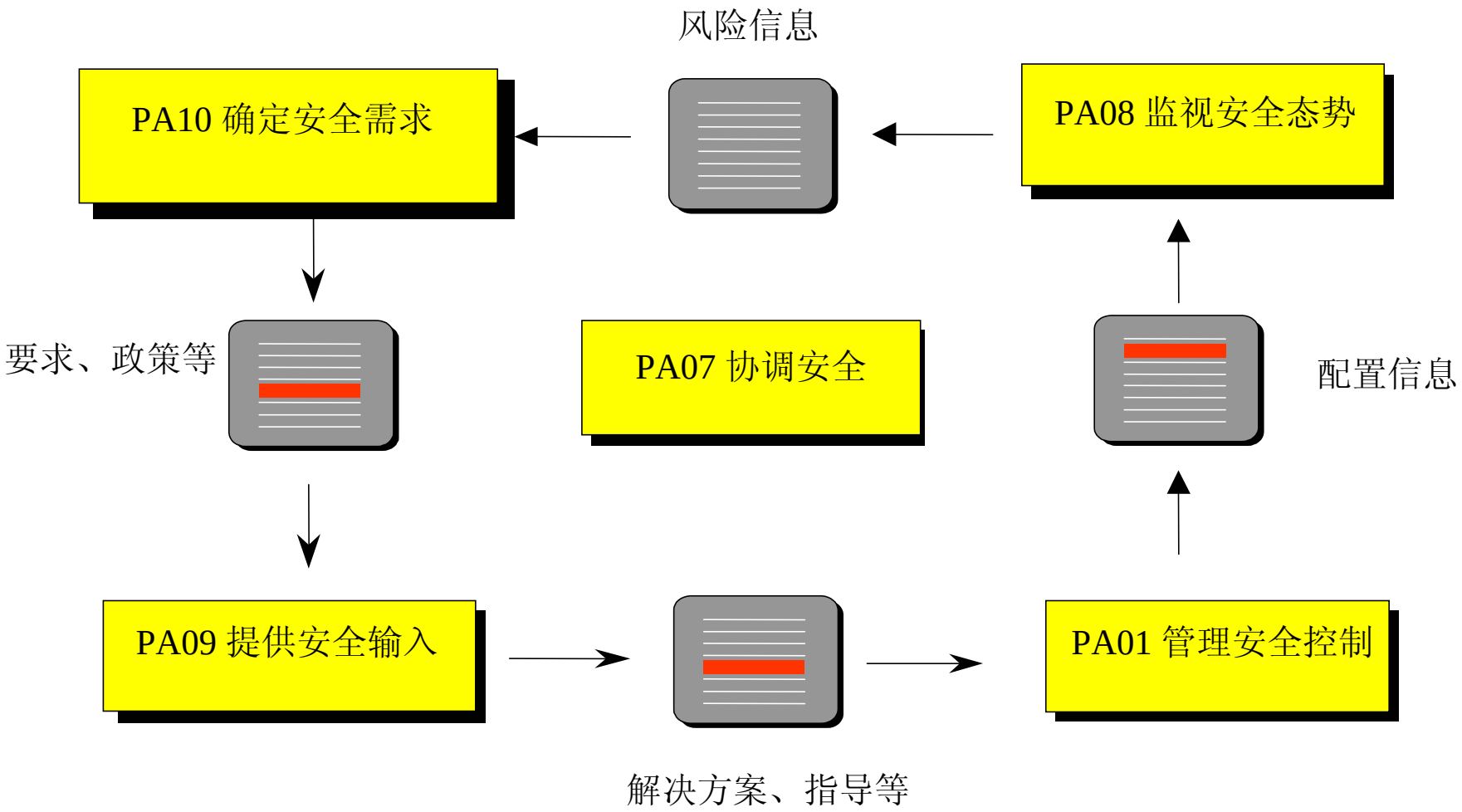
描述

- 任何位置和状态下的风险都是动态变化的。新的风险可能出现，现有的风险也会发生变化。因此，需要有规律的监视现有风险及特征，并检查可能的风险。本基本实施与BP 08.02中的通用性监视活动紧密相连。

工作结果:

- 风险监视报告——描述对风险的监视结果。
- 风险变化报告——描述风险的变化情况。

与工程过程相关的过程域



11个过程域

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

PA10 确定安全需求

- **概述**—确定安全需求的目的在于，明确地标识出系统的安全相关需求。确定安全需求涉及为系统安全定义基本原则，以此满足有关安全的所有法律、策略、组织要求。安全需求应该基于系统的目标运行安全背景、当前的安全和机构的系统环境，以及已标识的安全目标集来进行裁剪。与安全相关的需求集合是在认可系统是参照的系统安全基线。

- **目标**—
  - 在所有团体，包括客户之间达成对安全需求的共同认识。

PA10 确定安全需求 （续）

– 基本实施列表 —

- BP 10.01 获得对客户安全需求的理解。
- BP 10.02 标识出影响到系统的法律、政策、标准、外部影响和有关约束。
- BP 10.03 标识出系统的用途，以此来决定安全背景。
- BP 10.04 对系统运行形成一个高层的面向安全的认识。
- BP 10.05 形成高层目标，以定义系统安全。
- BP 10.06 为系统中实施的保护定义出一套一致的声明。
- BP 10.07 达成一致认识，是具体的安全需求能够满足客户的要求。

