2021 安全规划：安全流程成熟度的“定级、评审、整改”

随着高管层对网络安全的了解日益增强，在面临安全风险的任何领域，高管层都想知道：我们面临着哪些风险？我们的安全状况如何？我们对存在的安全风险该怎么办？安全运营指标很少能引起以业务为导向的高管层的共鸣，而安全流程成熟度则更好理解，也能够更有效得向高管层介绍公司的风险状况（请参见《安全之殇：如何将安全建设与商业价值挂钩》）。

大多数组织机构都有一定的安全基础，并不一定要从头开始制定全新的安全流程。相反，他们需要根据现有流程所处的发展阶段和成熟度情况进行修改、调整（请参见《2021 安全规划：三步搞定安全流程管理》）。但对于现有的安全流程，该如何进行安全成熟度评估呢？评估之后，又该如何逐步提高安全流程成熟度的级别，增强安全防御能力呢？

提高安全流程成熟度是提高企业安全计划的成本效益、向高管层展示安全计划的商业价值的一个有效方式。如果安全流程还不够成熟，那么，组织机构的安全管理计划可能会效率很低，甚至可能无效。**因此，对安全流程成熟度进行评估，并提高成熟度级别成为安全负责人进行年终总结汇报或为新一年制定安全规划时的关键一环。**下文，我们将对安全流程成熟度的“定级、评审、整改”进行详细介绍。

定级：成熟度级别

综合考量组织机构在管理流程、人员、技术、工具以及企业文化等因素后，通常可以将安全流程的成熟度划分为五个级别，其所表示的功能也是递增的：

- **级别 1：初始阶段**——管理层意识到企业安全防御能力很弱，并且会带来不可接受的风险。安全活动通常是临时性活动，以 IT 为重点。在大多数情况下，没有正式的安全防御计划。
- **级别 2：制定中**——高管层临时任命 CSO 来制定安全计划和策略。相关方开始就安全问题进行非正式交流。
- **级别 3：明确确定**——制定了安全策略和规则，并且确定了一些安全角色及其职责；但是，几乎没有问责制，也没有强制执行。安全工作仍主要集中在 IT 方面，并且企业安全意识仍然有限。
- **级别 4：管理完善**——已经对安全角色及其职责进行了明确定义，并且已经建立了由 CSO 领导、由业务管理者参与的正式安全委员会。企业正在从以 IT 为中心的方法转向网络安全。但是，业务线仍不接受相关的剩余风险。
- **级别 5：持续优化**——业务管理者现在已经明确接受所面临的剩余风险，并会对安全故障和违反安全策略承担全部责任。已经跨多个领域持续进行自我完善，并且可以确保组织机构内的人员都具有安全意识。

成熟度级别	描述
第1级-初始阶段	√采取的安全流程是临时的、孤立的和混乱的。 √只有个别人支持开展安全活动，但没有正式的安全计划，整个组织机构实施安全计划的意识或接受度有限。
第2级-制定中	√制定了安全发展愿景，并获得了高管层的支持。 √评估安全需求，分配职责并制定了安全实施计划。 √确定在安全管理的哪些方面存在差距。 √将安全计划在整个组织机构中推广落实。
第3级-明确定义	√已明确确定了目标、实践和绩效指标。 √制定了标准化的安全流程，还可进行有效集成，且已实施。 √正式的治理和合规模型已落实。
第4级-管理完善	√安全流程已成为企业文化的一部分，是企业运营和决策不可或缺的一部分。 √安全流程的实施效果是高度可预测的。
第5级-持续优化	√安全流程已完全成熟。 √所有安全投资都和业务决策关联在一起。 √随着人员、技术和业务需求的变化以及机会的出现，根据相关方反馈对安全流程进行持续的调整和优化。

