数据安全审计

伴随互联网、云计算、移动互联网等新技术的迅猛发展，无处不在的移动设备、无线传感器等设备以及数以亿计的互联网用户和企业产生的消费数据及经营数据使得各类信息呈现爆炸式增长。同时，数据的高度集中，共享开放和交叉使用以及数据流动的趋势也在不断加剧。组织由于数据管理、安全隔离、访问控制及数据加密等措施不充分而面临的网络入侵和信息泄露风险越来越大。

一旦数据的机密性、完善性和可用性受到损害，将不能支撑组织业务的健康运行；随着网络安全法的实施，国家对重要业务数据和个人敏感信息保护的力度也在加强，数据安全的违规成本已越来越高。因此，数据安全是数字经济时代生产力要素的必要属性，持续性开展数据安全审计已成为信息系统审计的重要内容。

本节所涉及的数据包括了日常数据和大数据（按结构化程度和数据规模）、个人信息和重要数据（按数据对象类型）的相关内容。本节将从数据安全治理、数据安全管理、数据生命周期安全管理、个人信息安全管理、重要数据安全管理、数据平台与技术安全管理等方面对数据安全的审计方法和步骤进行描述。

一、数据安全治理审计

（一）业务概述

数据是指对客观事件进行记录并可以鉴别的符号，是对客观事物的性质、状态以及相互关系等进行记载的物理符号或这些物理符号的组合。

数据安全风险涉及面较广，既体现在组织在治理层面的治理风险，还体现在数据在其生命周期和服务过程中的管理风险，以及伴随的个人信息和重要数据等敏感信息泄露和跨境流通风险。

（二）审计目标和内容

1. 董事会的职责

该控制项旨在从组织的治理层面，检查组织是否将数据的安全治理工作纳入组织治理工作范畴，建立健全包括风险管理和数据安全审计监督在内的架构体系，从而完善数据的安全合规管理。

2. 战略规划与价值实现

该控制项旨在检查组织是否依据董事会所明确的数据安全治理目标制定相关的安全战略。

3. 数据安全合规管理

该控制项旨在检查组织是否基于数据安全战略规划，建立健全数据安全管理制度体系，满足合规监管要求。

4. 数据风险管理

该控制项旨在检查组织是否从数据、人员、产品与服务等方面，建立并完善数据安全风险管理体系，并将其纳入组织风险管理体系当中。

5. 数据安全审计监督

该控制项旨在检查组织是否将数据的安全审计工作纳入到组织的安全审计体系范畴内，建立并完善针对数据安全审计的专项工作。

（三）常见问题和风险

1. 未建立数据安全治理组织架构及职责，无法自上而下推动相关数据安全治理工作的有序开展。

2. 未建立组织级数据战略规划，无法有效覆盖网络安全法及等级保护等相关法规与标准的要求，无法指明数据整体的发展目标和规划，不利于数据长远发展。

3. 未制定数据安全相关管理制度及流程，导致数据安全管控要求无法有效落实。

4. 数据安全风险评估执行不到位，未识别出重要的数据安全风险，不利于数据安全治理体系的持续优化。

（四）审计的主要方法和程序

1. 董事会的职责

（1）检查组织董事会和执行管理部门职责，是否将数据安全治理工作纳入到组织综合治理工作范畴当中，明确数据安全治理职责并对其安全治理予以承诺和支持，从战略、组织、架构和实施等多个环节提供保障。

（2）查阅组织数据治理的规章制度，明确数据安全治理需要达到的目标和定位，判断其治理目标是否与组织战略、业务战略、业务目标、业务需求相一致。

（3）检查组织是否建立跨部门的数据安全管理委员会和风险管理委员会，明确安全治理的角色和责任。

（4）检查组织是否建立基于满足业务战略的数据架构，并进行持续的评估、监督和改进。

（5）访谈组织信息科技治理负责人，了解组织是否已经或即将部署云服务平台，以及是否将基于云平台中的数据安全治理列入主要治理目标和任务当中。

2. 战略规划与价值实现

（1）访谈战略规划负责人或查阅组织经营战略规划，判断数据战略规划是否满足经营战略需要。（经营战略一致性）

（2）查阅组织数据战略规划，判断其战略内容是否与组织数据治理目标相一致，检查内容上是否包括数据服务战略、数据平台与应用战略，且战略规划内容是否涉及数据安全，体现《网络安全法》和网络安全等级保护等制度对于数据安全的相关要求。

