联邦信息系统与机构中安全与隐私防护的评估

建立高效的评估方案

核心问题

怎样获得**较高的成本转化率**?

如何依照特定的信息系统因地制宜地**定制评估计划**?

如何保证组织中在评估等方面的**一致性**?

机构中不同团体应怎样**合作**?

信息系统

硬件软件固件等技术的复杂结合体/
机构的成功在很大程度上依赖于信息系统的职能作用/

为信息系统所用的安全与隐私防护需要被评估，以提供必要的信息来帮助对其综合有效性的判定。安全与隐私防护的综合有效性则帮助确定该机构的操作和资产，对个体，对其他机构乃至对国家所带来的风险。

制定标准的目的是
帮助联邦政府实现更安全的信息系统

- 对安全控制和隐私控制进行**更一致、可比较和可重复的评估**，并获得可再现的结果;
- 促进对由于联邦信息系统的运行和使用而对机构运营、机构资产、个人、其他机构和国家造成的**风险的理解**;
- 促进对安全及隐私控制进行具有**更高成本效益的评估**，以判定整体管制的有效性;和
- 为机构官员创建**更完整、可靠和值得信赖的信息**，以支持风险管理决策、评估结果的互惠、信息共享，以及遵守联邦法律、行政命令、指示、法规和政策。

评估是一项信息收集活动而非安全或隐私的产出活动。

在已知威胁和漏洞信息，操作注意事项，信息系统对平台的依赖程度和对风险的容忍度的情况下，并为基于机构的政策和要求，在提供必要灵活性的基础上，制订对信息系统中安全与隐私控制的评估流程，并保证促进安全和隐私水平的一致。

应当根据确定特定评估所需的投入水平和保证需求，在最具成本效益的方式完成评估目标，并有足够的信心支持随后确定所产生的任务或业务风险。

在控制评估期间所产生的信息，可用于:

- 识别机构在实施风险管理框架时可能存在的问题或不足;
- 识别信息系统和系统运行环境中与安全和隐私相关的弱点和缺陷;
- 优先考虑风险缓解决策和相关风险缓解活动;
- 确认已识别的信息系统中与安全和隐私相关的弱点和缺陷在运行环境中已得到解决;
- 支持监控活动和信息安全和隐私态势感知;
- 促进安全授权决策、隐私授权决策和正在进行的授权决策;和
- 告知预算决策和资本投资流程。

2.0. 评估安全与隐私防护相关的基本内容

安全与隐私评估可以在系统开发生命周期的**多个阶段**有效实施，
从而使开发者相信这些被用于该信息系统或继承于其他信息系统的安全与隐私控制在其运用过程中是有效的。

安全评估常规来说是由系统开发者与系统集成商在系统开发生命周期中的开发/收购和实践阶段进行的。
隐私防护评估是由隐私管理处的高级机构官员和员工在系统开发生命周期的早期阶段进行的

评估和检测的**频率**会由机构或信息系统拥有着活通用控制提供者决定，并需要受到授权官员的批准。

在系统开发不同阶段进行评估的目的

起始阶段：
保证系统所需的安全与隐私控制是合理设计与开发和正确使用的，并保证在该系统被投入使用与维护阶段之前，能够与已确立的机构信息安全体系构架保持一致。

操作与维护阶段：
确保安全与隐私防护在操作环境中是仍然有效的，且面对持续进化的各种威胁仍然能起到有效的保护作用。

收尾阶段：
确保重要的机构信息在产品被出售之前已经被清除掉。隐私评估的进行则用于以确保其已遵守机构保留计划。

2.2 实施控制评估的策略

制订有广泛基础的，全机构范围的策略

↓

加速对整个信息系统范围内的高成本转化率的，一致的评估

以RMF
(Risk Management Framework)
起步

安全分类 → 以一种机构层面的视野，结合信息关键性与敏感性，以及企业体系构架和信息安全体系构架 → 确保各个单体系统的分类是基于机构的任务和业务目标的

安全与隐私控制的选择
（包括对通用控制的识别） → 最大化一个机构中通用控制的数量

- 显著降低开发成本；
- 允许机构集中和自动控制评估，从而分期偿还评估整个机构进行多个信息系统评估所带来的成本；
- 提高安全的连贯统一与隐私控制。

一个全机构范围的，能在RMF使用早期识别通用控制的方法，能加快形成一个更加全面化的，评估这些控制方法并且使信息系统持有者和授权官员共享必要的评估结果的策略的形成。

