云计算开源产业联盟
OpenSource Cloud Alliance for industRy,OSCAR

纸鸢开源公共知识库
KITE OPEN SOURCE PUBLIC KNOWLEDGE BASE

2024年中国企业开源治理全景观察

第一部分 概 述

概 述

2020年，中国信息通信研究院制定标准《开源治理能力评价方法 第 3 部分：成熟度模型》(Open Source Governance Maturity Model，简称“OSGMM”)，确立了企业开源治理能力框架 ，规定了企业用户在使用开源软件时应遵循的流程及规范，以及企业开源治理能力成熟度的评价方法 ，有效帮助了众多企业构建和提升开源治理能力。

为了解中国企业的开源风险治理举措和治理水平， 中国信息通信研究院依托金融行业开源技术应用社区（FINOC）、通信行业开源社区（ICTOSC）、汽车行业开源社区等组织，通过问卷调查的形式针对多个行业开展了开源软件治理能力成熟度调研， 以明晰开源治理的行业现状以及未来的蓄力方向。

OSGMM2.0

2024年中国企业开源治理全景观察

OSGMM2024参与者

OSGMM2024报告深入分析了来自七大行业（包括金融、通信、汽车、能源、互联网、软件和信息服务业及制造业）共121家不同规模企业的开源治理活动匿名数据，涉及的企业分布可参见图1和图2。此外，图3展示了企业在开源软件/组件方面的使用量级，图4揭示了企业在本年度最为关注的开源风险问题。

