御数坊 DGWorkshop

奇安信 新一代网络安全领军者

ifenxi

2021年企业数据安全治理调研报告

Research Report on Enterprise Data Security Governance

http://www.dgworkshop.cn

版权说明

前言

《中华人民共和国数据安全法》于2021 年 9 月 1 日起正式开始施行，这是我国第一部有关数据安全的专项法律，该法律也是我国大数据战略法制基础；数据安全保障和数字经济发展领域的重要基石。

在数字化转型的背景下，数据安全已成为企业最紧迫和最基础的问题。加强数据安全治理也已成为维护国家安全稳定，维护国家间良性竞争的重要战略。不论是政府部门还是公司企业，不论是互联网、金融等数字原生企业还是传统制造业等等，都离不开数据安全工作。可以说，数据安全与每个企业，每一个人都息息相关，我们时刻都在面临数据安全的问题。

为了能够提高数据安全治理工作效力，提供更贴近现代企业的数据安全治理方法，把握现代企业数据安全现状，御数坊特别邀请新一代网络安全领军者奇安信和数字化研究咨询机构爱分析共同发起《2021年企业数据安全治理调研》！意在于为数字化转型下的企业提供更多的启示。

调研报告发起方

发起及主办方——御数坊

御数坊（北京）科技有限公司成立于2014年12月，是一家核心团队在数据治理领域专注十年以上的专业机构。成立以来，御数坊曾参与多项数据治理领域国家标准编写。在数据安全方面，御数坊参与了信通院数据安全推进计划DSI中《数据安全治理能力评估方法》、《数据安全分类分级工具》、《数据安全服务能力分级要求》的编写工作。

我们已经成功服务多家大型企业，行业覆盖银行、证券、能源、地产、汽车、通信、制造、政府等领域。御数坊以“咨询服务+软件产品”的一体化交付模式让数据治理落地见效、持续运营，为客户搭建数据体系、解决数据问题、实现数据治理赋能。

御数坊以“协同化、智能化”的理念实现软件产品创新，打造出拳头产品“DGOffice数据治理办公室”软件平台，通过场景应用承载数据治理方法论思想、应用智能化引擎提质增效，让数据治理更简单、更规范、更高效、更智能。御数坊致力于真正解决中国客户多年以来的数据治理实践困惑和挑战，真正实现数据治理的客户成功！

特别鸣谢：

奇安信
新一代网络安全领军者

联合主办方——奇安信

奇安信科技集团股份有限公司（以下简称奇安信，股票代码688561）成立于2014年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务。凭借持续的研发创新和以实战攻防为核心的安全能力，已发展成为国内领先的基于大数据、人工智能和安全运营技术的网络安全供应商。同时，奇安信是2022年冬奥会和冬残奥会网络安全服务与杀毒软件的官方赞助商；此外，公司已在印度尼西亚、新加坡、加拿大、中国香港等国家和地区开展网络安全业务。

ifenxi

联合主办方——爱分析

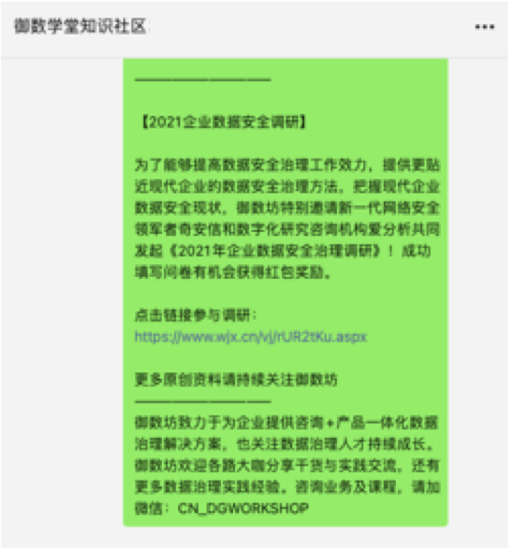
爱分析成立于中国数字化兴起之时，致力于成为决策者最值得信任的数字化智囊。凭借对新兴技术和应用的系统研究，对行业和场景的深刻洞见，爱分析为数字化大潮中的企业用户、厂商和投资机构，提供专业、客观、可靠的第三方研究与咨询服务，助力决策者洞察数字化趋势，拥抱数字化机会，引领中国企业数字化转型升级。

目录

一、数据安全调研基本背景及覆盖人群特征

我们认为：现代企业越来越重视数据安全的重要性，从调研的整体上看，更多的二线、三线城市也都纷纷加入到了数据化转型的队伍中来。企业面对数据治理或是数据安全治理等工作都回归务实，以实现数据价值为最终的目的，也是一切数据安全治理工作行动的指南。

1）调研问卷统计方式及数据统计



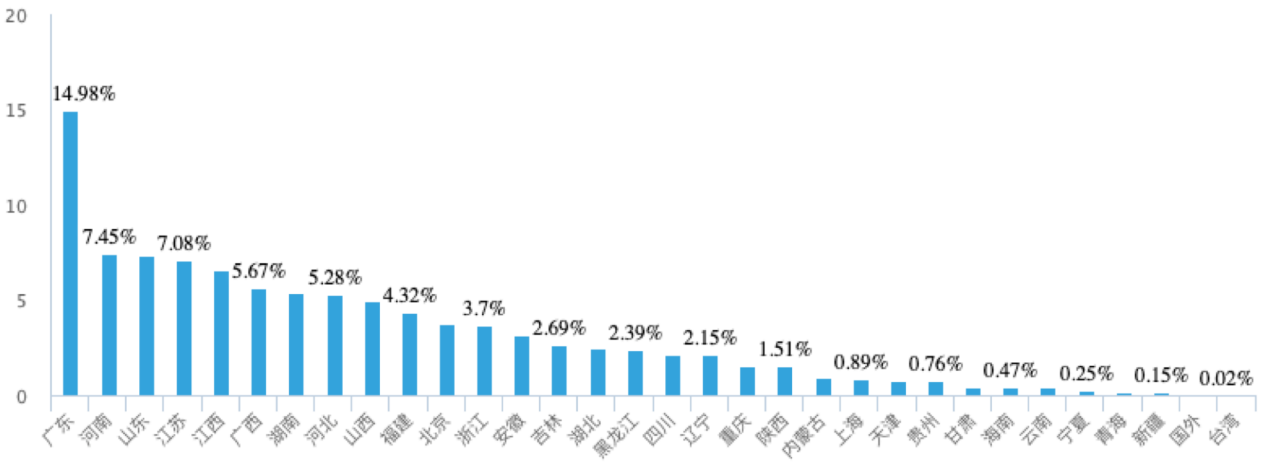
主要传播方式：包括但不限于御数坊社群文字推广，图片推广；公众号；朋友圈。（奇安信和爱分析在自有平台协助发布）

调研时间：2021年9月23日开始——2021年10月9日结束

收集数据：共收集数据5347份，去除无效问卷1296份，实际收集问卷4053份

2）覆盖地区统计

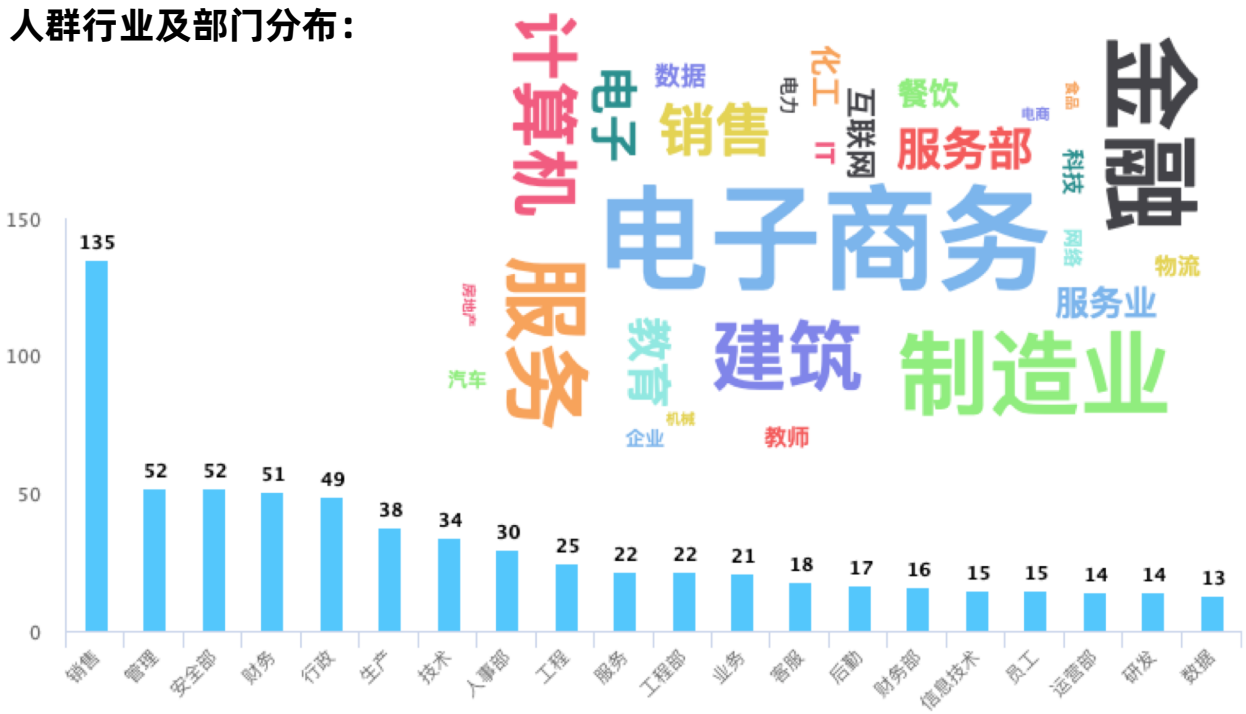
我们对所有4053份调查问卷的地域来源进行统计分析，本次调研问卷地域**分布前五名的是：广东，河南，山东，江苏，江西。**



