

IT 资产安全处置：实现高价值成果

缺乏 IT 资产处置解决方案的风险是巨大的。本文阐述金融服务机构如何通过安全处置报废的 IT 资产，实现安全、合规与环保目标。

截至2018年8月，金融服务机构的数据泄露事件已增加至103起，而2016年全年仅为37起。

这一数据充分说明了为何数据安全是金融服务业IT领导者的首要关注点。此外，他们还需应对一系列影响IT资产决策的法规，尤其是涉及报废或过时设备处置的法规。

通过正确的IT资产处置计划，金融服务机构可以：

- 提升数据安全与隐私保护，同时遵守不断变化的全球法规要求
- 通过二次营销降低总拥有成本（TCO）
- 最大限度减少对环境的影响

安全风险高

数据泄露是所有企业持续关注的问题。然而，银行和保险公司正在收集越来越多的个人及高度机密的数字化数据，进一步推高了安全风险。一台设备可能同时包含客户的敏感数据（如社会安全号码、银行账户信息、工资单）和公司专有信息（如收入预测、工资或申报数据）。

当需要处置已报废的IT资产和存储媒介时，数据丢失和被盜的风险显著增加。如果设备落入不良分子之手，或处置不当，均可能导致数据被盜、公司声誉受损以及知识产权流失。

金融服务业 IT 领导者深刻意识到IT资产处置（ITAD）的所带来的挑战。在最近的一项 IDG 调查中，他们列出了三大障碍：数据安全问题、监管链安全风险以及多地办公场所处理IT资产的不一致性。

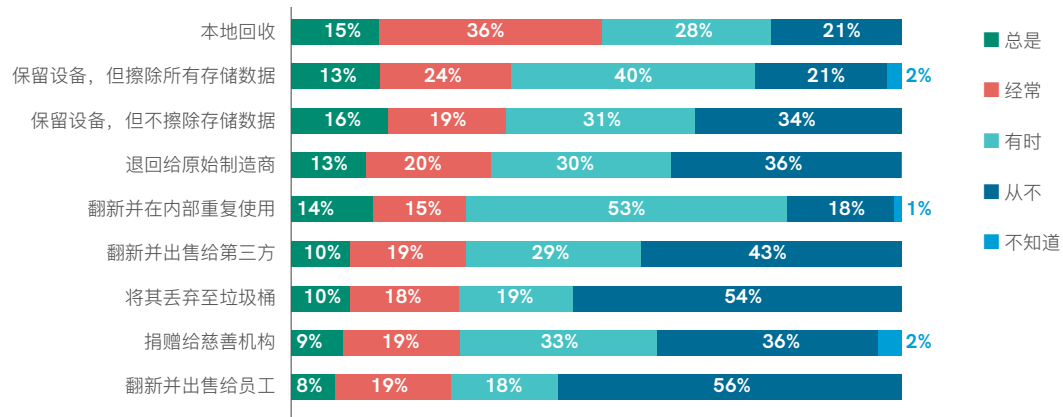
此外，这些高管还提到影响 ITAD 的多项法规，如 SEC 和 EPA 颁布的法规、欧盟的《通用数据保护条例》、《银行安全法》和《Gramm-Leach-Bliley 法案》。

然而，许多企业在认识到挑战、风险和法规后，并未采取适当行动来避免IT资产处置中的安全问题。例如，IDG 调查显示：

- 59% 的金融服务机构没有成文的 ITAD 政策
- 44% 的机构完全依靠内部团队进行设备处置
- 37% 的机构保留已报废的 IT 资产且未清除存储数据
- 28% 的机构将旧设备丢弃在垃圾桶中

35% 的公司未擦除已报废的 IT 资产上的存储数据

当今已报废的 IT 资产的处理方式 —— 所有受访者



Source: IDG

“不幸的是，有些公司并未完全合规操作，” Iron Mountain 的电子废弃物与 IT 资产安全处置团队成员 Brooks Hoffman 表示，“走捷径很容易，但这样做可能导致严重后果，甚至引发数据泄露。”

好消息是，解决方案并不复杂或繁重。

IT 资产安全处置：全覆盖所带给您的益处

一个设计合理的 IT 资产安全处置 (SITAD) 计划能够满足企业的所有目标。当被问及最希望在此类计划中看到什么时，金融服务机构的 IT 领导者表示希望：

- 确保敏感数据的安全性
- 满足数据隐私法规
- 符合环保法规
- 减少内部资源负担
- 实现环境可持续性

全覆盖的 SITAD 计划不仅能实现这些目标，还能提供更多价值。例如，Iron Mountain 的解决方案为金融服务公司提供 ITAD 政策制定框架。这些模板包括了资产追踪、数据安全、数据销毁和法规合规的流程与标准。

合适的 SITAD 方案还能在 IT 资产报废时确保监管链的安全可信。某些 ITAD 公司使用第三方服务运输旧设备。有时候，这些供应商可能将物流或运输环节分包，导致监管链存在漏洞。试想，如果运输司机未锁好装有您 IT 资产的车辆，将带来多大风险？

金融服务公司应选择获得 e-Stewards® 等独立标准制定机构认证的 ITAD 供应商。这样确保严格遵守法规和标准。

ITAD 供应商还可通过避免 IT 资产进入垃圾填埋场或其他废弃流程，帮助实现环境和社会责任目标。由于美国各州和地方在联邦电子废弃物法规外可能另有具体要求，因此该领域非常复杂。

最后，银行和保险公司应积极考虑已报废的 IT 资产的二次营销。借助合适的 ITAD 合作伙伴，企业可通过最大化转售价值来降低总拥有成本。

关键结论

金融服务机构掌握大量敏感数据，若缺乏安全的 IT 资产处置计划，则将面临巨大风险。确保全公司范围内正确实施 ITAD 比以往任何时候都更重要。

如果公司 75% 的 ITAD 操作合规，意味着 25% 的操作仍存在问题。这是不可接受的。” Hoffman 强调。

Iron Mountain 的 IT 资产安全处置解决方案确保安全销毁企业的 IT 资产、回收或重新利用以实现最大价值。

了解更多：www.ironmountain.com/sitad