（3）访谈信息系统战略规划负责人，了解组织信息化及信息安全战略规划要求，判断数据安全战略是否与信息系统安全战略和需求相一致。（信息系统安全战略一致性）

（4）查阅数据安全战略规划，判断其从内容上是否体现组织对于个人信息（隐私）保护和重要数据保护治理方面的要求。

3.数据安全合规管理

（1）查阅组织制定的与数据管理相关的制度与规范，从而判断其是否符合数据安全相关的政策、法律、法规等各项监管要求。

（2）检查组织的数据安全管理相关制度与规范，查看其内容是否涵盖国家和社会生产的重要数据的安全管理要求，个人信息的保护要求，数据跨境传输与共享的安全管理要求，以及密码使用要求。

4.数据风险管理

访谈组织风险管理负责人，询问组织是否将数据风险管理纳入组织风险管理体系当中，重点突出数据、人员、产品/服务三个方面，并建立数据安全内控体系；数据方面，以数据生命周期为出发点，识别全周期面临的威胁和自身脆弱性，分析数据服务安全风险和应对措施需求；人员方面，基于数据安全管理需要，基于员工日常数据操作行为，识别风险并建立风险量化机制和信息安全评价指标体系；产品/服务方面，以对个人信息和重要数据保护为目的，构建产品/服务提供商在组

织、规范、设计、流程、监控等一系列的安全风险评价体系和控制机制。

5.数据安全审计监督

（1）访谈组织审计负责人，询问组织是否将数据安全管理审计纳入到组织安全审计管理体系内。

（2）访谈组织审计负责人或信息安全审计负责人，了解组织是否建立负责数据安全监督与审计管理的职能机构及制度与规范，了解组织对数据服务及其用户操作行为审计的方法和内容。

（3）查阅组织有关数据安全审计的制度和规范，了解针对数据安全审计的方法、频率和周期，并查阅相关审计报告。

二、数据安全管理审计

（一）业务概述

数据安全管理是指保护数据免受威胁的影响，确保业务的连续性，降低业务可能面临的风险，为业务部门提供有力保障。

（二）审计目标和内容

1.数据安全组织管理

该控制项旨在检查组织为落实数据安全治理工作及其战略规划，是否从组织层面设置跨部门的数据安全管理机构及负责人，明确安全管理职责。

2. 人员与意识管理

该控制项旨在基于组织对数据安全管理的要求和需求，从人员安全管理、资源建设与技能培养、职责落实与考核等三方面进行检查，判断人员综合管理的落实情况。

3. 制度与规范管理

该控制项旨在从制度层面检查组织是否制定并完善数据安全管理的制度体系及其落实情况。

4. 元数据安全管理

该控制项旨在从元数据的安全管理角度，检查组织是否建立完善的元数据安全管理规范，并从技术层面予以安全保障。

5. 数据及平台（系统）管理

该控制项旨在从数据平台（系统）管理角度，检查组织是否对平台（系统）及其管理之下的数据制定相应的安全规范与标准，实现统一管理，并与组织经营战略中的安全需求相一致。

6. 服务接口安全管理

该控制项旨在从服务接口角度，检查组织是否完善接口安全管理的制度和规范，并用技术手段保障接口间数据传输的安全性。

7. 数据供应链安全管理

该控制项旨在从供应链安全管理角度，检查组织在存在上下游数据交换的前提下，制定相关管理规范，满足合规监管要求。

8. 数据安全审计管理

该控制项旨在从审计角度，检查组织是否落实数据安全审计与监督的要求，对组织的数据服务开展安全审计，同时确保国家对于日志管理的安全合规要求。

（三）常见问题和风险

1. 数据安全组织架构及责任人缺失，导致数据安全管控要求无法落实。

2. 未定期开展数据安全意识宣贯，由于安全意识不足，导致数据不经意的泄露。

3. 元数据安全管控不到位，导致元数据血缘关系模糊、可追溯性不强，影响元数据与数据标准的结合。

4. 未部署数据管控平台，无法对数据标准、数据质量、元数据进行规范化管控和技术实现。

5. 数据服务接口与应用在其内部跨安全域间的接口调用未采用包括安全通道、加密传输等安全机制可能带来的风险。

6. 未建立数据供应链安全管理方针，无法落实上下游供应链间数据交换和使用的要求，不利于供应商之间的数据交换与共享。

（四）审计的主要方法和程序

1. 数据安全组织管理

（1）访谈组织人力管理部门或信息安全管理部门负责人，了解组织是否设置专门的数据安全管理机构和责任人及其相关的部门和岗位。

（2）访谈数据安全管理机构负责人，了解组织目前是否制定与数据安全相关的包括数据服务安全追责在内的规章制度，并定期对责任部门和安全岗位组织安全检查，形成检查报告；组织目前数据及其服务平台与应用的安全规划、安全建设、安全运营和系统维护工作整体情况；组织是否清楚地界定服务提供者、数据使用者（包括终端用户与设备）；是否设置专职的数据服务安全岗位，建立规范化的数据服务安全保护、评估及考核专职队伍。