省份	数量（份）	百分比（%）
广东	607	14.98
河南	302	7.45
山东	298	7.35
江苏	287	7.08
江西	266	6.56

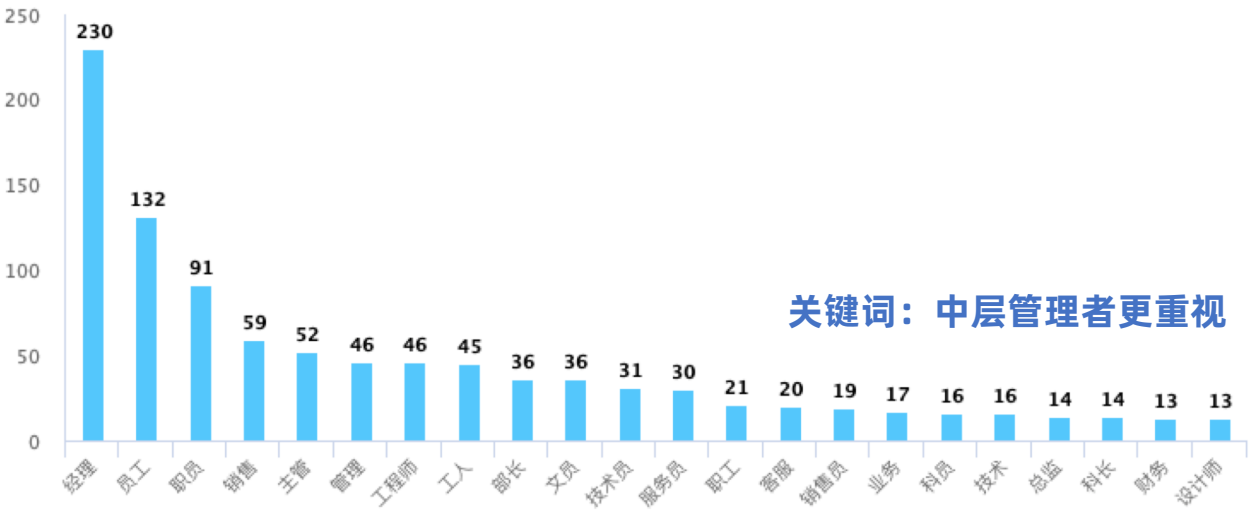
3）人群特性统计

人群行业及部门分布：



关键词：新兴行业突显，业务人员关注广泛

人群职务统计

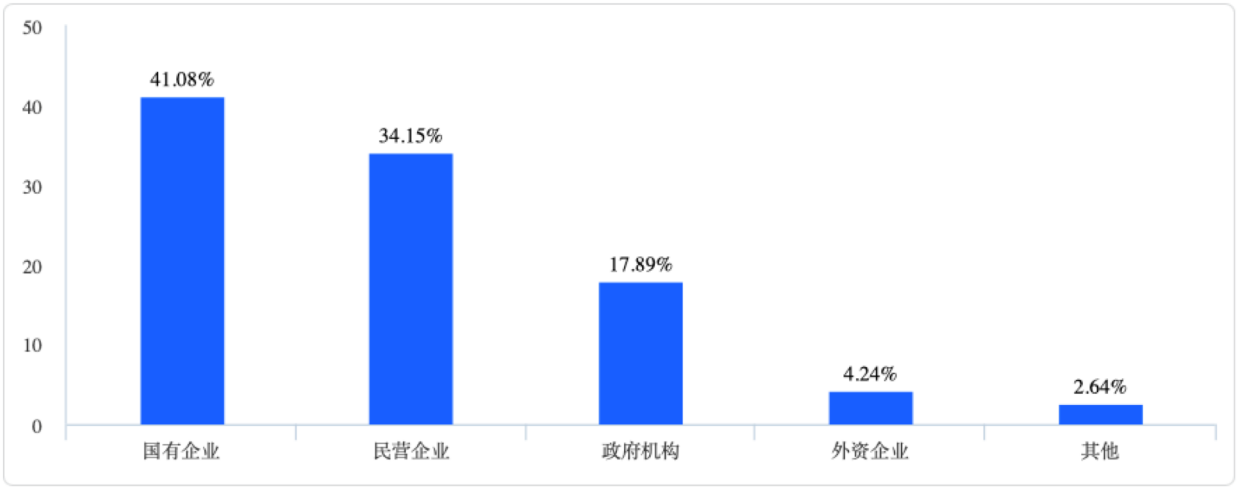


关键词：中层管理者更重视

二、企业数据安全治理环境及现状

1）题目统计

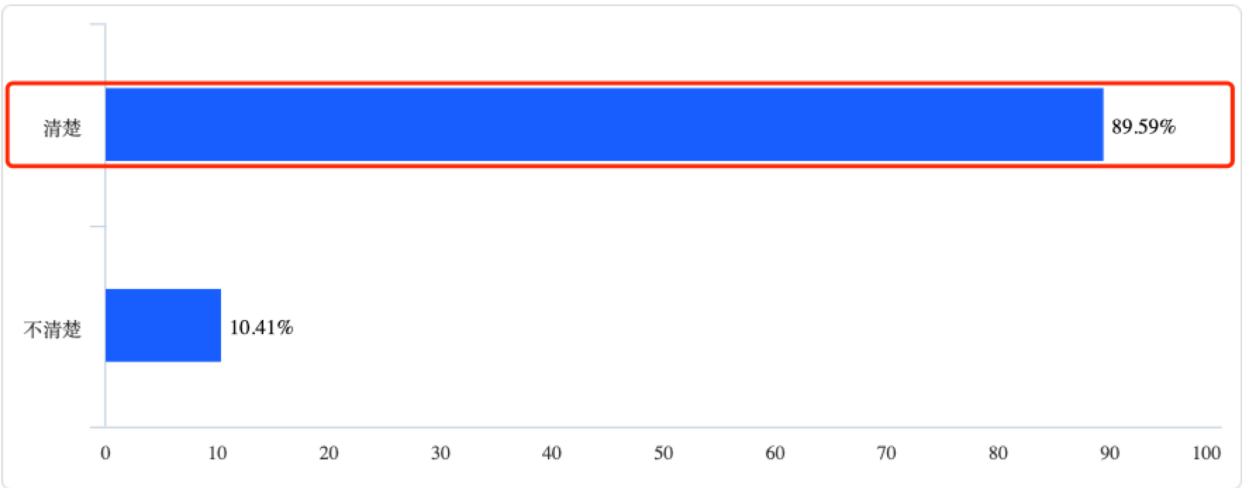
1.您所在单位的性质?



关键词：国企、民企

本次调研主要集中在国有企业和民营企业。政府和外资企业关注度较低。

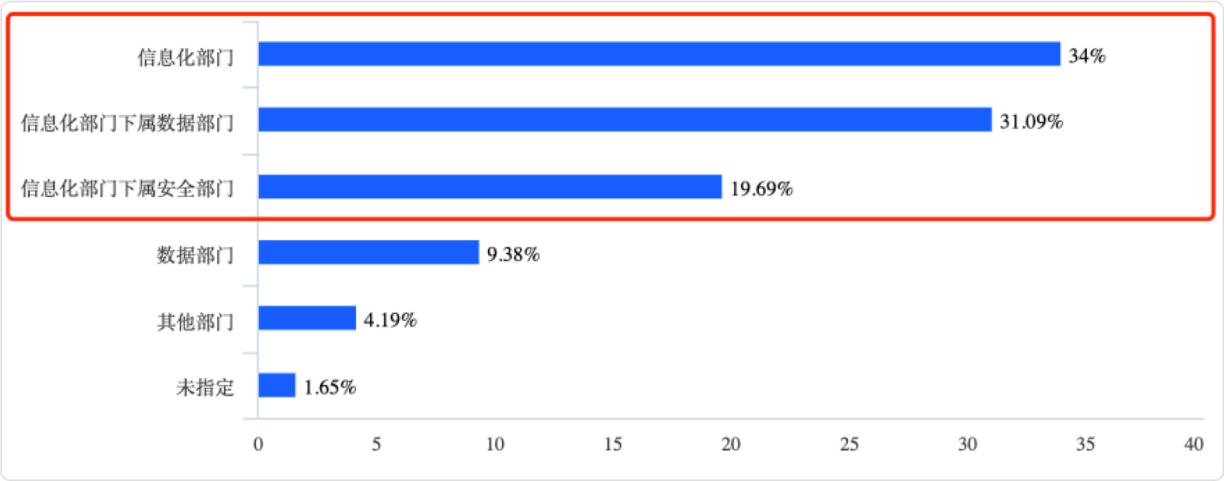
2.您是否完全了解跟您单位相关的数据安全方面的相关法律法规的监管要求?