与核心机构官员共享必要的信息系统评估结果有以下好处：

- 提供检查所有信息系统评估结果的能力，与依据符合机构特点和信息系统安全分类已经风险评估，作出任务/业务相关的风险减轻活动的决定的能力；
- 提供一种对整个机构的信息系统中，系统性缺点和弱点的更加全面的大观，以及一个开发解决全机构范围内信息安全与隐私问题的对策；
- 提高机构对威胁，易受攻击性的了解，以及针对通用信息安全和隐私问题的有更高成本效益的解决策略。

机构还可以促进一种**更加目标明确的具有更高成本效益的评估过程**的形成，通过：

- 为其具体操作环境与需求开发更加具体的评估过程（而不是把这些任务降级给各控制评估师或者评估团队）；
- 提供可用全机构使用的工具，模版和技术，以此来支持在机构中更加连贯一致的评估。

以及与利益相关团体的合作…

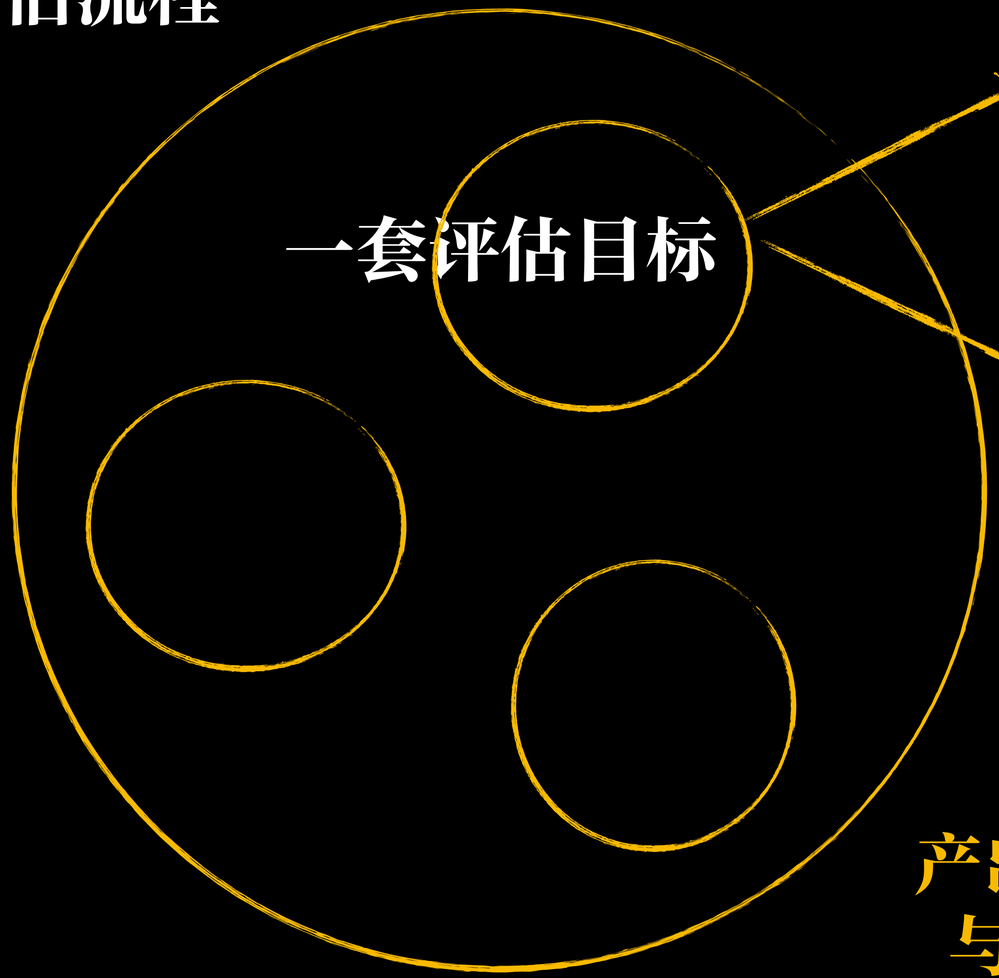
2.3. 建立一个有效的保证案例(Assurance Case)