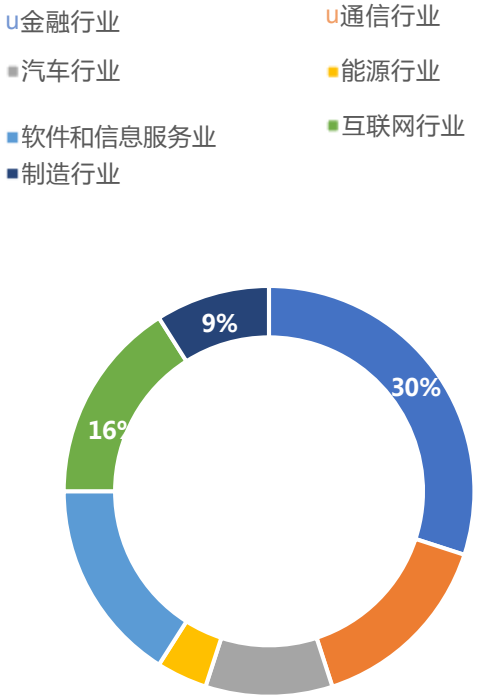

图1 OSGMM参与企业所处行业

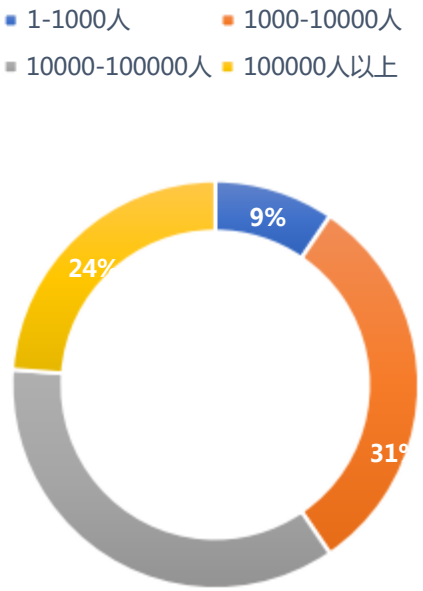

图2 OSGMM参与企业规模

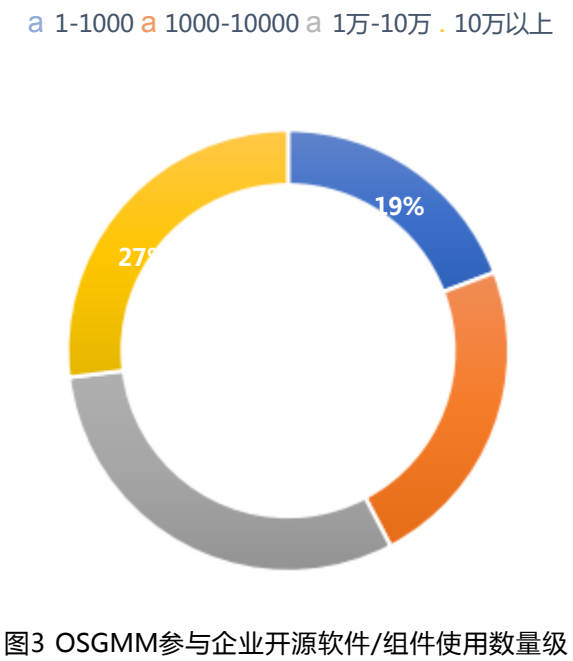

图3 OSGMM参与企业开源软件/组件使用数量级

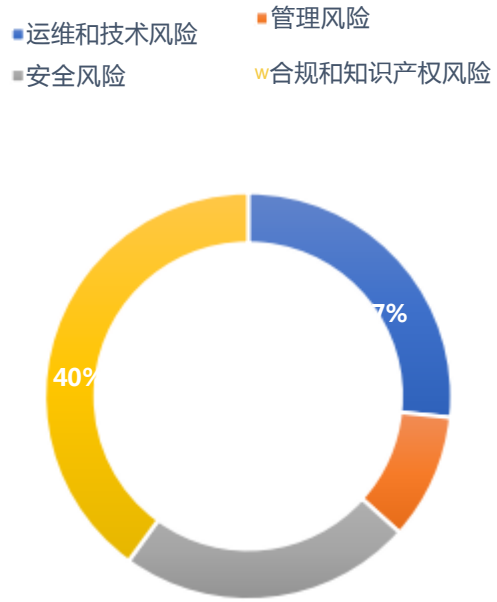

图4 OSGMM参与企业最关注的开源风险

OSGMM2.0

2024年中国企业开源治理全景观察

第二部分 洞察

OSGMM框架

OSGMM1.0整体框架由**开源软件应用治理**的3个能力要素和7个过程环节组成，包括：组织机构、管理制度、风险管理、软件测评、开发测试、运维管理、持续跟踪、退出管理、存量软件管理、第三方软件管理等领域的40余项活动。

为降低**开源软件应用风险**，OSGMM活动可视为在企业开展开源软件治理过程中所实施的控制措施，以预防、检测、纠正或控制开源软件使用所带来的系列风险。OSGMM活动级别代表了参与企业各项能力水准，具有【基础执行能力】被指定为“**基础级**-第1级”，具有【统一组织规划能力】被指定为“**增强级**-第2级”，具备【自动化的执行能力】被指定为“**先进级**-第3级”。