2.人员安全管理

（1）访谈人力资源管理和数据安全管理负责人，了解组织是否基于数据生命周期各阶段数据服务和系统服务相关的工作范畴和安全管控措施，制定数据服务人力资源安全策略。

（2）访谈数据安全管理负责人，了解是否明确数据服务相关重要岗位及其角色安全要求，建立重要岗位角色清单和授权机制。

（3）访谈人力资源管理负责人，是否就数据安全管理的关键岗位做好人力资源培养和储备工作。

（4）访谈人力资源管理负责人，是否在组织内部针对所有接触个人信息和重要数据等敏感信息的全职员工

与操作须知，并抽检保密协议和制度知晓的记录。

（5）访谈人力资源管理负责人，了解组织是否建立第三方人员安全管理制度，对接触个人信息、重要数据等数据的人员进行审批和登记，并要求签署保密协议，定期对这些人员行为进行安全审查，并调阅相关管理制度、保密协议和历史审批与登记记录。

（6）检查组织是否建立数据安全教育培训机制，分别针对数据操作人、数据安全管理人员和第三方人员制定培训计划，并定期对全员，特别是关键岗位人员进行能力检查和考核，考核应纳入到个人与组织的绩效考核体系当中，查阅教育培训与考核的历史记录。

3.制度与规范管理

（1）调阅并检查组织是否制定包括数据服务在内的数据安全管理制度和规范、数据分类分级规范和标准、数据安全人员能力要求及向第三方提供或共享数据时的安全管理制度和标准，其中，制度在范围上应覆盖数据全生命周期。

（2）检查制度和标准是否得到定期评审和更新，并分发至机构数据服务部门和操作人员，抽样访谈数据操作和管理人员，了解其对制度规范的知晓情况并查阅制度规范的更新记录。

4.元数据安全管理

1）检查组织是否建立与数据服务相关的元数据及其管理规范、与数据服务安全架构相应的安全元数据管理规范和数据访问控制策略，从而明确元数据管理角色及其授权控制机制和查询限制。

（2）检查元数据的安全管理制度和规范是否包括：依据资产分类分级策略所建立的元数据安全属性的自动/手工分级机制；可依据元数据安全属性建立标记的策略及标记定义和管理机制。

（3）检查组织是否从技术手段上实现：对表字段、表与上下游表的血缘关系查询进行安全设置和查询限制。可对表访问操作权限进行限制。

（4）检查组织是否建立针对元数据操作的审计制度，并确保对元数据的操作具有可追溯性。

5.数据及平台（系统）管理

（1）检查组织是否建立数据资产安全管理规范和数据资产分类、分级方法、标准、操作指南、数据资产分类分级变更审批流程，并对其进行定期审核和更新。

（2）检查组织是否对数据资产实施登记制度，其应明确数据资产管理相关方及管理责任、数据资产管理范围和属性，并调阅数据资产登记目录清单。

（3）检查组织是否在技术上建立综合的数据管理平台或系统，实现对数据资产的统一管理，包括：是

管理的目标和原则；数据系统平台的规划和建设应与组织经营战略和平台（系统）全生命周期的安全需求相一致。可依据数据资产和数据主体安全分级要求建立相应的标记策略、访问控制、数据加解密、数据脱敏等安全机制和管控措施。

6.服务接口安全管理

（1）检查组织是否制定与数据服务接口安全管理有关的控制策略和安全规范。

（2）检查组织的数据平台与应用在其内部跨安全域间的接口调用是否采用包括安全通道、加密传输等安全机制。

7.数据供应链安全管理

（1）访谈组织数据管理部门负责人，了解组织目前是否存在数据供应链上下游间数据交换和使用的现象，若存在，则了解并查看：组织是否建立与数据供应链安全管理有关的规范和安全方针，其应明确数据供应链安全目标、原则和范围，并对其进行查阅；组织是否识别并建立数据供应链上下游间数据交换和使用的合规要求及合规目录，从而确保其数据交换和使用的合规；建立数据供应链目录和相关数据源数据字典，明确数据供应链的责任部门和人员。