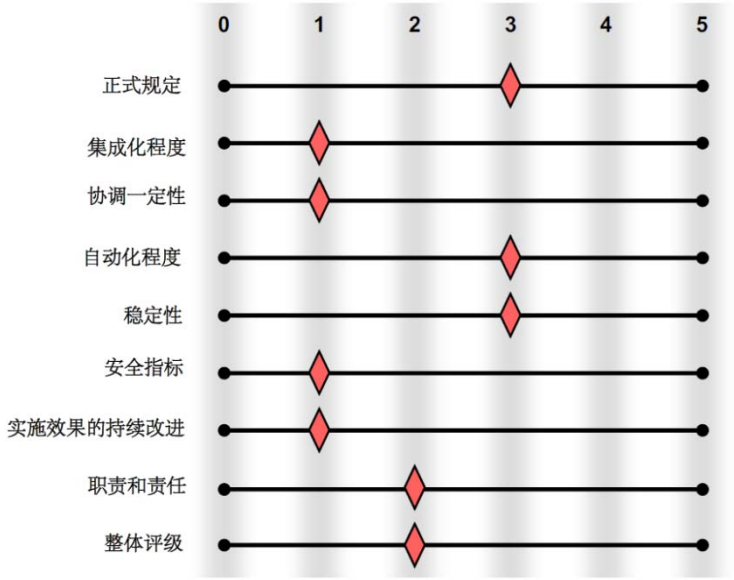
评审：安全流程成熟度评估标准

通常可以通过以下标准来评估流程成熟度：

- **正式规定**——在多大程度上对安全流程做出了正式规定、进行了记录并付诸实践？
- **集成能力——**安全流程与其他相关流程之间的集成程度如何？这不仅包括与其他安全流程的集成，还包括与相关操作和服务管理流程的集成。例如，安全事件响应流程通常与 IT 问题管理流程集成在一起。
- **协调一致性**——安全流程在多大程度上促进或阻碍了组织团队之间的协作？安全流程在设计时要最大程度地减少涉及到的不必要的组织层级。
- **自动化**——就安全流程的性质来说，在多大程度上实现了自动化？重要的是要考虑某个流程是否适合自动化。例如，补丁管理流程可能更适合自动化，而涉及人际交流和沟通的地方则不太适合。
- **稳定性**——安全流程的变更频率如何？任何新流程不可能从一开始就是完美无缺的，安全流程刚制定下来时通常需要进行多次调整，才能实现新流程的预期效果。
- **指标**——与安全流程相关的特定指标有用吗，合适吗？指标是否实际用于衡量和追踪安全流程的实施效果？是否可以通过指标了解安全流程的价值？
- **实施效果**——指标能在多大程度上促进安全流程的持续改进？流程的有效性和效率是否随着时间的推移而提高？安全流程的预期实施结果是否已实现？
- **职责和责任**——已确定的人员在多大程度上接受并执行各自的职责和责任？

维度/阶段	初始阶段	制定中	明确定义	管理完善	持续优化
正式规定	未确定	有些文档记录	有正式规定	优化对安全流程的定义	持续改进安全流程的定义
集成能力	无集成或临时集成	集成能力有限	可以与安全和运营流程集成	与运营流程集成	全面集成；定期改进
协调一致性	无法实现协调一致	组织架构决定了流程	流程决定组织架构	实现了协调一致性，并持续优化	定期改进
自动化	无自动化	开始研究自动化方案	实施基本的自动化	有限的工具集成	全面的工具集成
指标	没有制定指标	主要是效率指标	效率与服务级别指标	用于持续改进的指标	用于监控变更影响的指标
实施效果	未确定	效果差	制定并实现了预期目标	效果可靠，并不断优化实施目标	持续改进
职责与责任	不正式或不存在	制定了治理结构	确定并接受职责与责任	完成并优化职责与责任	改进职责与责任分配

对安全流程成熟度进行自我评估本质上是一种非常主观的做法。但是，只要尽可能诚实地进行评估，最大程度地做到公开透明，这也是一种有效方法，可以指出在哪些领域存在改进的机会，也可以说明企业的安全状况。