关键词：普及性高

参与调研的大部分用户都对数据安全相关的法律法规有所了解，可见数据安全相关法律法规的普及性相当高。

3.您所在单位由哪个部门牵头负责数据安全工作？

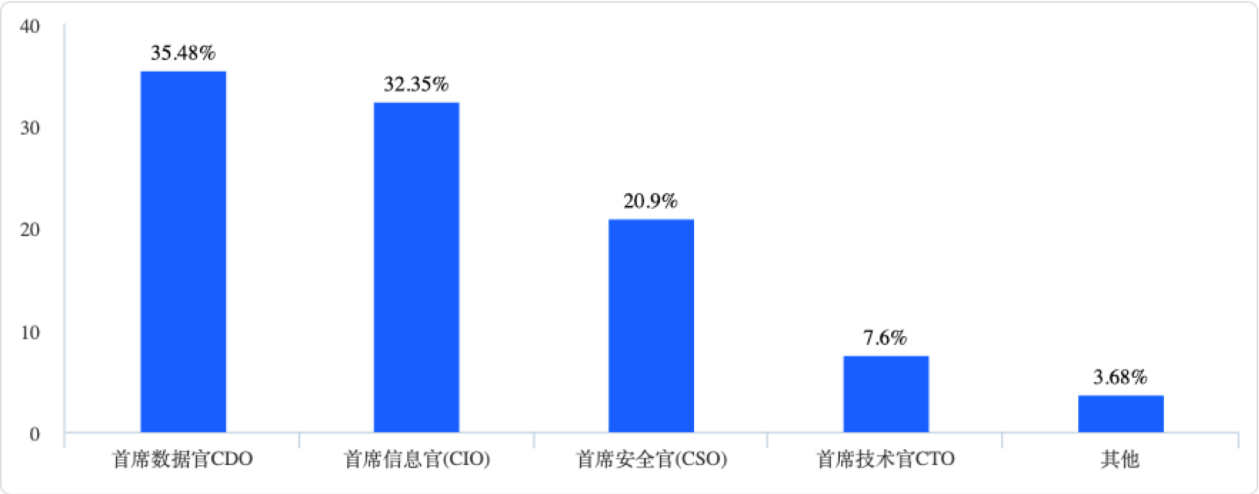


关键词：信息化部门的新挑战

大部分企业都已经设立了信息化部门，同时数据安全相关任务也归属于信息化部门下的独立数据部门或安全部门，目前建立独立于信息化部门的数据部门的企业数量还不多，数据工作仍在信息化工作统筹。

企业信息化建设是个持续的过程，是伴随着企业的发展持续终身的。信息部门就是将各方串在一起的关键连接线，其对信息化的建设成效起着极大的影响和作用。随着企业信息化的深入，信息的重要性愈加凸显，信息部门的地位也会日趋重要起来，逐步由被动支撑向主动支撑转变，由生产支撑向管理支撑提升进行演变，逐步成为企业信息中心数据中心，乃至成为企业决策支持中心。随着数字化转型的进程，关于数据安全方面的工作也对现代企业的信息化部门提出了更新的挑战。

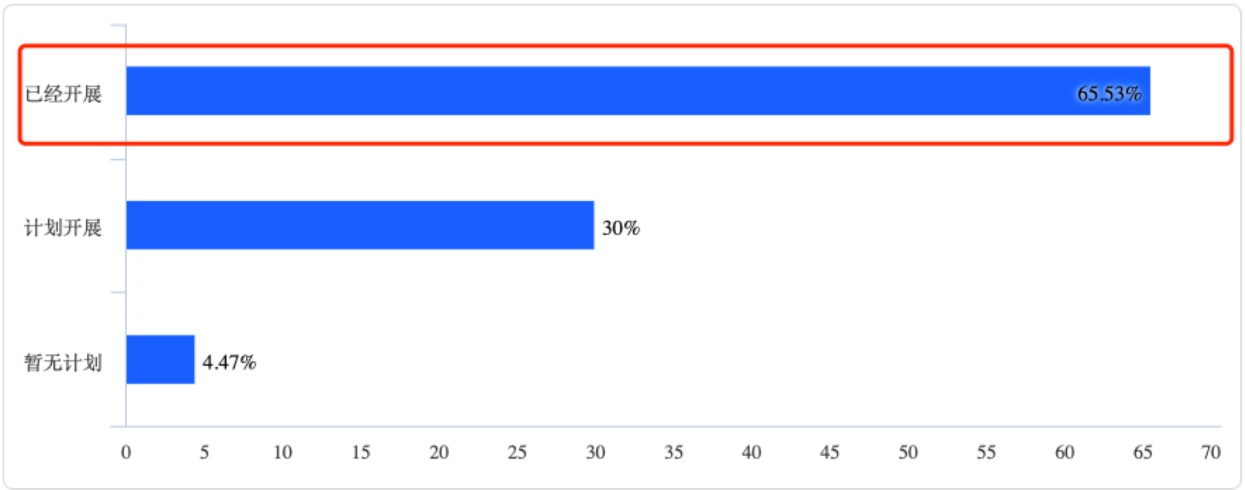
4.您的单位数据安全重大事项由谁决策？



关键词：专职专干

大部分企业为了能够顺利开展数字化转型工作，都积极建立了信息化部门或是数据团队，相关数据工作也都有具体的专职部门执行，数据安全相关决策者也会由专业专职人员负责。

5.在《数据安全法》及《个人信息保护法》颁布实施后，您的单位是否会依据《数据安全法》《个人信息保护法》的要求加强数据安全方面的建设？



关键词：响应积极，投入建设

大部分企业已经开始开展数据安全相关的建设，同时部分企业也计划开展相关建设项目。可以看出企业对于数据安全重视程度很高，大部分企业响应积极，并开始投入数据安全相关建设项目。

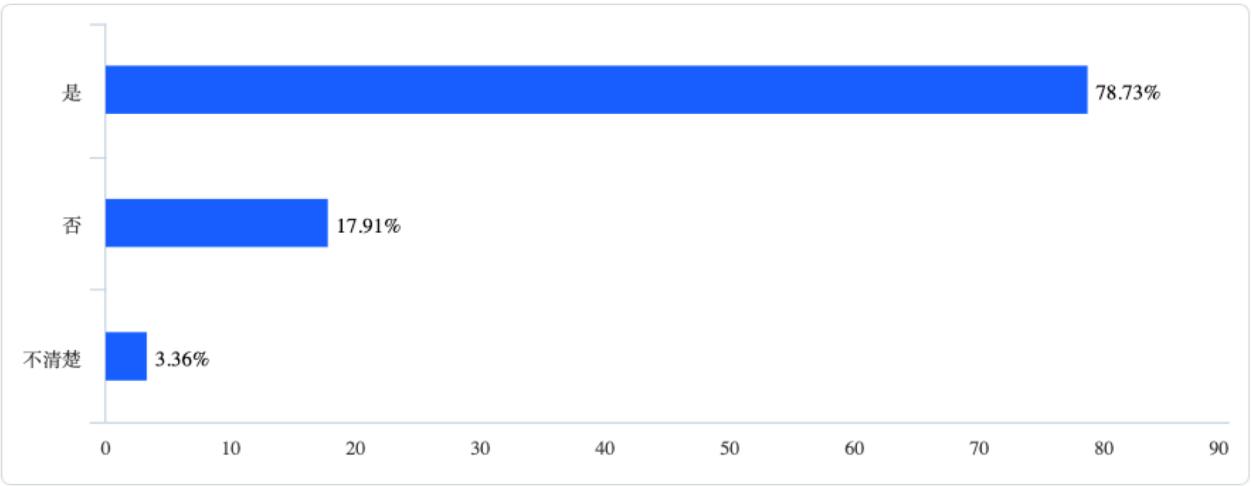
2）总结

我们认为：调研第一部分主要针对企业数据安全治理环境及现状的内容进行调研问题设置。可以看出大部分企业都已经建立了数据安全专职团队，相关工作也逐渐规范化、专业化，将数据安全放在了企业数据治理的重要位置，同时也积极响应国家出台的相关“数据安全法律法规”，切实完善企业数据安全团队建设，制度建设，体系建设。数据安全相关法律法规的颁布也加快了企业对于数据安全体系建设的步伐。

三、企业数据安全治理进程及数据安全普及程度

1）题目统计

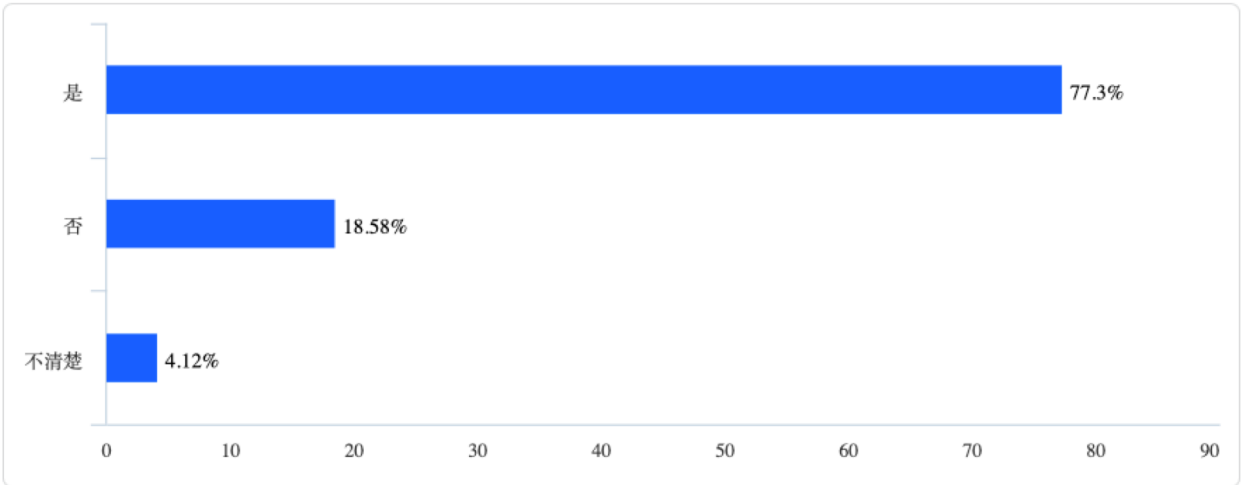
6.您的单位是否明确了数据安全的组织架构，比如决策层、管理层的相关角色及岗位职责？