保证案例是一个证据体，它组织成一个论证，以证明某些有关信息系统的主张成立（即有保证）。当需要证明一个系统具有一些复杂的特性（如安全性、安全性或可靠性）的时候，就需要一个保证案例。

- 在系统开发生命周期过程中收集各种该信息系统正常运行，产出符合预期的操作和产生所希望的结果从而达到该系统与该组织关于安全与隐私要求的证据；
- 用一种可以使得决策者能在作出基于风险的与操作或系统使用的决定时，能有效利用的方式来，呈现这些证据。

评估师所获得的证据使得合适的机构官员能够针对安全与隐私控制以及信息系统的整体安全隐私状态作出客观决定。

2.3. 评估流程



一套相关的可能的评估方法与对象

一套关于评估中特定安全与隐私控制的决定声明

决定声明与安全或隐私防控内容有关（即安全/隐私防控功能），以此保证评估结果到基础操作要求的可溯源性。

产出的评估结果用于帮助人们对安全与隐私防护的整体有效性做出决断

评估对象

指出了具体的需要被评估的事物，并附以

1．明确说明	与信息系统相关的基于文件的工件（如：政策，流程，计划，系统安全与隐私要求，功能规范，构架设计等）
2．机制	信息系统所使用的具体硬件，软件和固件保护措施和对策。
3．活动	支持一个信息系统的具体的保护相关的包括人的动作（例如：实施系统备份操作，监控网络交通，演习应急计划等）。
4．个人	个人，或者个人群体，是应用以上说述的明确说明，机制，活动的人。

评估方法

1. 定义了评估师行为的本质。

审查Examine

查阅，观察，研究或者分析一个或多个评估对象的过程（即明确说明，机制或者活动）
便于评估师理解，澄清疑惑或者获得证明。

问讯Interview

通过举行组织中个人与个人或个人团队之间的讨论，
从而又一次促进评估理解，澄清疑惑或获得证明。

测试Test

是一次或多次地在具体条件下运用评估对象（即活动或机体）
来比较实际产出行为与理想产出行为之间的差距。

评估方法

2. 用相关数字，深度和覆盖面分级定义评估的人力投入水平

深度属性

基本的（basic），聚焦的（focused）和全面的（comprehensive）

描述了审查，问讯和测试的严格程度和详细程度

闻讯Interview

描述了审查、问讯和测试过程的范围和广度，

包括了明确说明文件的数量和类型，机制，待审查和测试的活动，需要从他处问讯的个人的数量和类型

一个特定的评估方法所采用的深度和覆盖属性值是由机构所提供的明确的评估需求而定的。

随着开发，实施和操作过程中评估需求的升高，评估活动的严格性和范围也会随之增加

CP-9	INFORMATION SYSTEM BACKUP 信息系统备份		
	评估目标： 判断该机构是否：		
	CP-9(a)	CP-9(a)[1]	定义了一个与恢复时间目标及该信息系统的应急计划相同说制订的恢复点目标一致的频率，以进行该信息系统中用户级别信息的备份。
		CP-9(a)[2]	以机构定义的频率来进行该信息系统中用户级别信息的备份
	CP-9(b)	CP-9(b)[1]	定义了一个与恢复时间目标及该信息系统的应急计划相同说制订的恢复点目标一致的频率，以进行该信息系统中系统级别信息的备份。
		CP-9(b)[2]	以机构定义的频率来进行该信息系统中系统级别信息的备份
	CP-9(c)	CP-9(c)[1]	定义了一个与恢复时间目标及该信息系统的应急计划相同说制订的恢复点目标一致的频率，以进行该信息系统中包括安全相关记录在内的信息系统记录备份。
		CP-9(c)[2]	以机构定义的频率来进行该信息系统中包括安全相关记录在内的信息系统记录备份。
	CP-9(d)	保护了在储存位置的备份信息的机密性，完整性和可获得性	
	可能需要用到的评估方法与对象： 审查：【从以下选择：应急计划政策；处理信息系统备份的流程；应急计划；备份储存位置；信息系统备份登陆或记录；其他相关文件或记录】 问讯：【从以下选择：机构中对信息系统备份负责的员工；机构中对信息系统安全负责的员工；】 测试：【从以下选择：组织中实施信息系统备份的过程；全自动化的支持或实施信息系统备份的机件；】		