BP 10.01 获得对客户安全需求的理解

描述

- 本基本实施的目的在于，收集所有有助于全面理解客户安全需求的信息。这些需求受到安全风险对客户重要性的影响。系统预期运行的目标环境也会影响客户与安全相关的需求。

工作结果：

- 客户安全需求的陈述——对客户安全需求的高层描述

BP 10.02 标识有关的法律、政策和约束

描述

- 本基本实施的目的在于，收集所有可能对系统安全产生影响的外部影响。可能的外部影响包括法律、法规、策略和商业标准。全局和局部政策的优先权应得到确定。必须说明系统客户提出的安全需求，并从中理解其安全意义。

工作结果:

- 安全约束——影响系统安全的法律、政策、法规和其它约束
- 安全轮廓——安全环境（威胁、组织策略）；安全目的（例如，需对抗的威胁）；安全功能和保证需求；在基本原理中要阐述按这些要求开发的系统为什么能够满足其安全目标

BP 10.03 识别系统安全背景

描述

- 本基本实施的目的在于说明系统的背景是如何影响安全的。它涉及对系统（例如，情报、金融、医疗）用途的理解。系统的任务处理和运行概要均要在安全考虑下加以评估。应对系统面临的威胁深入理解。评估性能和功能需求对安全可能产生的影响。运行的约束条件也要受到检查，以考察其对安全的影响。
- 为定义系统的安全边界，环境可能也包括与其它机构或系统的接口。要标识接口组件位于安全边界的内侧或外侧。
- 机构的许多外部因素也影响机构的安全需求。这些因素包括策略上的倾向性和政治重点的改变、技术发展、经济影响、全局性事件以及信息战。由于这些因素没有一个是静态的，因此需要监视和定期地评估这些变化可能造成的影响。

工作结果:

- 预期的威胁环境
- 评估对象——待评估的系统或产品的安全特性（类型、预期的应用、通用特性、使用限制）

BP 10.04 形成对系统运行的安全认识

描述

- 本基本实施的目的在于形成一个高层的、面向安全的认识，包括角色、职责、信息流、资产、资源、人员保护以及物理保护。还要考虑在安全要求的约束下，机构如何运作。这些应在运行安全概念中提出来，而且应该包括对系统体系结构、流程和环境的高层面的安全认识。与系统开发环境有关的要求也要在这一阶段进行收集。

工作结果:

- 运行安全概念——对系统形成面向安全的认识（角色、职责、资产、信息流、过程）
- 概念性安全体系结构——一个安全体系结构的概念性见解；见BP 09.03安全体系结构。

BP 10.05 形成安全的高层目标

描述

- 本基本实施的目的在于，标识出为了向运行环境中的系统提供足够的安全而需满足的安全目标。PA 06“建立保证论据”中确定的系统保证目标也会对安全目标产生影响。

工作结果：

- 运行/环境的安全策略——资产再管理、保护和向机构内外分发时需要遵循的规则、指令和措施。
- 系统安全策略——支配资产怎样被系统或产品进行管理、保护和发布的规则、指令和措施。

BP 10.06 定义安全相关需求

描述

- 本基本实施的目的在于定义系统的安全相关需求。这一实施应确保每个需求与相关的政策、法律、标准、安全要求以及系统的约束条件协调一致。这些需求应完备地定义出系统的安全需求，包括那些通过非技术手段提供的需求。通常有必要定义或确定目标的逻辑或物理边界，以确保所有的方面都被提到。这些需求应与系统目标建立映射关系或发生关联。与安全相关的需求应被清楚地、简明地陈述，而且彼此不应发生矛盾。无论何时，安全都应将对系统功能和性能的任何影响降到最小。安全相关需求将为目标环境中的系统安全性提供评价的基础。

工作结果：

- 安全相关的需求——直接影响系统的安全运行，或要求与具体安全策略相符的有关需求。
- 可跟踪性矩阵——将安全需求映射成解决方案需求方法（例如，体系结构、设计、实现），并进一步映射到测试和测试结果。

BP 10.07 达成对安全得一致性认识

描述

- 本基本实施的目的在于，使所有有关团体能就安全需求达成一致性意见。当讨论普遍性用户时，安全需求要满足安全目标集。具体化的安全应能完备的、一致地反映有关的政策、法律和用户需求。在未达成一致性意见之前，应标识出相关问题，必要时可以返工 。

工作结果:

- 获认可的安全目标——陈述期望目标，以对抗已识别的威胁，和/或遵从已标识的安全策略（已被顾客认可）。
- 安全相关需求的基线——安全相关需求的最小集，得到所有相关团体（特别是客户）的认可。

11个过程域

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

PA09 提供安全输入

- **概述**—提供安全输入的目的在于为系统的规划者、设计者、实施者或使用者提供他们所需的安全信息。这些信息包括安全体系结构、设计或实施的备选方案以及安全指南。同时与基于PA 10“确定安全需求”中标识的安全需求，安全输入可以面向必要的机构成员而产生、分析和提供。此外，还应在这些成员间达成协调。