关键词：建立团队，岗位细分

更多的企业明确了数据安全组织架构内的角色，数据安全治理相关工作正在逐步细化。企业也注重明确数据安全组织架构中的各个岗位的职责。

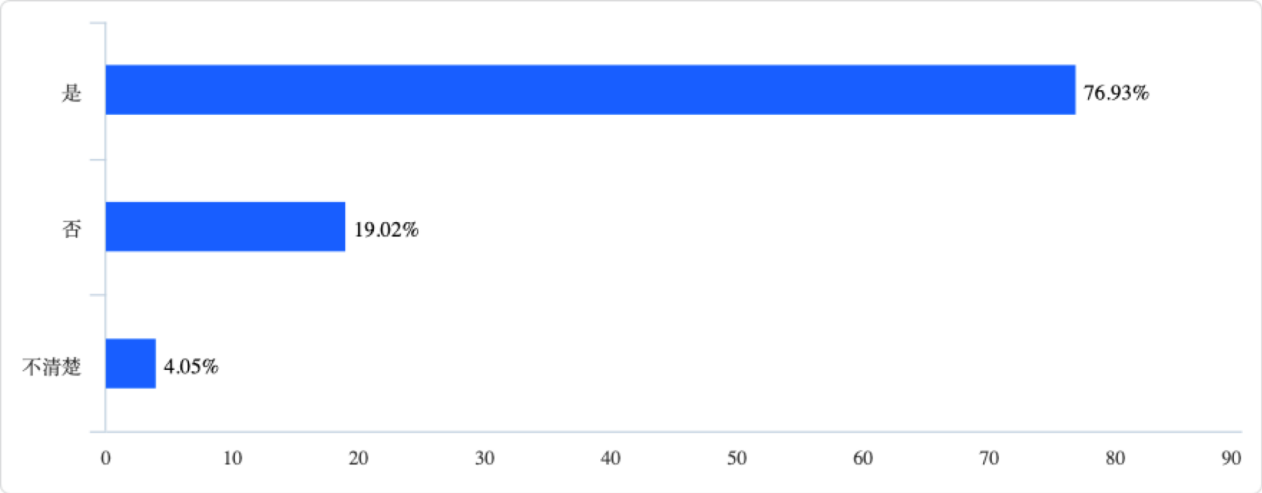
7.您的单位是否设立了数据安全管理岗位进行数据安全的日常管理运营工作，并明确了该岗位的角色及岗位职责？



关键词：明确职能，加强管理

大部分企业已经将数据安全管理工作实践落地，建立专门的数据安全管理团队，明确团队中数据安全负责人的岗位职责。企业面对数据安全建设普遍表现出积极态度，高效完成相关工作以及体系建设，对数据安全工作重视程度很高。

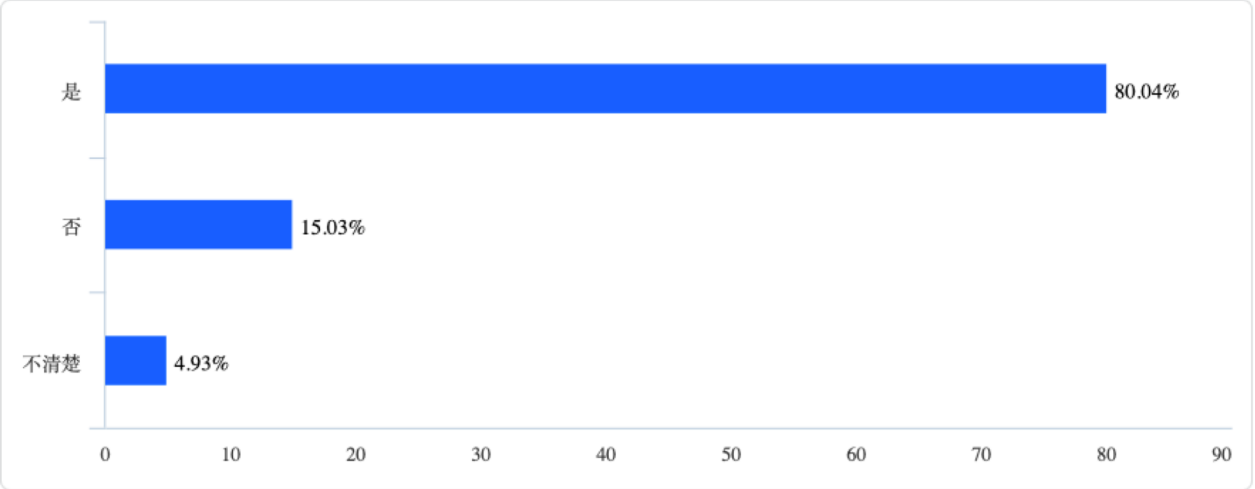
8.您所在单位是否制定了数据安全管理制度，比如《数据安全管理办法》《敏感数据操作规范》等相关数据安全的制度及规范？



关键词：制定规范，有效管控

企业内部多数已经制定了适用于本企业数据安全相应的规范及办法，也是对国家层面“数安法”的快速相应，可以看出大部分企业已经开始落实数据安全建设工作。

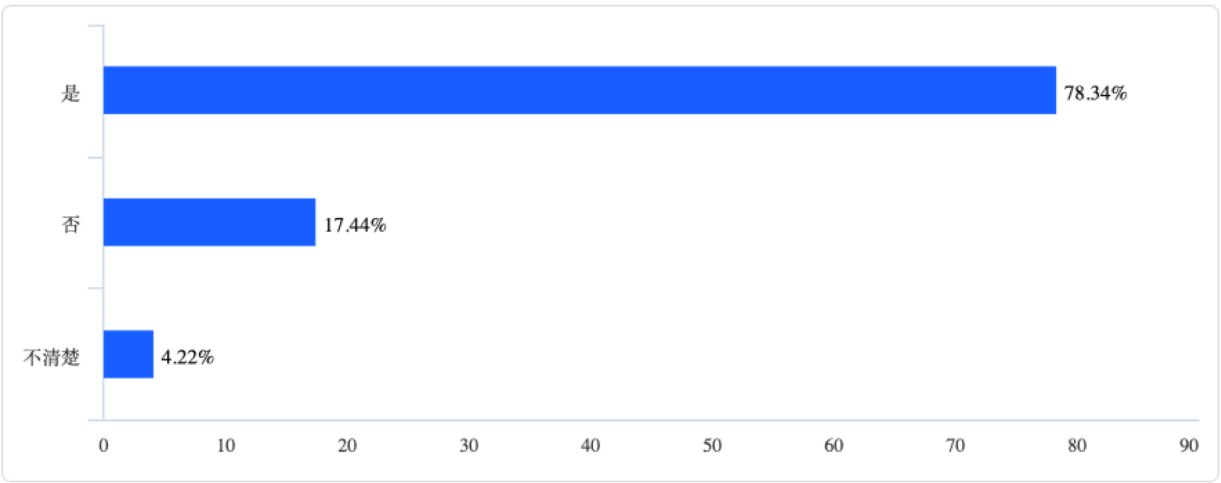
9.您所在单位是否开展了数据分类分级的相关工作？



关键词：付诸实践，保障安全

已经开展了数据分类分级的企业居多，对于数据安全重要性，大部分企业都已经有所意识，并已经开展完成了数据分类分级的数据安全保障工作。

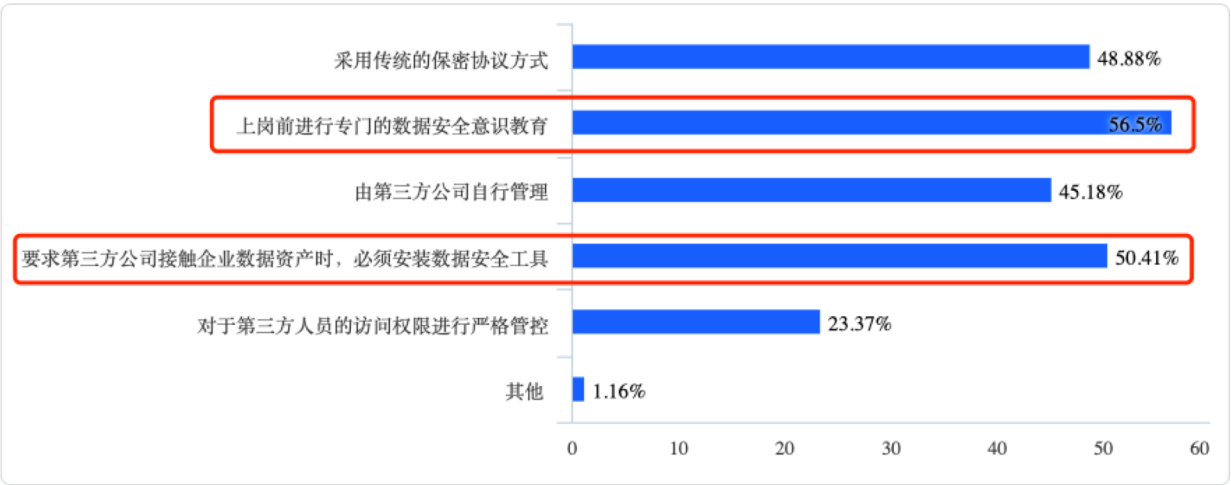
10.您所在单位是否对敏感数据进行梳理识别，并建立敏感数据资产清单或者重要资产目录？