CP-9(3)	信息系统备份 | 关键信息各自的储存位置		
	评估目标： **判断该机构是否：**		
	CP-9(3)[1]	CP-9(3)[1][a]	定义了关键性的信息系统软件和其他需要将备份储存在一个独立设施的安全相关信息；或者
		CP-9(3)[1][b]	定义了关键性的信息系统软件和其他需要将备份储存在一个并非位于操作系统中的防火容器中的安全相关信息；或者
	CP-9(3)[2]	定义了关键性的信息系统软件和其他需要将备份储存在一个独立设施的安全相关信息或者一个并非位于操作系统中的防火容器中的安全相关信息中；	
	可能会使用到的评估方法与对象： 审查：【从以下选择：应急计划政策；处理信息系统备份的流程；应急计划；备份储存位置；信息系统备份登陆或记录；其他相关文件或记录】 问讯：【从以下选择：机构中对信息系统备份负责的员工；机构中对信息系统安全负责的员工；】		

左：安全控制的评估流程

右：安全控制加强版的评估流程

安全内容自动化协议（SCAP）

用于支持安全控制评估过程并促进更加有效和更高的成本转化率的评估。

SCAP是一个集合，其中收集了与基于一种赋予SCAP许可的工具之间互操作性的标准格式来实现证明的收集自动化与描述自动化相关的明确说明。

SCAP的明确说明中定义了评估标准的格式，也叫做SCAP内容，可以被交换和提供给评估工具。这个内容可以使用来使来自机器和人类制作的证明的收集和评估过程自动化。SCAP还定义了捕获和支持说收集的结果和评估工件给出的结果的交换所使用的格式。通常，可以使用SCAP来收集和评估的面向机器的构件与机制有关(例如，配置设置、已安装的硬件/软件、对策的操作状态)。此外，可以使用Open Checklist Interactive Language (OCIL)收集面向人的工件，例如那些与明确说明规范和活动相关的工件。OCIL是一个SCAP的组件规范，支持收集基于标准的格式和闻讯数据在标准格式下的表达。SCA的自动化解决方案的内容驱动特性可以用于支持对安全和隐私控制做出灵活并且连贯一致的评估。

3.0. 实施有效的安全与隐私防护评估的过程

3.1. 评估前的准备

一系列与评估的费用，进度和执行表现有关的问题。

- **从机构的角度准备：**

确保政策对涵盖安全和隐私控制评估的适当涵盖到位，并为所有受到其影响的组织元素所理解;
确保在安全或隐私控制评估步骤之前，RMF中的所有步骤都已成功完成，并受到了适当的管理监督；
确立评估的目标和范围（即评估的目的和正在评估的内容）
……

- **安全与隐私管制评估师/评估小组对各自的评核工作的方法的准备：**

对机构的运营(包括任务、功能和业务流程)有总体了解，以及作为特定评估的对象的信息系统如何在组织运营中起到支持作用;
了解该信息系统的结构（即系统体系构架）以及正在评估的安全或隐私控制（包括特定于系统的、混合的和通用的控制）；
…

- **机构在选择安全或隐私控制评估人员时**，既需要考虑其技术能力，也要考虑其独立性的高低。机构需要确保评估人员拥有对特定于系统的、混合的和通用控件进行成功的评估所需的技能和技术专长。

3.2 研发安全与隐私评估计划

步骤

- 根据安全计划和隐私计划的内容以及评估目的和范围，确定哪些安全和隐私控制/控制加强版本将被包括在评估中;
- 根据评估中所包含的安全或隐私控制和控制加强版本，选择在评估过程中所使用的适当的评估流程;
- 定制选定的评估流程(例如，选择合适的评估方法和对象，分配深度和覆盖率属性值);
- 开发额外的评估程序，以解决特殊出版物800-53没有充分涉及到的一些安全要求或隐私要求或控制;
- 优化评估程序，减少重复工作(例如，对评估程序进行排序和整合)，并提供高成本转化率的评估解决方案;
- 完成评估计划，并获得执行计划所必需的批准。