- **目标**—
  - 应检查系统中所有事项的安全意义，并与安全目标相协调。
  - 项目组所有成员都应理解安全问题，以使他们各司其职。
  - 解决方案中应反映出所提供的安全输入。

PA09 提供安全输入 （续）

– 基本实施列表 —

- BP 09.01 与设计者、开发者和用户的合作，确保各方对安全输入需求达成共同的理解。
- BP 09.02 判断在工程选择时所需的安全约束和安全考虑。
- BP 09.03 标识出与安全相关的工程问题备选解决方案。
- BP 09.04 利用安全约束和考虑因素对工程的备选方案进行分析并区分优先级。
- BP 09.05 向其它工程组提供安全相关的指南。
- BP 09.06 向运行系统的用户和管理员提供与安全相关的指南。

BP 09.01 理解安全输入要求

描述

- 安全工程与其它领域相协调，以判断这些领域所需的安全输入的类型。安全输入包括安全相关的指南、设计、文档或思想。输入可以为多种形式包括文档、备忘录、电子邮件、培训和咨询。
- 这些输入基于PA 10“确定安全需求”中的安全需求。例如，软件工程师就可能需要一套安全规则支持其工作。同系统相比，某些输入与环境的关联性更强。

工作结果:

- 安全工程和其它领域间达成的一致性意见——定义安全工程如何向其它领域提供输入（例如，文档、备忘录、培训、咨询）
- 对所需输入描述——对安全输入的每一类提供机制做出标准化定义

BP 09.02 确定安全约束和考虑

描述

- 本基本实施的目的在于为工程选择确定出所有的安全约束和考虑。安全工程组完成分析，从而为需求、设计、实现、配置和文档等确定出所有的安全约束和考虑。安全约束可在系统生命期内的所有时间进行标识，并且可在许多不同的抽象层上进行标识。注意这些约束或是肯定（总是如此）或是否定（绝对禁止如此）。

工作结果:

- 安全设计标准——对整个系统或产品设计作决定时所需的安全约束和考虑。
- 安全实施原则——用于系统或产品实施（例如，使用特定机制、编码标准）的安全约束和考虑。
- 文档要求——对支持安全需求所需的特定文档（例如，管理员手册、用户手册、特定设计文件）的标识。

BP 09.03 标识安全备选方案

描述

- 本基本实施的目的在于标识出与安全相关的工程问题的备选解决方案。这一过程要反复进行，将安全相关的需求转化为具体的实现。这些解决办法可以多种形式提供，如体系结构、模型和原型。本基本实施涉及对安全相关需求的分解、分析和重组，直到确定有效的备选方案 。

工作结果:

- 系统体系结构的安全考虑——理论层次上描述系统各关键组件在满足安全需求方面的相互关系
- 安全设计文档
- 安全模型——对系统实施的安全策略进行形式化，必须标识出系统在管理、保护和发布信息时所使用的规则集和措施。
- 安全体系结构——关注系统体系结构的安全问题，描述与安全有关的规则、基础性概念、功能和服务
- 依赖性分析（保护措施的关系及其赖性）

BP 09.04 分析工程备选方案的安全性

描述

- 本基本实施的目的在于分析和排列工程备选方案的优先级。 使用BP 09.02中确定的安全约束和考虑，安全工程师可以评估每个工程备选方案，并向工程组提交建议。此外，安全工程组还应考虑其它工程组的工程指南。
- 这些工程备选方案不限于BP 09.03所标识的安全备选方案，还可以包括来自其它领域的备选方案。

工作结果:

- 对各种研究结果和建议作平衡——联系BP 09.02中标识的安全约束和考虑因素，对所有工程的备选方案作分析
- 对各研究结果进行端到端平衡——对整个产品、系统或过程的整个生命周期中各种决策进行分析的结果，关注于那些为了满足其它目标（例如，成本、功能性）而对安全做出缩减的区域。

BP 09.05 提供安全工程指南

描述

- 本基本实施的目的在于，制定安全相关的指南，并把它提供给工程组。安全工程指南由工程组用来对体系结构、设计和实现作出决策。

工作结果：

- 体系结构建议——包括能支持可满足安全需求的系统体系结构开发的约束和原则。
- 设计建议——包括指导系统设计的原则或约束
- 实现建议——包括指导系统实现的原则或约束
- 安全体系结构建议——包括定义系统安全特性的原则或约束
- 保护的理念——对如何实施安全的高层次描述，包括自动的、物理的、个人的以及管理机制
- 设计标准、理念、原则——关于系统如何设计的约束（例如，最少的特权、隔离安全控制）
- 编码标准——关于系统如何实现的约束

BP 09.06 提供运行安全指南

描述

- 本基本实施的目的在于，开发与安全相关的指南并提供给系统用户和管理员。本运行指南告诉用户和管理员在以安全的方式进行安装、配置、运行和终止系统。为确保这一目的，运行安全指南的开发应在生命周期内提早开始。

工作结果:

- 管理员手册——描述系统管理员以安全的方式安装、配置、运行和终止系统时的作用和权力
- 用户手册——描述系统提供的安全机制及这些机制的使用指南
- 安全轮廓——安全环境（威胁、组织策略）；安全目标（例如：要对抗的威胁）；安全功能和保证需求；在基本原理中要阐述按这些要求开发的系统为什么能够满足其安全目标
- 系统配置指南——确保运行能满足安全目标的系统配置要求

11个过程域

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

PA01 管理安全控制

– 概述 —管理安全控制的目的在于确保已集成到系统设计中的预期的系统安全性确实能够在最终系统运行状态中实现。

– 目标 —安全控制能得到正确地配置和使用

– 基本实施列表 —

- BP 01.01 建立安全控制的职责和可追究性，并通知到机构中的每一个人
- BP 01.02 管理系统安全控制的配置
- BP 01.03 管理所有的用户和管理员的安全意识、培训和教育项目
- BP 01.04 对安全服务及控制机制的定期维护和管理

PA01 管理安全控制（续）

过程域注解 —

- 本过程区面向的是安全控制机制的管理和维护活动，这些安全控制机制将在开发环境和运行系统中得到管理和维护。
- 本过程区将进一步确保安全级别不会随时间发展而降低。
- 对一个新设备的控制管理应该集成到现有设备的管理控制中去。

BP 01.01 建立安全职责

描述

- 本过程应确保安全责任人员的行为能够得到追踪（既可追究性），并授予安全责任人相应的行动与权力。
- 同时也应该确保所采用的所有安全控制是明确的并且一致性的应用。
- 此外还应该确保所采纳的安全管理结构，不但要通知管理层内的所有人，而且也应通知整个机构。

BP 01.01 建立安全职责 （续）

工作结果

- 一个机构的安全结构图表—标识出机构中与安全有关人员及其角色。
- 文档化安全角色—描述每个与安全有关的组织角色及其职责。
- 文档化安全职责—详细描述每个安全职责，包括预期的职责表现及职责的审查与实施。
- 文档化安全责任（可追究性）—描述谁对有关安全的问题负责，确保所有的风险均可追踪到责任人。
- 文档化安全权限—标识一个机构中每个成员允许做的事情。

BP 01.02 管理安全配置

描述

- 所有设备的安全配置需要管理。由于系统安全很大程度上依赖于许多相关组件（硬件、软件与程序），而常规配置管理实施不必关心安全系统所需的互相关联性。

BP 01.02 管理安全配置（续）

工作结果

- 所有软件更新的记录— 记录系统的所有软件与软件更新的许可证、序列号和回执，包括日期、个人责任和修改描述。
- 所有发布问题的记录— 包括对软件发布期间所遇到的任何问题以及怎样解决它的描述。
- 系统安全配置— 它是一个描述系统硬件、软件及通信的当前状态的数据库，包括硬件位置、软件发布和相关的信息。
- 系统安全配置的修改— 描述对系统安全配置的任何修改，包括修改人的名字、修改的描述、修改的理由以及修改的时间。
- 所有确认的软件更新记录— 一个跟踪软件更新的数据库，包括修改的描述、修改人的名字以及修改的时间。

BP 01.02 管理安全配置（续）

工作结果

- 可信软件发布的定期综述— 描述最近的可信软件发布活动，注意到出现的任何困难和作用情况。
- 安全需求更改— 跟踪对系统要求所作的任何修改，修改的原因可能是基于安全理由或对安全有影响。这样有助于保证修改及其作用是合乎安全策略的。
- 对设计文档进行安全修改— 跟踪对系统设计文档所作的任何修改，修改的原因可能是基于安全理由或对安全有影响。这样有助于保证修改及其作用是合乎安全策略的。
- 安全控制实现— 描述系统中安全控制的实现，包括配置的详细情况。
- 安全审查— 描述相对于所希望控制实现的系统安全控制的当前状态。
- 控制撤销— 描述删除或取消安全控制的程序，包括过度控制计划。

BP 01.03 管理安全意识培养、培训和教育项目

描述

– 所有员工的安全意识培养、培训和教育都需要管理，其管理方式与其需要管理的意识、培训和教育管理方式相同

工作结果

- 用户对安全培训材料的审查
- 所有意识培养、培训和教育活动的日志和培训结果
- 对用户关于安全意识培养、培训中掌握的知识水平的定期评估
- 培训、意识培养及教育材料的记录

BP 01.04 管理安全服务及控制机制

描述

- 安全服务及机制的一般管理类似于其它服务及机制的管理，这包括保护它们避免破坏、偶然事故和人为故障，并与法律和政策要求一致。

BP 01.04 管理安全服务及控制机制（续）

工作结果

- 维护和管理日志— 根据系统安全机制对维护、完整性检查和运行检查进行记录。
- 定期的维护和管理检查— 包括对最近的系统安全管理及维护工作的分析。
- 管理和维护失效— 跟踪记录系统维护方面的问题以便标识需要额外关注的地方。
- 管理和维护例外— 内容包括对正常管理及维护程序的例外情况的描述，其中包括该例外情况出现的原因和持续的时间。
- 敏感信息清单— 描述系统中各种类型的信息和这些信息应怎样得到保护。
- 敏感介质清单— 描述系统中存储信息所用的各种类型的介质和每种介质应怎样得到保护。
- *净化*、降级和撤消— 描述一些保证在信息敏感性降低或者介质被净化或处置后，不出现不必要风险的程序。