关键词：建立护盾，守护资产

现代企业对于数据资产认识程度逐步提高，在数字化转型的大背景下，企业都会尤为注意自己数据的安全性以及数据价值的体现，所以大部分企业也会积极的开展对敏感数据的梳理以及建立敏感数据资产清单，为企业发展建立坚固的护盾，守住自身的数据资产，同时发挥数据价值，顺利完成数字化转型任务。

11.您所在单位在与第三方进行合作时，在数据安全方面是如何管理的？



关键词：更多的数据安全管理方式

企业间合作不断加强与发展，传统的保密协议以及上岗前的数据安全规范培训方式，仍然会被部分企业使用，通过规范条款以及法律约束将企业数据安全保护起来。当然也有大部分企业会采用数据安全工具来对企业数据资产进行自动化、智能化的监管与保护，并且应用软件方式加大数据保护的方式也逐渐得到更多企业的信任与青睐。由于企业间合作越来越频繁，涉及到的业务越来越广泛，对于限制访问权限来硬性把控数据流通的方式逐渐被企业摒弃，比例越来越小，企业也都更希望在互通有无的基础上实现更大的数据价值。

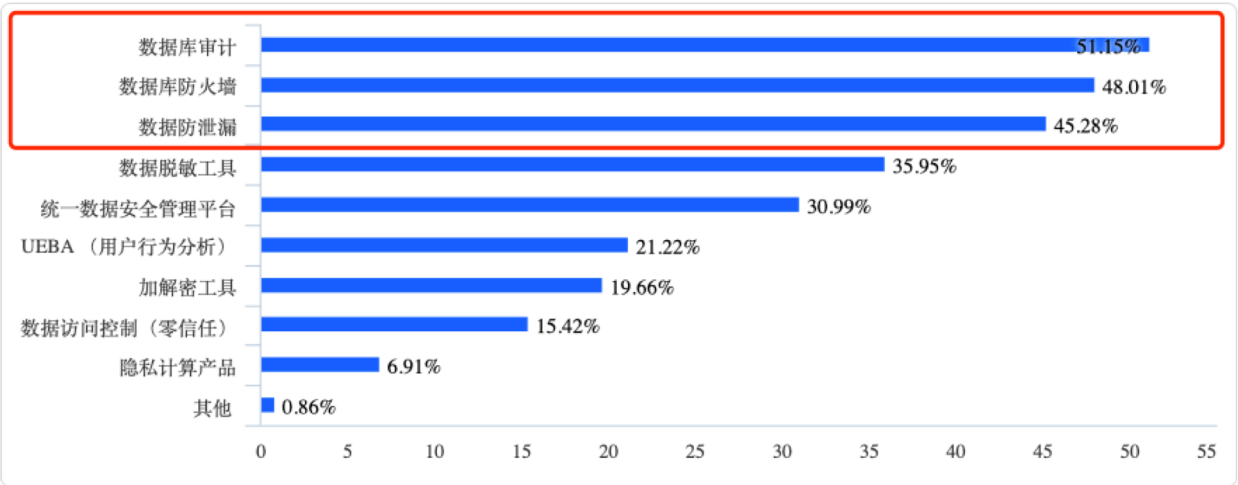
2）总结

我们认为：第二部分主要针对数据安全进程与数据安全治理普及程度进行调研。结果显示企业对数据安全意识提高，建设数据安全体系决心加强，基础的数据安全建设已经在大部分企业中开始实施。在日益紧密的企业间合作中，保障企业数据安全互通有无，发挥数据价值最大化成为了现代企业追求的目标，数据安全体系的建设，也是数字化转型成功的重要基石。

四、企业数据安全治理工作的实施及工具选取使用

1）题目统计

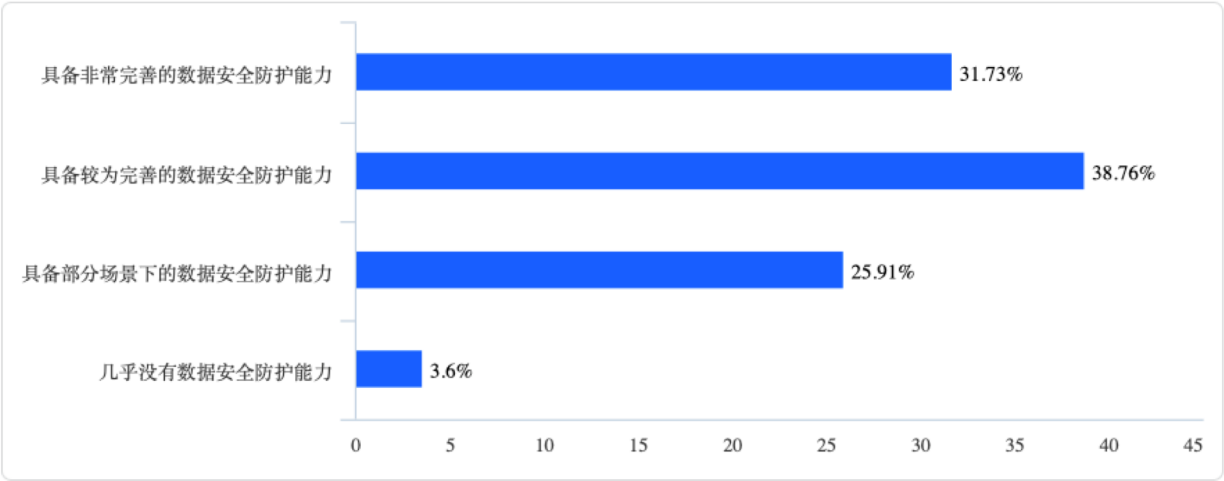
12.您所在单位用到了哪些数据安全技术工具？



关键词：防护革新，传统仍在

企业应用的数据安全技术工具最多的为数据库审计工具，在当下数据库审计作为目前用户接受度最高，使用最为广泛的数据安全产品，有其突出的优势，但如果只是单纯的具有日志记录和审计功能已经不能完全满足用户的需求，其功能必须得到进一步的扩展。传统的防火墙以及防泄漏工具仍然占有主要地位，其他安全工具的认识程度不高，有很大的宣传与普及空间。

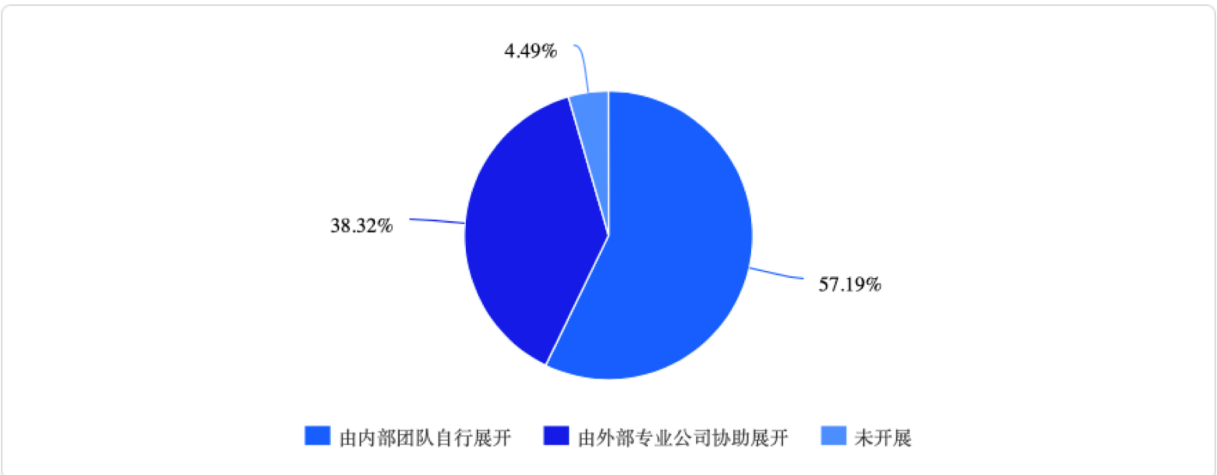
13.您所在单位的数据安全方面的防护技术水平能力处于什么样的水平？



关键词：防护水平自信满满

参与调研的企业大部分具备了完善的安全防护能力，企业对自身数据安全建设都比较有信心。但企业是否真的有充分的数据安全防护能力还要具体看企业实际建设情况。

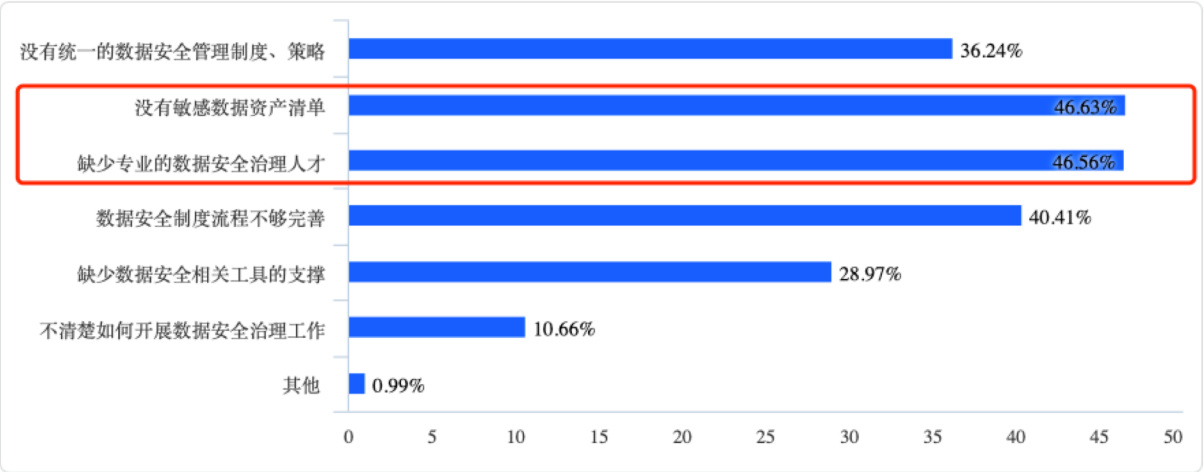
14.您所在单位是如何开展或者计划如何开展数据安全治理工作的？



关键词：数据治理，先从内部开展

现阶段数据安全治理工作主要是内部团队开展，当然也有不少的企业愿意让专业的外部公司来协助开展相关工作。整体来看企业面对数据安全治理或是数据治理工作的现状是采用“内外”结合的方式来完成相关工作的。