3.2 研发安全与隐私评估计划

- 根据安全计划和隐私计划的内容以及评估目的和范围，确定哪些安全和隐私控制/控制加强版本将被包括在评估中;
- 根据评估中所包含的安全或隐私控制和控制加强版本，选择在评估过程中所使用的适当的评估流程;
- 定制选定的评估流程(例如，选择合适的评估方法和对象，分配深度和覆盖率属性值);
- 开发额外的评估程序，以解决特殊出版物800-53没有充分涉及到的一些安全要求或隐私要求或控制;
- 优化评估程序，减少重复工作(例如，对评估程序进行排序和整合)，并提供高成本转化率的评估解决方案;
- 完成评估计划，并获得执行计划所必需的批准。

- 选定满足提出的评估目标的合适的评估方法与对象;
- 选择合适的深度和覆盖率属性值，以确定评估的严格程度和范围;
- 识别出单独记录的安全评估计划或隐私评估计划已评估过的通用控制，且不需要重复执行评估流程;
- 开发适用于特定的信息系统/特定平台的或特定机构的评估流程（这些流程可能可以由所提供的流程改编得到）
- 收录以往的评估中其结果被认为是可用的的评估结果
- 对评估程序作出适当调整，以便能够从外部提供者那里获得必要的评估证据

与评估方法和对象相关的考虑—

被选择的评估方法和对象是那些在产出用于决定声明中的做出决定的证据，被认为是必要的方法和对象。

评估过程中的潜在/可能用到的方法和对象被作为资源提供，以帮助适当的方法和对象的选择，而非为了限制选择。

机构使用他们的判断选择潜在的评估方法并选择与每个被选择的方法相关联的评估对象列表。

机构倾向于选择那些以最高成本转化率的方式来对确定与评估目标相关的决定的做出贡献的方法和对象。

对评估结果的质量的衡量是基于所提供的逻辑依据和原因的可靠性的，而不是所应用的具体方法和对象。在大多数情况下，没有必要将每一种评估方法都应用于每一个评估对象上以获得预期的评估结果。而对于某些评估而言，使用一种目前并未列在潜在方法列表中的方法可能是更加合适的。

与深度和覆盖范围相关的考虑

机构所选择的值是基于正在被评估的信息系统的特征(包括保证需求)以及要做出的具体决定而定的。深度和覆盖范围的属性值与机构明确要求的保证需求相关(即评估的严谨程度和范围与保证需求呈直接正相关关系)。对于安全控制，SCAP检查单提供了基于概要文件的机制，该机制允许根据一个信息系统所期望的保证需求定制属性值和选择特定的控制需求。这些检查单使得使用经过SCAP验证的产品进行可定制的自动化评估成为可能。

与通用控制相关的考虑

通用控制可能曾经作为机构的信息安全程序或隐私程序的一部分被评估，或者作为信息系统的一部分被评估，而该信息系统提供被其他组织系统继承的通用控制。也可能有单独的计划用于评估通用控制。

如果通用控制还没有被评估或需要重新考虑,以作出必要安排来在当前评估中包括或者提及通用控制评估结果。

通用控制的某些特定于系统的方面有时不被负责该控件的通用方面的机构实体所涵盖。这些类型的控件被称为混合控件。

与系统/平台和机构相关的考虑

用于针对处理特定于某系统和某平台或特定于机构的依赖关系。

与评估证据再利用相关的考虑

在确定总体安全或隐私控制有效性的证据体中，考虑重用以前被接受或被批准的评估结果。以前被接受或被批准的评估包括: (i) 被该机构管理和支持的多种信息系统的通用控制的评估；(ii) 作为控制执行的一部分被审查的安全或隐私控制的评估(例如CP-2要求审查应急计划)；(iii)机构信息安全持续监控程序中产生的与安全有关的信息；在安全控制评估或隐私控制评估中使用以前的评估结果的可接受性，由评估结果的用户协调和批准。至关重要的是，信息系统所有者和通用控制提供者必须与授权官员和其他适当的机构官员合作，以确定使用以前评估结果的可接受性。在考虑重用以前的评估结果和这些结果对当前评估的价值时，评估师需要确定: (i) 评估证据的可信度； （ii）从前的分析的适当性；(iii）评估证据在当前信息系统运行状况的适用性。如重复使用以前的评估结果，则应当在安全评估计划或隐私评估计划以及安全评估报告或隐私评估报告中记录原始评估的日期和评估类型。如果适用，SCAP工具提供的标准化安全评估结果可以被多团体重复使用。

