某银行信息科技部 ISMS 审核案例

推荐机构：广州赛宝认证中心服务有限公司
认证领域：信息安全管理体系审核
审核时间：2023 年 9 月 18 日—9 月 21 日
审核人员：段沛鑫（组长/组员）

一、背景简介

随着数字经济的快速发展，我国银行业务服务模式与技术架构发生了深刻变革。尤其在数字化转型背景下，信息安全作为保障银行业务稳定连续运行的基础，正面临更大的挑战。为适应行业发展要求，控制潜在风险，构建良好的安全运营体系已经成为了银行企业信息安全建设工作的重点。

二、过程介绍

经过初步访谈审核员了解到，该公司虽然成立时间较短，但在信息安全领域已建立起了相对完善的技术防护体系，并开展有安全运营工作，安排专职人员跟踪处理安全事件。

由于良好的安全运营工作是信息安全保障的基础，审核员将审核关注点聚焦于公司安全运营和事件处理环节。通过深入了解，审核员发现公司通过部署“威胁监测与分析系统”收集和分析安全事件，系统通过规则将发现的安全事件划分为多个等级，并通过工单的形式推送报告安全事件，公司采购有安全厂商提供的运营服务，专人负责对事件进行处置，要求“失陷”和“高危”等级必须要上报处理。

审核员进一步查看“威胁监测与分析系统”，发现系统连续多日报告有“失陷”等级的安全事件，跟踪检查公司安全事件处理报告和运营日报也未见反映此事件。审核员随后询问值守人员原因，值守人员解释称该事件之前已判断为误报因此未处理，追踪查看提供的误报说明报告发现记录的情况与事件情况并不相符，无法说明此事件同样为误报。审核员继续跟进，发现公司值守人员编制的《运营日报》与系统每日报告的事件数据不一致，值守人员未能给出合理解释。

综合上述情况，审核员认为公司安全运营工作在执行过程存在纰漏，第三方

公司提供的安全运营服务存在质量问题，且公司未进行有效管理。故根据上述情况开具一般不符合，并建议公司重视对第三方服务公司安全服务质量的跟踪控制，改善安全运营工作效果。

三、客户收益

公司信息科技部领导表达了对案例中不符合项的认同，对此案例中反映的安全公司服务问题、安全运营工作问题高度重视，末次会议后就安排进行了相关整改工作。后续公司在安全运营流程改进，平台告警策略优化等方面进行了整改，同时还针对审核组提出的安全开发、堡垒主机审计、终端防护、数据安全等领域的建议项进行了改进。