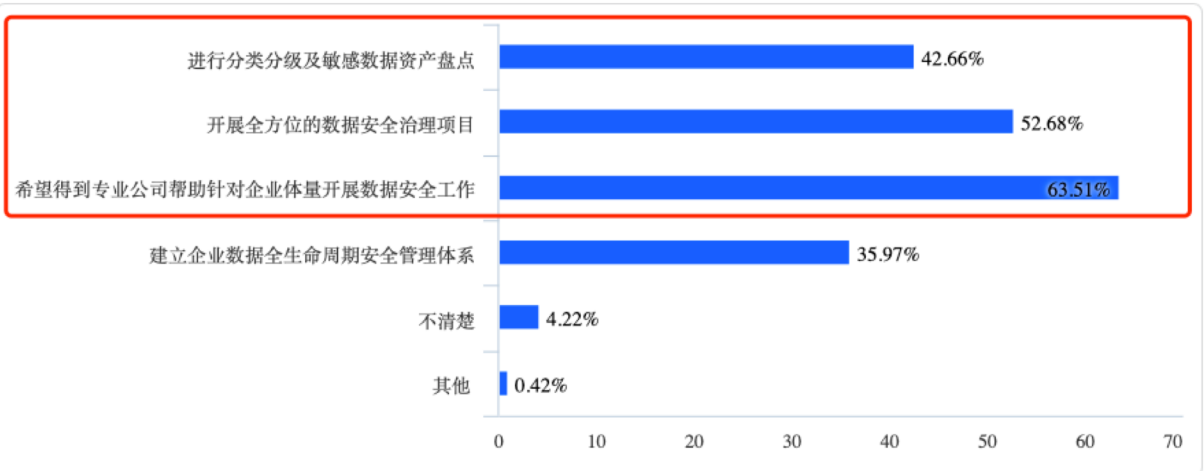
15.您认为您的单位在数据安全治理方面的挑战有哪些？



关键词：数据安全人才缺口大

大部分企业面临的挑战集中在数据资产梳理和数据安全人才引进上，没有明确的敏感数据清单，导致企业内部团队在数据资产的梳理工作上压力比较大。数据人才缺口越发显著，数据人才继续补充。其次，企业中如何制定更加完善的数据安全管理制度及制度流程也是相对比较棘手的问题。

16.您所在单位在数据安全治理领域最希望得到怎么样的服务？

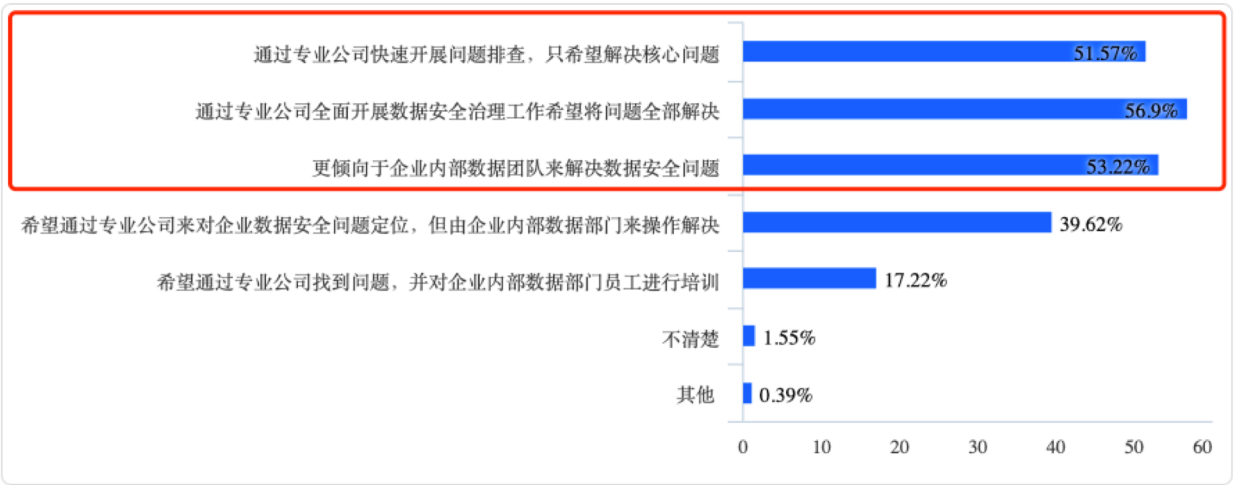


其他选项中包括：培训

关键词：希望赋能但仍有顾虑

大部分企业仍然希望通过专业的外部公司来为企业指明方向，并带领企业顺利开展数据安全治理工作，推动数据安全体系建设。企业苦于没有专业对口人才，面对数据安全治理工作无从下手。但外部公司是否会对企业内部数据存在威胁是需要关注的问题。能够提出保证数据安全的前提下为企业构建更为安全的数据体系才是数据治理服务提供商应该考虑的问题。

17.您更希望通过哪种方式解决数据安全问题？

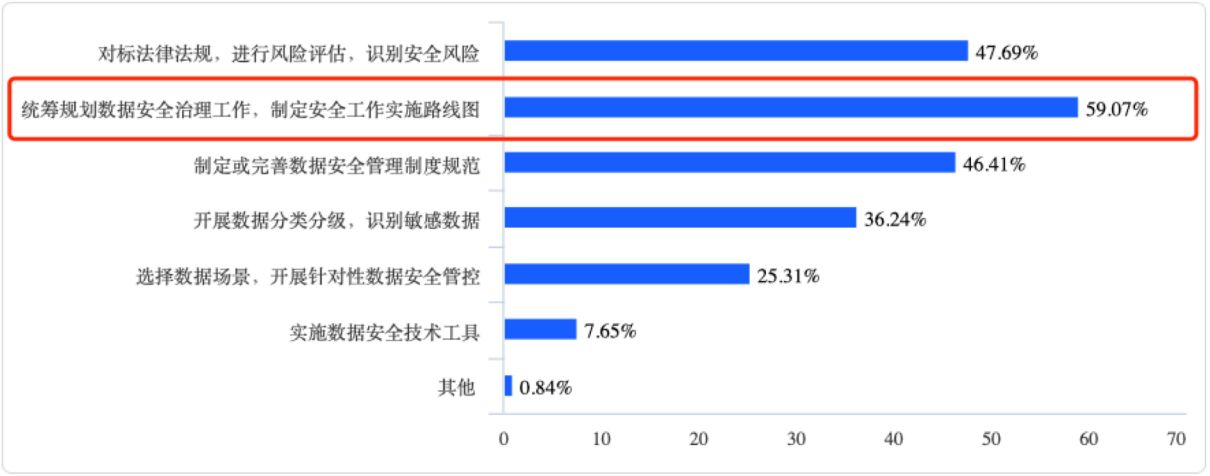


其他选项中包括：没有安全问题需要解决

关键词：专业公司备受青睐

面对解决核心问题和全面排查问题的需求，企业更愿意交给专业数据治理公司来提供服务。也有很大一部分企业基于对自由数据安全的顾虑，仍然会选择让自己的数据团队来解决数据安全问题。所以，如何提供更加安全的服务模式是专业数据治理公司应该亟待解决的问题。

18.您认为所在单位数据安全领域当前最紧迫需要开展的工作是？

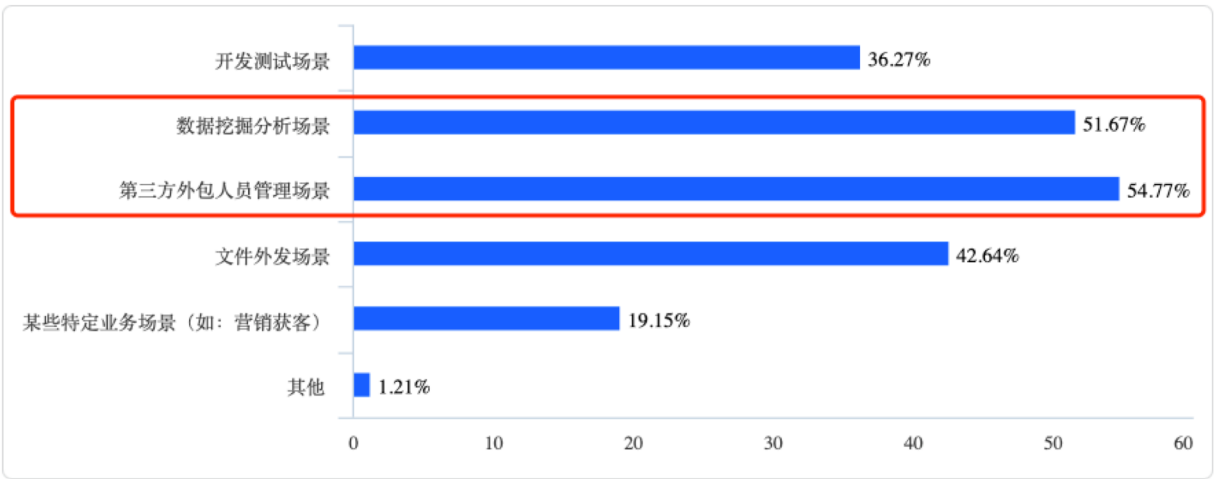


其他选项中包括：没有可开展的工作

关键词：没有方向感

面对数据安全治理工作，大部分企业缺乏方向感，实际应用阶段由于没有专业的指导，工作体系化不强，导致数据安全建设漏洞百出，进程缓慢，专职人员热情减退，得不到领导支持。面对以上问题企业更急迫能够得到专业赋能，贴合国家层面法律法规，完善数据安全制度规范，建立健全数据安全管理体系。