- **随时间变化的与安全控制和隐私控制相关的情况**
- **从以前的评估到现在所经过的时间**
- **以前的评估的独立程度**
- **与外界信息系统相关的考虑**

3.2.1 决定哪些安全或隐私控制将会被评估

3.2.2 选取评估安全或隐私控制的流程

3.2.3 定制评估流程

3.2.4 为机构专用的控制研发评估流程

3.2.5 优化选定的评估程序以确保最大化的效率

- 合并和巩固评估流程以节省成本
  - 调整评估安全性或隐私控制的顺序:
  - 在其他控制之前对某些安全控制和隐私控制进行评估，提供有用的信息，促进理解并帮助更有效地评估其他控制。

3.2.6 完成评估计划并获得执行计划的批准

3.3. 进行安全与隐私控制评估

3.3. 进行安全与隐私控制评估

安全评估计划或隐私评估计划经组织批准后，评估师或评估小组将按照商定的时间表执行该计划。确定评估团队的规模和团队构成(即技能集,技术专长和组成团队的个人的评估经验)是依据机构要求和发起评估所做出的风险管理决策的一部分。

评估摘要可向授权官员提供一份简要的评估报告，报告集中关注了评估的强调部分，主要调查结果的梗概，以及针对所评估的安全或隐私控制中的弱点和缺陷而提出的解决建议。

评估目标是通过将指定的评估方法应用于选定的评估对象，产生下列结果之一：(i) 满意(S)或 (ii) 非满意(O)。

评估师的调查结果是关于所评估的安全或隐私控制方面的发现所做出的公正，真实的报告。对于每一项非满意的调查结果，评估师会指出安全或隐私控制中被结果所影响到的部分(即在控制方面被认为不满意的或不能被评估的部分)，并描述该控制与计划或预期状态的差异。评估人员还在安全或隐评估报告中还应提到，非满意的结果会对机密性、完整性和可用性造成损害的潜在可能性。这种表示法反映了由于缺乏特定的保护，开发可能导致出现的结果。

3.4 分析评估报告结果

由高级机构官员对评估报告中的评估结果定义风险危机程度与资源分配优先级。最终，评估结果和任何后续减轻措施(由更新后的风险评估知会)由信息系统所有者或通用控制提供者，与指派合作机构官员合作，来触发被认证官员用于判断信息系统安全或隐私状态关键文件的更新及其对进行授权操作的适用性的更新。这些文件包括安全计划和隐私计划、安全评估报告和隐私评估报告，以及各自的行动计划和转折点。

3.5 评估安全和隐私性能

当机构采用性能(Capability)的概念时，自动化和手工评估都需要考虑到所有包含安全或隐私性能的安全控制和隐私控制。评估师知道控制是如何协同工作来提供这些性能的。这样，当评估识别出性能中的某种失败时，就可以根据控制之间建立的关系，进行对根本原因的分析，以确定对失败负责的特定控制或基于控制间关系而对该失败负责的控制。