11个过程域

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

PA 08 监视安全态势

- **概述**—监视安全态势的目的在于确保标识并报告所有的可能导致安全问题的所有安全违规、试图的违规或错误。监视外部和内部环境可能对系统安全造成影响的所有因素。

- **目标**—
  - 探测和跟踪内部和外部安全有关的事件。
  - 根据策略，响应突发事件。
  - 根据安全目标，标识并处理运行中安全态势所发生的改变。

PA 08 监视安全态势 （续）

– 基本实施列表 —

- BP 08.01 分析事件记录，以确定事件的原因，过程以及将来可能出现的事件。
- BP 08.02 监视威胁、脆弱性、影响、风险和环境方面的变化。
- BP 08.03 识别与安全相关的突发事件。
- BP 08.04 监视安全措施的性能和功能的有效性。
- BP 08.05 检查系统的安全状态，确定有必要对系统实施的修改。
- BP 08.06 管理对相关安全相关事件的响应。
- BP 08.07 确保安全监视的结果得到适当的保护。

BP 08.01 分析事件记录

描述

- 检测安全相关性信息的历史和事件记录（包括日志记录）。通过多条记录中的相关事件所用元素，应该能识别出感兴趣的事件。之后，多条事件记录可以融和为一条事件记录。

工作结果:

- 描述每个事件——识别出每个探测到的事件的来源、影响和重要性。
- 建立日志记录和来源——从各种来源生成安全相关事件的记录。
- 事件标识参数——描述系统各部分能够和不能够收集的事件。
- 列出所有目前的单个日志记录报警状态——标识根据单个日志记录采取行动的所有要求。
- 列出所有目前的单个事件报警状态——找出根据事件采取行动的所有要求，这些事件由多个日志记录形成。
- 定期报告已出现的所有报警状态——将从多个系统得到的报警列表进行综合处理并作初步分析。
- 日志分析和归纳——对最近出现的报警进行分析并报告损耗的结果。

BP 08.02 监视变化

描述

- 查找可能影响当前安全态势有效性的任何变化，不管这种影响是正面的还是负面的。
- 任何系统实施的安全应该与威胁、脆弱性、影响和风险相关联，因为它们与系统的内部和外部环境有关。这些因素没有一个是静态的，而变化既影响有效性，也影响适应性。必须监视所有因素的变化，并分析这些变化以评估它们对安全有效性的影响。

工作结果：

- 变化报告——识别出任何可能影响系统安全态势的内部或外部变化。
- 定期评估这些变化对安全的影响——对安全态势的变化进行分析，确定它们的影响和作出响应的需要。

BP 08.03 识别安全突发事件

描述

- 判断是否发生了安全事件，说明事件的详细情况，并在必要时做出报告。安全事件可利用历史事件的数据、系统配置数据、完整性工具和其它系统信息来检测。由于某些事件会经过一个较长周期时间后才出现，因此这种分析可能涉及到与系统长时间状态进行比较。

工作结果:

- 事件列表和定义
- 事件响应指南
- 事件报告
- 每一次所检测到的入侵事件报告
- 定期作出事件摘要

BP 08.04 监视安全防护措施

描述

- 检测安全措施的性能，以标识出安全措施性能的变化 。

工作结果:

- 对安全措施做出定期的状态描述——描述现有安全措施的状态，以检测出可能的错误配置或其它问题。
- 对安全措施做出定期的状态摘要描述——提供对现有安全措施的状态摘要，指出事件趋势、需要进一步增加安全性的区域以及减缓安全性后可能节约的成本。

BP 08.05 检查安全态势

描述

- 由于威胁环境、运行需求和系统配置等方面会出现变化，一个系统的安全态势可能会发生改变。本实施在于复查系统中实施安全的理由，并审查对其他工程领域或方面提出的安全需求。

工作结果：

- 安全性复查——包括描述当前安全风险环境，现有的安全态势和进一步查看安全态势对安全风险的针对性。
- 风险接受检查——由适当的正式授权机构提供声明，以表明运行该系统有关的风险是可以接受的。

BP 08.06 管理安全突发事件响应

描述

- 在许多情况中，系统的连续可用性是非常关键的。由于许多事件不能预防，因而对破坏的响应能力是至关重要的。应急计划要求标识出允许系统失效的最长时间；标识出系统中的重要功能组件；标识出并制定恢复战略和计划；测试这个计划；维护这个计划。
- 在某些情况中，应急措施可能包括对突发事件的响应和与攻击者（例如：病毒、黑客等等）的对抗。

工作结果:

- 系统恢复优先级列表
- 测试时间安排
- 测试结果
- 维护时间表
- 突发事件报告
- 定期检查
- 应急计划

BP 08.07 保护安全监视的记录数据

描述

- 如果监视活动的成果不可信任，那么监视活动就没有价值。本实施包括对相关日志、审计报告和相关分析结果的封存和归档。

工作结果：

- 列出全部归档的日志和相应的保存周期——标识安全监视结果的存储位置，以及废弃日期。
- 对应归档的日志的现场定期检查结果——描述已经丢失的报告并标识出必要的响应。
- 归档日志的使用——识别出归档日志的使用者，包括访问时间、目的及任何注解。
- 定期对随机选择的归档日志的实施有效性和可用性测试的结果——分析随机选取的日志并确定它们是否完整、正确和有用，以确保能对系统安全进行的充分监视。

11个过程域

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

PA 07 协调安全

- **概述**—协调安全的目的在于保证所有团体都有一种参与安全工程活动的意识，并确实能够参与到安全工程活动中。由于安全工程不能独立地取得成功，所以这种参与工作是至关重要的。这种协调涉及到要保持所有项目人员与外部团体之间的开放交流。多种机制可以用于在这些团体之间协调和沟通安全工程的决策和建议，包括备忘录、文档、电子邮件、会议和工作组。

- **目标**—
  - 项目组的所有成员都要具有并参与安全工程工作的意识，才能充分发挥他们的作用。
  - 有关安全的决策和建议是相互沟通和协调一致的。

PA 07 协调安全 （续）

– 基本实施列表 —

- BP 07.01 定义安全工程协调目标和相互关系。
- BP 07.02 标识出安全工程的协调机制 。
- BP 07.03 促进安全工程的协调。
- BP 07.04 用标识出的机制去协调有关安全的决策和建议。

BP 07.01 定义协调目标

描述

- 许多团体需要有一种参与安全工程的意识，并的确的参与到安全工程活动中。要通过检查项目结构、信息需求和项目要求来决定与这些团体共享信息的目标。建立与其他团体之间的联系和承诺（义务关系）。成功的联系可有许多形式，但必须被全体参与的团体所知晓、接受。

工作结果:

- 信息共享协议——描述团体间共享信息的过程，标识参与团体、介质、格式、期望值和频率。
- 工作组的成员关系和日程表——描述本机构的工作组，包括他们的成员、成员的角色、目的、进度和后勤。
- 组织标准——描述各工作组之间及用户之间沟通安全相关信息的过程和程序。

BP 07.02 识别协调机制

描述

- 有许多方法可以与其他工程组共享安全工程的决策和建议。本活动识别在项目中协调安全的不同方法。

  在同样一个项目上有多个安全组是常见的。这些情况下，所有的工作组都应该为了一个共同的目标而工作，接口标识、安全机制选择、培训及开发工作都需要以某种方式进行，以保证每个安全组件放置在运行系统中时都能如愿工作。另外，所有工程组必须理解安全工程工作及其活动，以便使安全能完好地集成到系统中去。客户也必须知晓有关安全的事情和工作，以确保安全需求能得到恰当地标识和考虑。

工作结果:

- 交流计划——包括用于工作组成员之间以及与其它团体之间需要共享的信息、会议日期、过程和程序。
- 通信基础设施的要求——标识工作组成员之间以及与其它团体之间共享信息需要的基础设施和标准。
- 会议报告、报文、备忘录的模板——描述各种文档的格式，保证标准化和有效的工作。

BP 07.03 促进协调

描述

- 成功的关系依赖于良好的促进手段。在具有不同优先级（重要性）的不同机构之间进行沟通有可能会发生一些冲突。本基本实施确保争端以合适的、富有成果的方式得到解决。

工作结果：

- 冲突解决的程序——标识出有效解决机构中实体之间和实体内部冲突的方法。
- 会议议程、目标、行动条目——描述会议中讨论的议题、强调需要阐述的目标和行动项。
- 行动项的跟踪——确定行动项的工作和解决的计划，包括职责、时间表和优先级。