整改：如何提高安全流程成熟度级别

对于成熟度，安全人员最关心的问题是——如何逐渐提高安全流程成熟度。从一个成熟度级别发展到下一个级别并没有那么简单。通常，大多数组织机构至少需要一年的时间才能提高到一个级别。但也并不是所有组织机构都需要达到最高成熟度级别。实际上，对于许多组织机构来说，这可能是完全不现实的——要么是因为不需要采取最严格的安全控制，要么是因为实施成本过高。下面我们介绍五个成熟度级别中每个级别的关键特征，并推荐了提升到下一个生熟度级别所需的改进措施。

从 1 级到 2 级

在 1 级成熟度时，组织机构通常没有正式的安全防御计划，也没有指定的个人承担总体的安全责任。安全活动通常是承担 IT 职责的人来完成。但由于开展的安全实践活动不充分，企业可能会处于无法接受的风险水平。

安全流程成熟度从 1 级提升到 2 级的改进建议：

- 请高管层同意制定正式的安全防御计划。
- 任命一名临时的 CSO，并赋予 CSO 制定和开展安全防御计划的权力和预算。
- 开展并完善成熟度评估。
- 对组织机构中现有的安全活动进行分类，据此来制定安全计划。

从 2 级到 3 级

在 2 级成熟度时，组织机构会积极主动地管理安全计划，并且尽全力了解自身的安全风险情况，包括安全要求、可用资源以及业务运行环境。这就会促使临时委任的 CSO 制定人员配备计划，编写策略方案，并评估整个企业内的安全意识状况。但这时尚无正式的信息安全治理或指导委员会。从根本上而言，信息安全仍然是以 IT 为中心的问题。

安全流程成熟度从 2 级提升到 3 级的改进建议：

- 建立具有跨职能、多学科的治理机制，制定明确的安全章程。
- 正式任命 CSO，组建安全团队并执行安全计划。
- 完成核心安全流程目录的制定与实施。
- 建立有效的安全培训计划，对员工行为和企业文化产生影响。

从 3 级到 4 级

在 3 级成熟度时，组织机构已经创建了坚实的安全策略体系，并且还制定了职责划分 RACI 表，确定了各个安全人员的职责。虽然这时已经制定了安全策略和规则，但是对这些规则的问责制和执行尚处于早期阶段，安全活动仍然主要以 IT 为中心。安全方面的进步仍然是由高级管理层“自上而下”的关注驱动的，并且企业安全意识仍然有限。

安全流程成熟度从 3 级提升到 4 级的改进建议：

- 了解业务经理和其他相关方的业务决策，寻求他们的指导，将治理体系落实到位。
- 实施强大的安全策略框架和管理计划。
- 最终确定并分配责任，明确记录谁负责什么内容，并将职责划分情况报送高管层。
- 建立符合组织机构年度战略计划的信息安全架构。
- 解释安全指标并使用这些指标来向高管层介绍相关的风险状况。

从 4 级到 5 级

在 4 级成熟度时，组织机构已经确定了正式的安全职责。但业务部门并没有明确接受剩余风险。组织机构正式建立了跨部门的委员会，支持安全专业人员和业务部门之间加强沟通交流。企业的安全工作正在逐渐放弃以 IT 为中心的模型，将安全职责转移给 CSO。现在，可以通过现有的流程解决所有可以合理预期的风险，并使用安全指标来确保能够实现预期目标。

安全流程成熟度从 4 级提升到 5 级的改进建议：

- 确保业务管理者和其他业务流程负责人对剩余风险承担一定责任。

- CSO 至少每半年向董事会报告一次安全计划进展情况以及与主要业务目标相关的剩余风险。
- 制定一个持续改进流程，确保对安全流程进行不断优化。
- 启动变更管理功能，支持对安全计划进行优化调整，对环境、技术和业务变更做出响应。

写在最后

通常，组织机构对安全流程的投资要比其他 IT 领域的投资落后三到五年，但安全流程成熟度却是决定企业安全计划有效性、效率的关键因素。对此，安全负责人可以根据上文中列出的评估标准和改进建议，来完善流程成熟度有差距的地方。

在安全负责人进行总结汇报、进行年度规划时，从安全流程成熟度的角度出发，不仅可以让高管层更清晰地了解企业自身的安全风险水平，还能够向高管层就如何改善安全流程提出有效建议，展现安全计划的价值所在！