19.您认为数据安全最适合切入的应用场景是？

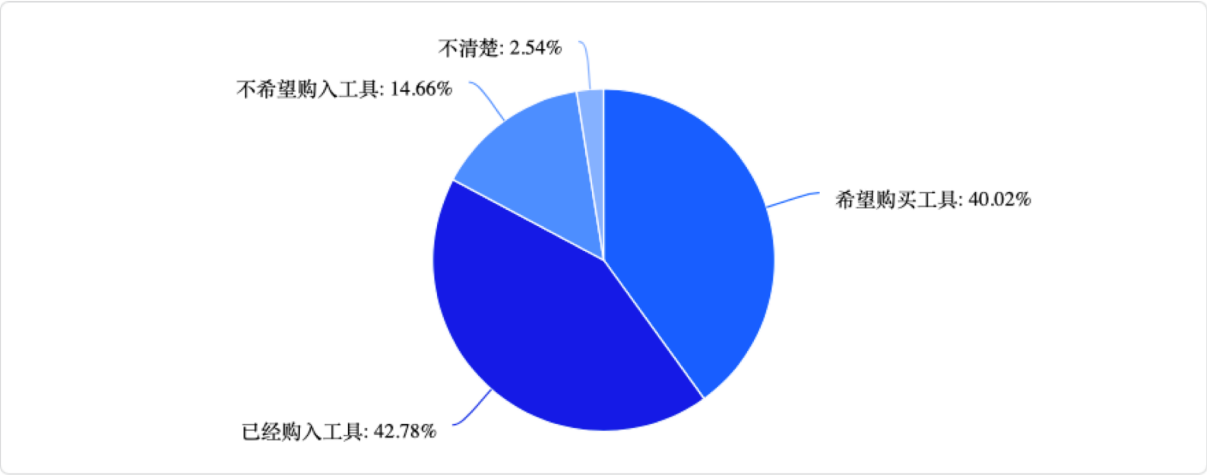


其他选项中没有包括内容

关键词：数据对外谨小慎微

总体来看企业对于涉外的数据都会谨慎小心，数据安全的切入点也正是这些对外流动的数据，企业更关注对于数据流动过程中的安全程度，也更希望数据安全体系在这些对外的数据活动中提供保护。

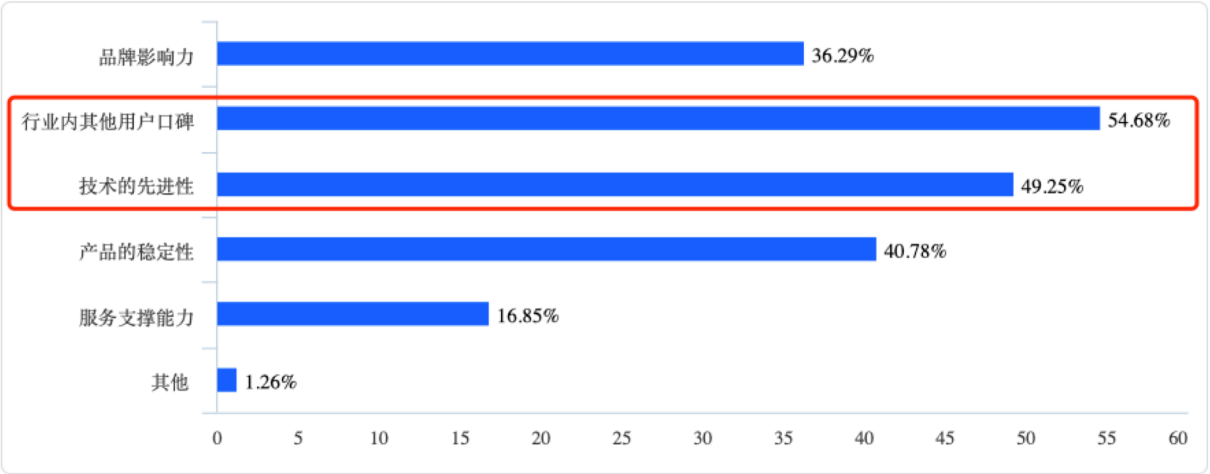
20.您所在单位是否希望通过工具来完成数据安全治理工作？



关键词：工欲善其事必先利其器

针对数据安全治理工作，企业普遍希望通过工具来解决问题，同时大部分企业已经购置了数据安全相关的工具。

21.您所在单位在选择数据安全技术工具的时候会考虑什么因素？



其他选项中包括：得到业内认可

关键词：口碑是王道

企业选择工具最为看重的是业内口碑，其次关注于技术先进性，作为软件产品行业口碑是最能够吸引和打动客户的关键因素。

22.您所在单位数据安全领域今年的工作重点有哪些？

【开放性问题】（对所有答案进行分类统计如下）

填写开放问题总数为2443条			
其中有效信息为1459条			
我们对1459条记录进行筛选分析，统计归总形成下表			
序号	归纳项目	数量（条）	占比
1	建立数据安全体系（政策、规章、制度、流程等方面）	118	8%
2	建立网络安全体系（包括防泄漏、隐私计算等工作）	220	15%
3	引进数据安全工具（包括防火墙、VPN等网络安全硬件）	437	30%
4	具体实施数据安全项目（分类分级、盘点、防泄漏等具体工作）	480	33%
5	开展企业内训和员工培训（包括各种形式的培训）	204	14%

2）总结

调研第三部分主要针对数据安全实施及数据安全治理工具进行调研。可以看出企业对于数据安全方面更希望通过工具来完成，并且大部分企业已经购置了数据安全相关的工具。同时也能看出企业在数据安全治理中纠结的部分，虽然很希望通过专业数据公司的专业团队来完成数据安全建设工作，但有对涉外数据抱有顾虑心态。所以如何提供更具安全可靠的数据安全治理服务就成为了专业数据公司需要优化的问题。数据治理人才缺口越发显著，企业内部数据团队缺乏专业人员，如何快速培养数据人才，解决数据治理人才缺口问题也尤为突出。

*** 未进行分析的题目内容涉及客户隐私信息不在此报告体现**

五、御数观点

观点来源：御数坊数据安全工作组

○ **从整体的调查结果来看**，越来越多的企业开始重视数据安全及个人信息保护，说明了数据安全法的发布产生的影响力非常大。同时企业为了贯彻数据安全法的要求进行数据安全建设和数据安全治理，也已成为众多企业已经开始或者计划开始的一项重要工作。

○ **从企业对数据这个新的生产要素的关注度来看**，数据安全与数据治理正在快速融合，很多的企业在进行企业级数据治理的时候都把数据安全的治理作为数据治理的一个非常重要的组成部分，或者基于数据治理的工作成果进一步开展数据安全治理，并且数据安全治理往往充分开展了数据资产的盘点梳理、数据认责及权限管理等数据治理的工作。

○ **从数据安全的组织架构来看**，大多数企业已经明确了数据安全组织架构的职责和定义，并且设置了数据安全的管理运营岗位，统筹数据安全建设的管理运行和建设规划工作；这也反映了大多数企业在数据安全基础建设上已经完成了基础的组织架构建设工作；但是通过调查也发现了一个现象，数据安全的管理职责在很多企业依然由信息科技或者IT部门承担，而非专门的数字化处或者大数据部门负责，反映出数据安全的职责与传统的网络安全的职责边界并未清晰界定。

○ **从数据分类分级的调研结果来看**，大多数的企业已经进行了初步的分类分级的工作，已经按照数据安全法的要求和行业规范进行了基础的分类分级相关工作，制定了分类分级的标准和规范。但是如何将分类分级的工作与数据安全管控的要求结合起来形成数据安全的统一管控策略目前还是很多企业有待解决的一个难题。

○ **从数据安全工具使用及搭建环境来看**，大多数企业对于数据安全技术工具的使用和关注更多的停留在数据库安全和终端数据防泄漏层面，这两个方面也是大多数企业在做数据安全技术工具采购或者部署时优先考虑的防护手段，同时这也体现了企业在针对结构化数据和非结构化数据的安全管控方面的主要抓手。新的数据安全技术和应用如隐私计算、零信任、UEBA等目前还未得到普遍的认可和采购，一方面反映了大家对于新技术新应用的适用性存在观望的态度，另外一方面也反映出目前的数据安全技术市场在新技术新产品的推广应用上还需要更多的时间来验证。