BP 07.04 协调安全决定和建议

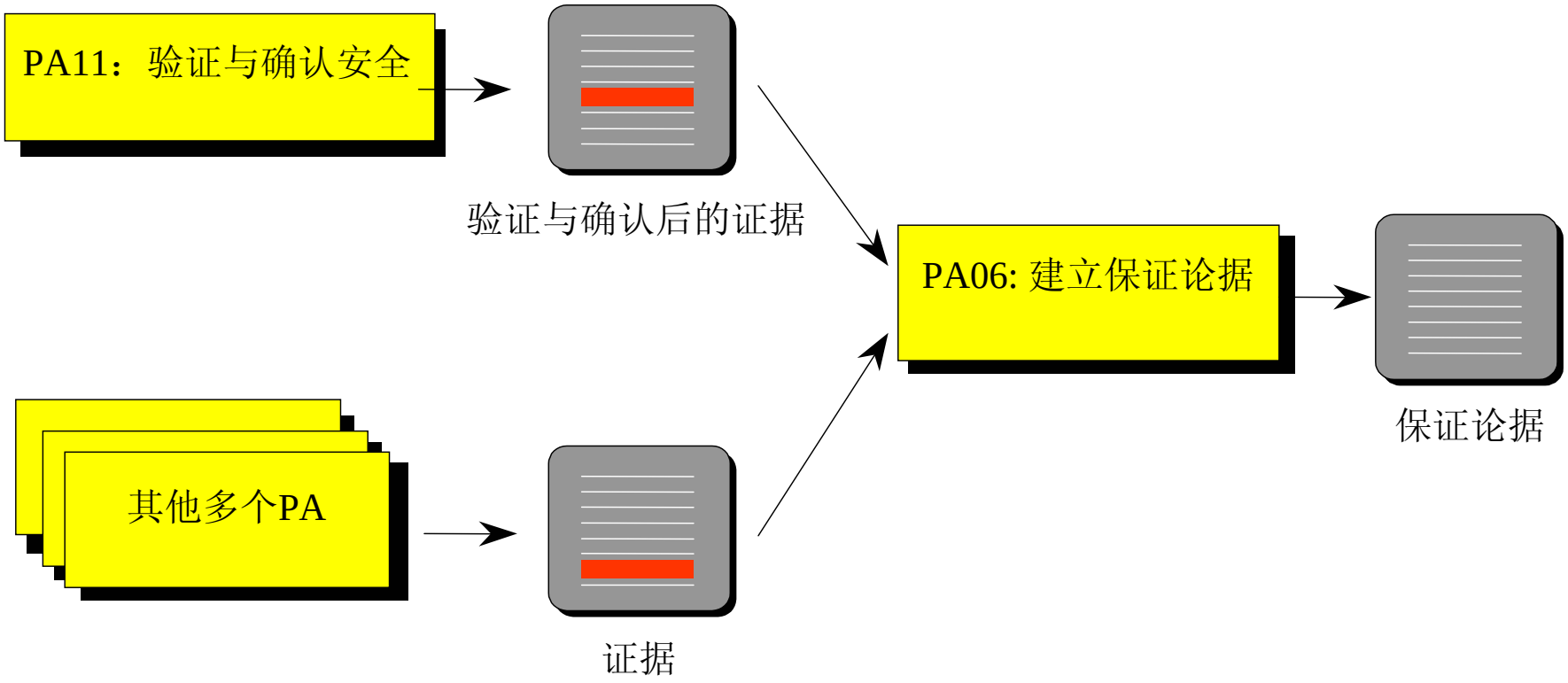
描述

- 本基本实施的目的在于在各种安全工程师、其他工程组、外部实体及其他可能的团体中沟通安全决策和建议 。

工作结果:

- 决定——通过会议报告、备忘录、工作组会议纪要、电子邮件、安全指南或公告牌将有关安全的决策在相关团体间进行交流。
- 建议——通过会议报告、备忘录、工作组会议纪要、电子邮件、安全指南或公告牌将有关安全的建议在相关团体间进行交流。

与保证过程相关的过程域



11个过程域

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

PA11 验证与确认安全

- **概述**—验证和确认安全的目的在于确保工程解决办法能够得到验证和确认。通过观察、示范、分析和测试，解决方案要在安全需求、体系结构和设计等方面得到检查。客户的运行安全验证将进一步对该方案提供确认。

- **目标**—
  - 解决方案满足安全需求
  - 解决方案满足客户运行安全需求 。

PA11 验证与确认安全 （续）

– 基本实施列表 —

- BP 11.01 标识待验证和确认的解决办案。
- BP 11.02 定义验证和确认的办法和严格程度。
- BP 11.03 验证解决办案是否实现了与上一抽象层相关的要求。
- BP 11.04 验证解决办案是否能最终满足客户的运行安全需求
- BP 11.05 为其他工程组收集验证和确认的结果。

BP 11.01 标识验证和确认对象

描述

- 本基本实施的目的在于，分别地标识出验证和确认的对象。验证行为可证明解决方案已得到了正确地实施，而确认行为则证明了解决办法是有效的。它也涉及与整个生命周期内所有工程组的协调。

工作结果：

- 验证和确认计划——对验证和确认工作的定义（包括资源、时间表、验证和确认的工作结果）

BP 11.02 定义验证和确认方法

描述

- 本基本实施的目的在于，定义验证和确认的方法和严格程度。标识过程涉及到选择那一种方法去对工程中每个需求实施验证和确认。严格程度可说明出验证和确认的力度和粒度，这要受到PA 06“建立保证论据”中保证战略的影响。例如，某些项目只对需求的符合性进行简单地审查，而另一些则可能要求非常严密的检查。
- 这一方法论还应包括维护可跟踪性的手段，跟踪的内容很多，从客户的运行安全需求到安全需要，到解决办法，到验证和确认结果的方法。

工作结果:

- 测试、分析、演示和观察计划——定义出验证和确认方法（例如，测试、分析）和严格程度（例如，非正规或正规的方法）
- 测试流程——定义测试每种解决办法时所采取的步骤。
- 跟踪方法——描述验证和确认结果如何能跟踪到客户的安全要求和需求。

BP 11.03 实施验证

描述

- 本基本实施的目的在于，验证解决方案是否实现了上一抽象层相关的要求，包括PA 06“建立保证论据”中所标识的保证要求，从而验证解决方案是正确的。有许多验证需求的方法，包括测试、分析、观察和演示。所用的方法在BP 11.02中标识。局部需求和整个系统的需求都要受到检测。

工作结果:

- 来自测试、分析、演示和观察得出的原始数据——验证办法实施后的结果。
- 问题报告——在验证解决办案能否满足需求过程中发现的不一致。

BP 11.04 实施确认

描述

- 本基本实施的目的在于验证解决办案能否最终满足客户的运行安全需求。许多种方法可以用来完成这项工作，包括在一个运行环境，或有代表性的测试环境中去测试解决办案。所使用的方法应在BP 11.02中被标识。

工作结果：

- 问题报告——在验证解决办案能否满足需求这一过程中发现的不一致。
- 不一致——标识出何处出现了解决方案不能满足安全需要的情况。
- 无效的解决办法——不能满足客户安全需要的解决办案。

BP 11.05 提供验证和确认的结果

描述

- 本基本实施的目的在于为其他工程收集并提供验证和确认的结果。验证和确认的结果应以某种易被理解和使用的方式所提供。所有结果应被跟踪，以确保需求、解决办案，到测试结果的可跟踪性。

工作结果:

- 测试结果——测试的结果文档
- 可跟踪性矩阵——将安全需求映射成解决方案需求方法（例如，体系结构、设计、实现），并进一步映射到测试和测试结果。

11个过程域

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

PA 06 建立保证论据

- **概述** —建立保证论据的目的在于清楚地告诉客户，其安全需求已获满足。一个保证论据是一系列清晰陈述的保证目标。这些目标是由多个保证证据所支持，保证证据的来源和抽象级各不相同。
  - 本过程包括标识和定义保证需求；证据的产生和分析活动；支持保证需求所需的附加证据。此外，对这些活动所生成的证据进行收集、整理并准备提交。
- **目标** —工作结果和过程要清晰地向客户提供其需求已获满足的证据

PA 06 建立保证论据 （续）

– 基本实施列表 —

- BP 06.01 标识安全保证目标
- BP 06.02 定义面向所有保证目标的安全保证战略。
- BP 06.03 识别并控制安全保证证据
- BP 06.04 对安全保证证据进行分析
- BP 06.05 提供安全保证论据，以证明客户的安全需求得到满足

BP 06.01 标识安全保证目标

描述

- 由客户确立的保证目标显示了用户对系统安全性的信任程度。系统安全保证目标规定了系统安全策略所提供的安全可信程度。该目标的充分性由开发者、集成者、客户和签字机关共同确定。
- 对新增的的安全保证目标或已有目标的修改的均须得到确认，该工作要在工程机构内部和外部安全相关人员间得到协调（例如客户、系统安全认证机构、签字机关、用户等）。
- 为反映变化，应不断的更新安全保证目标。需要对安全保证目标作出的修改情况 包括客户、系统安全认证机构、签字机关、用户等对可接受风险程度的变化。
- 安全保证目标必须清晰地沟通，以确保没有异议。如有必要，应加入合适的解释。

工作结果：对安全保证目标的陈述

BP 06.02 定义保证战略

描述

- 安全保证战略的目的在于规划并确保安全目标能够正确地实现。安全保证战略在实施中所产生的证据应能（向系统的签字机关）提供一个可接受的信心级，使其确信系统的安全措施足以管理安全风险。通过制定和实施安全保证战略，可实现对保证活动的有效管理。对保证需求的尽早标识和定义对于产生必要的支撑性证据是必要的。通过不断外部协调来理解和查看客户对保证需求的满意程度，这有助于确保得到高质量的保证需求包。

工作结果:

- 安全保证战略——描述用于满足客户安全保证目标的计划，并标识应负责的责任方

BP 06.03 控制保证证据

描述

- 安全保证证据要根据安全保证战略中的定义，通过与所有安全工程过程域相互配合，在不同抽象层面上标识出保证证据。这些证据要受到控制，以确保他们对当前的工作结果来说具有通用性，对安全保证目标来说具有关联性。

工作结果:

- 安全保证证据仓库（例如，数据库、工程记录、测试结果、证据日志记录）——在开发、测试和使用期间产生的所有证据要在库中存储，可以采用数据库、工程记录、测试结果或证据日志记录等多种形式。

BP 06.04 分析证据

描述

- 引入保证证据分析，是为了保证所收集的证据能满足安全目标，从而满足顾客的安全需求。对保证证据的分析可说明系统安全工程和安全验证过程是否充分且足够，因而是否可以判断安全机制和安全特性是否令人满意的被实现。此外，对保证证据的分析，确保了工程实施结果相对于基线系统是完善和正确的。当保证证据不充分或不足够的情况下，本分析可能导致对支持安全安全目标的系统、安全工作结果和过程进行必要的修订。

工作结果:

- 保证证据分析结果——标识和概述保证证据仓库中证据的强度和不足。

BP 06.05 提供保证论据

描述

- 开发出一个全面的安全保证证据，以表明对安全保证目标的遵循性，并将保证证据提供给客户。保证论据是一系列已声明的保证目标的集合，由多层抽象度的保证证据所支持。为了满足安全目标，必须对提交证据中的缺陷和安全保证目标中的缺陷进行审查。

工作结果:

- 含有支撑性证据的保证论据——由各种保证论据支持的一个结构化的保证目标集。