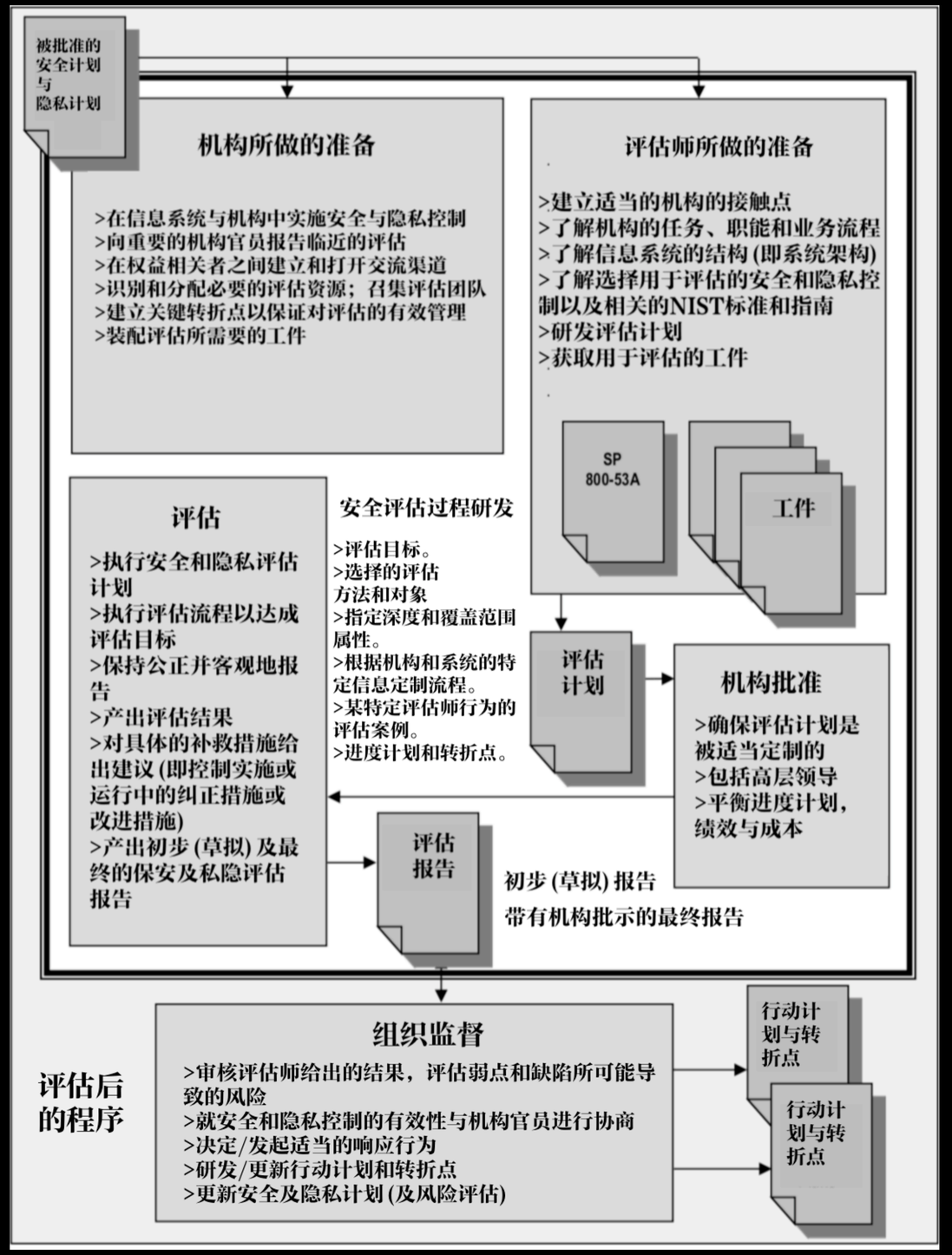
对由信息系统处理，存储或传输的信息的保护,很少来自单一的安全保障或对策。

通过采用性能的概念，机构可以获得对下事物的更大的可见性和更好的理解：

A. 控制间的关系(即依赖关系);
B. 特殊控制在机构定义的性能上的失败导致的影响;
C. 控制的弱点或缺陷的潜在严重程度。

但是，这种方法可能会增加评估的复杂性，并且当特定的功能受到特定安全性或隐私控制失败的影响时，需要对根本原因进行故障分析，以便确定哪些控制或控制导致了故障。机构定义的性能中包含的控制越多，就越难以确定导致失败的根本原因。定义的性能之间也可能存在交互，这可能会增加评估的复杂性。

如果发现一个控件既没有对定义的性能做出贡献，也没有对系统的总体安全性做出贡献，那么机构将重新访问RMF步骤2，定制控制集，并在安全计划中记录根本原因。



包括评估前，中，后期实行的活动在内的安全与隐私控制的评估过程的总结