2）查阅组织与上下游数据供应链服务商签署的合作协议，检查协议是否：明确数据供应链上下游责任和义务,并检查是否采用安全技术保障措施确保数据供应链上下游对数据交换、使用的安全、可靠与合规；明确数据供应链中数据的使用目的、供应方式、保密约定等内容。

（3）检查组织是否对数据供应链上下游的数据服务提供者和数据使用者的行为进行合规性审核和分析，并查阅相关记录和报告。

8.数据安全审计管理

（1）访谈组织负责数据审计的负责人，询问组织是否明确对于数据安全审计的要求、审计范围、审计方式。

（2）访谈组织负责数据审计的负责人，询问对数据服务平台（系统）部署审计产品，登录安全审计产品并查看审计日志是否完整，其保存期限是否符合国家强制要求并具有防篡改的功能。

（3）查阅历史审计报告，了解审计对象是否包括与数据相关的物理环境、网络传输、平台/系统、数据库及存储介质，以及基于数据平台/提供者，数据提供者，服务提供者和内部服务/数据使用者针对主要操作、敏感行为、敏感数据流通等安全事件。

处理、交换（共享、应用）、销毁等阶段下对流动的数据进行综合管理。

（二）审计目标和内容

1.数据收集

该控制项旨在针对数据收集过程，检查组织是否依据收集数据的敏感性对其进行数据标识，从而基于该标识进行后续数据操作处理的监控。

2.数据传输

该控制项旨在针对数据传输过程，检查组织是否根据传输过程的安全性划分安全域，并根据安全域的级别采取相应的安全控制措施，防范数据遭受窃听或泄露，确保数据的完整性。

3.数据存储与恢复

该控制项旨在针对数据存储，检查组织是否对所存储的数据采取安全措施，确保其安全性和完整性，同时，根据组织对于数据可用性的要求，检查组织是否采取备份措施。

4.数据处理与加工

该控制项旨在针对处理和加工过程，检查组织是否对可接触到数据的人员基于角色采取身份验证和访问

据非法访问或敏感信息遭到泄露。

5.数据使用与安全审计

该控制项旨在针对数据使用过程，检查组织是否采取身份验证和访问控制措施，防止人员对于数据的非法访问，并采取加密和脱敏等技术手段，防止在使用环节造成信息泄露并对使用环节进行安全审计。

6.数据共享与流动

该控制项旨在针对组织存在数据共享与流动，特别是跨境流动时，是否制定相应的规范制度和审批流程，满足国家合规监管要求。

7.数据归档与销毁

该控制项旨在检查组织是否针对数据归档与销毁过程，并基于数据敏感程度制定完善的管理制度与规范流程，防范在该过程中出现数据泄露。

1.在数据生命周期管理期间，由于在人员、管理、技术三个层面没有建立适用的数据安全管理体系，使得数据安全管理的效率与效果低下。

2.未实现数据分类分级管理或分级方法不合理，导致未按照不同类别建立不同的安全控制措施，导致保护过重或保护不当。

3. 数据在收集、传输、存储和恢复、处理和加工、使用与审计、归档与销毁等过程中，由于缺乏有效的数据加密和访问控制，容易导致数据泄露风险。

4. 数据在共享与流动，特别是跨边界和跨境流动时，由于未制定相应的安全规范制度和审批流程，容易产生违规风险。5. 数据销毁机制不健全或执行不严格，导致销毁过程中敏感数据的泄露。

（四）审计的主要方法和程序

1. 数据收集

（1）检查组织是否根据数据分级分类管理制度中定义的数据类型、安全等级对所收集的数据进行标识，特别是敏感数据，并根据数据标识和合规要求进行后续传输、存储等流程的跟踪和监控。

（2）对收集的数据进行抽查，检查是否对已收集的数据进行标记。

2. 数据传输

（1）访谈网络安全管理员，询问组织是否在数据传输过程中进行安全域的划分。

（2）访谈网络安全管理员，询问数据在跨域传输，特别是在非安全域传输时是否采用安全加密机制确保传输链路的安全可靠和对数据进行安全加密，查阅组织网络拓扑图并进行实质性查验。

（3）通过执行渗透，获取传输数据包，查验数据包的完整性和保密性措施是否有效。

3. 数据存储与恢复

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/427066040041006144