○ **从数据安全的企业认知及相关工作计划来看**，数据安全治理成了很多企业都非常关注的一个话题，数据安全治理工作是数据安全建设的先行条件已经成了大家的共识，但是数据安全治理如何开展、如何执行、如何落地成为大多数企业在做数据安全治理时都会面临的难题，一部分的由安全团队自行研究后开展工作，一部分希望由外部专业服务机构介入帮助企业进行数据安全治理工作。在企业内部自行开展数据安全治理工作时往往会遇到敏感数据资产识别以及人员的专业能力不足的问题，影响了数据安全治理工作开展的进度和效率。而借助外部专业服务机构进行数据安全治理可以让企业少走弯路，通过完整的数据安全治理流程解决数据安全治理开展遇到的问题。

○ **从数据安全工具选用上看**，数据安全治理工具的需求也成为很多企业在数据安全建设过程中遇到的一个普遍的需求，对于数据资产的管理、自动化的分类定级、数据访问权限的管理、数据安全管控策略的统一输出等安全需求，都需要具体的数据安全治理工具来完成，同时很多企业对于数据安全治理工具的采购更关注行业用户的口碑和技术的先进性方面，都希望能引入高效智能化的数据安全治理工具帮助企业解决数据安全治理过程中亟待解决的资产管理、分类分级、权限管控、统一策略等几方面的难题。

六、御数坊提供的服务

数据治理软件产品

利用先进技术使数据治理更简单、更规范、更高效、更智能

数据治理咨询服务

提供全域、全生命周期、端到端的数据治理咨询方案

数据管理能力评估

企业数据管理能力评估服务（DCMM/CMMI）提升企业数据管理能力

数据治理人才认证及培训

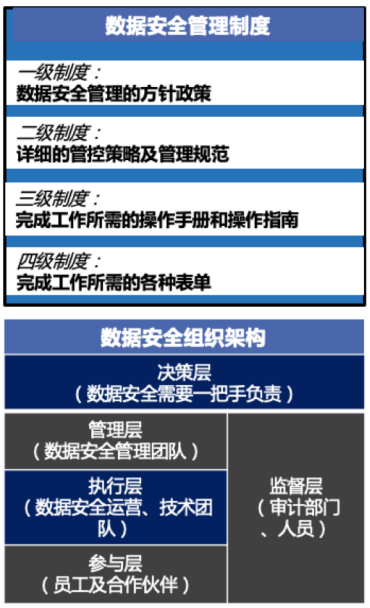
开展企业数据团队内训及数据从业者CDMP国际认证服务

基于本次调研报告，御数坊也在数据安全治理领域提供如下服务：

数据安全智能化软件服务 —— DGOffice数据管理办公室

资产层面的安全定级，百万级字段全量扫描分类定级时间一小时内完成，客户实际反馈准确率80%以上。

数据安全制度体系建设咨询服务



数据防泄漏实施专项咨询服务

数据防泄漏管控方案

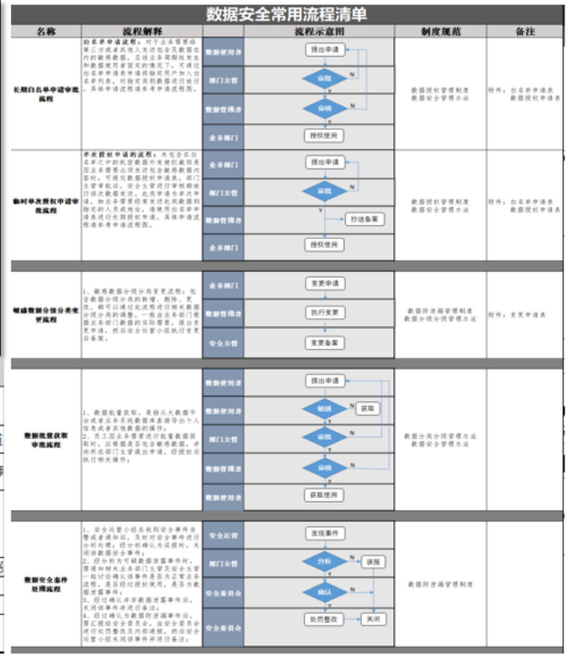
数据密级	数据发送	数据防泄漏通道管控措施							
		Web	邮件	IM	云应用	移动存储	FTP	打印	文件共享
企业机密	公司外部	阻止	阻止	阻止	阻止	阻止	阻止	N/A	N/A
	公司内部	阻止	审批	阻止	阻止	阻止	阻止	审批	加密
企业秘密	公司外部	阻止	审批	阻止	阻止	阻止	阻止	N/A	N/A
	公司内部	审批	审计	阻止	阻止	阻止	审批	审计	加密
内部公开	公司外部	告警	审计	阻止	阻止	阻止	告警	N/A	N/A
	公司内部	放行	放行	阻止	阻止	阻止	放行	放行	放行
外部公开	公司外部	放行	放行	放行	放行	放行	放行	N/A	N/A
	公司内部	放行	放行	放行	放行	放行	放行	放行	放行

数据防泄漏保护动作

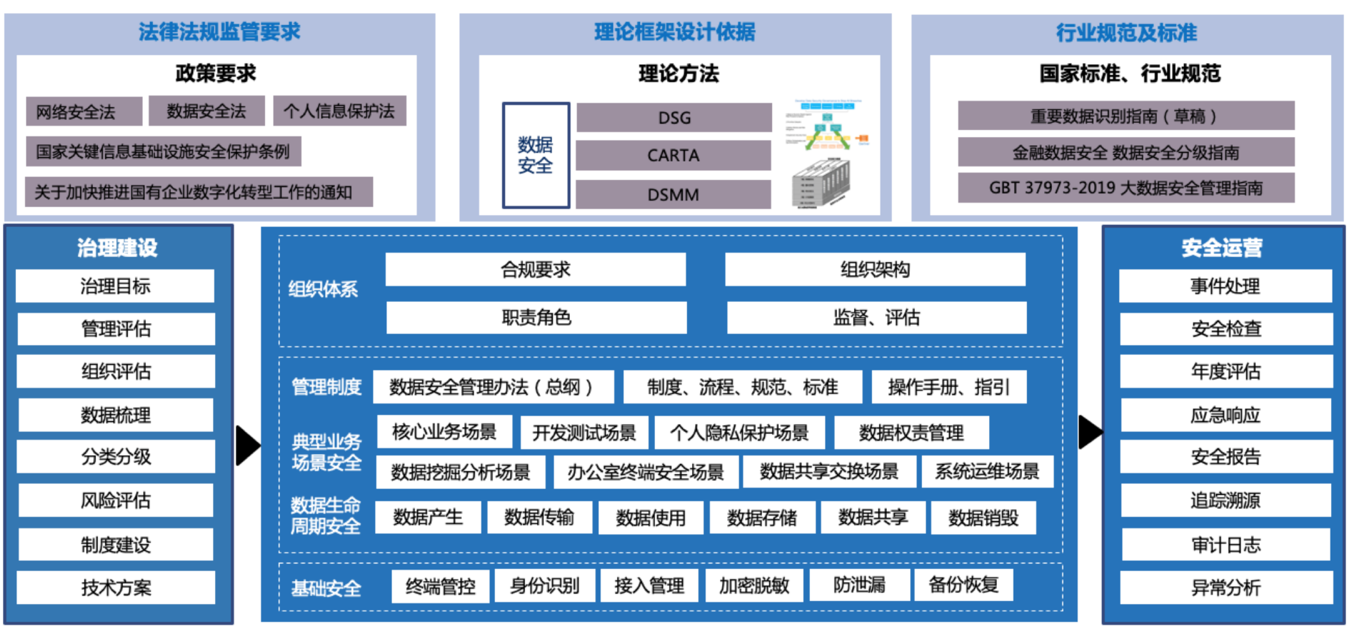
阻止	检测到敏感数据进行阻断文件传输操作，被阻止后数据传输中断。
审批	通过邮件方式申请需要并将对外发送的数据相关内容进行报备，通过审批后，会获得授权码，IT安全管理员收到通知后使用该授权码，该用户发送的敏感数据会执行审计动作。
告警	检测到敏感数据后记录本次敏感数据传输信息及证据文件作为审计日志，本次数据发送时弹出告警窗口，要求选择是否继续发送，如果选择发送就会正常进行数据发送，如果选择取消，文件发送被取消。
审计	检测到敏感数据后记录本次敏感数据传输信息及证据文件作为审计日志，本次数据发送正常进行。
加密	检测到敏感数据后记录本次敏感数据传输信息及证据文件作为审计日志，本次数据发送内容会被加密后存储。（主要针对U盘拷贝及共享文件夹上传）
放行	对该类数据不检测其数据内容，数据被放行，不会记录该次数据发送相关证据文件及事件信息。

数据防泄漏常见通道解释

Web	Web通道主要包含http及https通道
邮件	邮件通道主要为邮件客户端发送邮件通道
IM	主要包含微信、QQ、钉钉等聊天消息工
云应用	主要包含常见的网盘应用比如百度云盘、有道云笔记、印象笔记等具备文件及数据同步到云端能力的云应用客户端。
移动存储	主要为U盘、移动硬盘等USB口存储类外
FTP	主要是通过FTP协议方式上传下载的行为
打印	主要是通过打印机打印文档的行为
文件共享	主要是指通过内部共享文件目录或者共享文件服务器上传文件行为



数据安全治理咨询服务



邮箱：info@dgworkshop.com.cn

咨询电话：13581752030

地址：北京市海淀区中关村南大街甲6号铸诚大厦B座706室

邮编：100086