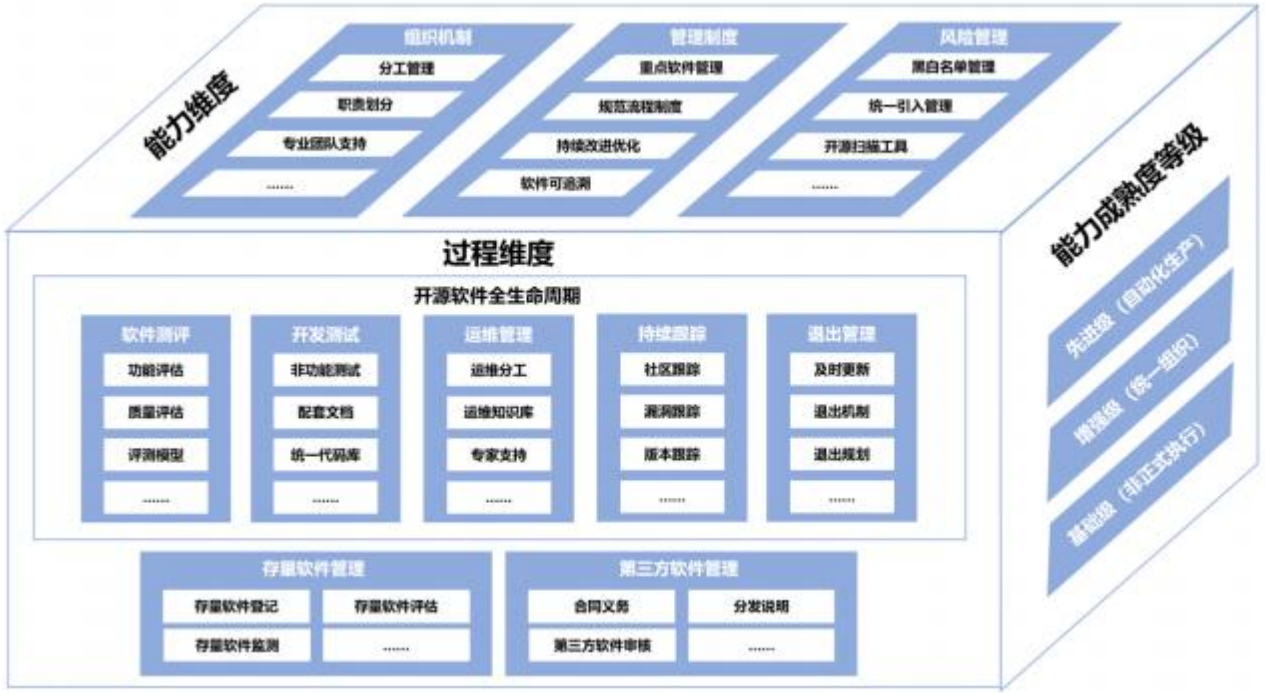

图5 OSGMM1.0模型

OSGMM开源治理活动TOP10

下表列出了2024开源治理全景观察数据池中观察到次数最多的**10项**活动，以下活动皆常见于成功的开源治理实践中（**增强级及以上**）。数据表明，如果组织正在制定自己的开源治理计划，应考虑采取这些活动。

OSGMM2024开源治理活动TOP10	
活动出现频率	**活动描述**
100%	制定开源软件的引入、使用、维护、退出等方面的制度规定
100%	在引入开源软件后，对开源漏洞、许可证信息进行持续跟踪
100%	明确企业开源治理的目标、原则、范围和流程，为后续的开源工作提供指导
100%	成立全职/兼职开源管理团队或办公室，负责企业内部的开源治理工作
98%	登记内部所有存量软件
94%	定期开展（一年2次及以上）开源相关培训
93%	通过合同义务确保软件供应商遵循企业的开源软件治理要求
90%	建设开源管理平台，辅助管理和统计开源软件信息情况及风险信息处置情况
89%	针对系统软件需求编制安装部署规范、使用操作手册等相关配套文档

88%	在引入开源软件时，进行同类软件对比与社区健康度评估工作

OSGMM2024-各领域关键活动实践情况

组织机制

Q:是否有明确的开源软件治理规划(治理目标、年度计划等)？

- **洞察：** 部分企业对于开源软件治理战略重要性认识不足，开源治理缺乏客观性和系统性，重度依赖过往经验，仅由事件触发治理机制。
- 超**53%**的被调研企业不具备明确的开源软件治理规划（治理目标、年度计划等）。

管理制度

Q:贵公司是否具备企业级开源软件管理制度？

- **洞察：** 部分企业开源软件管理主要依靠相关人员过往经验，针对重要开源软件能够形成配套管理制度，但未制定企业级的开源软件流程制度规范，未提出对开源软件全生命周期中的风险管理要求。
- 超**38%**的被调研企业不具备**企业级**开源软件管理制度。

OSGMM2.0

2024年中国企业开源治理全景观察

OSGMM2024-各领域关键活动实践情况

风险管理

Q:企业内处理开源组件安全漏洞的方式有哪些？（多选）

- **洞察：**根据安全漏洞风险等级的不同，企业处理开源组件安全漏洞的方式也有所不同；依靠内部力量处理开源组件安全漏洞所需投入资源较多，对运维人员能力要求较高，通常并非企业首选。
- 约97%的被调研企业通过**版本升级**处理开源组件安全漏洞；72%的被调研企业通过**手动应用补丁**应对安全漏洞；27%的被调研企业视情况**替换组件**或者**删除该组件**，约10%的企业不做处理。

软件测评

Q:在引入开源软件时，会进行哪些评测工作？（多选）

- **洞察：**大部分企业在引入开源软件时进行了软件功能评估、同类软件对比，但在项目活跃度评估、行业认可度和软件质量评估以及服务支持评估方面仍有改进空间。
- 98%的被调研企业在引入开源软件时，进行软件**功能评估**以及**同类软件对比**工作；53%的企业进行**项目活跃度**评估；48%的企业进行**行业认可度**评估及软件质量评估；约23%的企业会进行服务支持评估；2%的企业不进行任何评估。

OSGMM2.0

2024年中国企业开源治理全景观察

OSGMM2024-各领域关键活动实践情况

开发测试

Q:与外部开源社区的交互状态是？

- **洞察：** 当前我国大部分企业对于开源软件还仅停留在使用层面 ，未进行对外开源贡献 ，这与开源软件在我国发展较晚 ，我国企业对于开源共建共享的意识不足等因素有关。
- 约**86%**的被调研企业**仅使用**外部开源社区项目 ，关注开源社区动态； 14%的被调研企业还会参与外部开源社区贡献和建设 ，与外部开源社区建立起良好的沟通反馈机制。

运维管理

Q:开源软件确定对应负责管理部门的原则是？

- **洞察：** 企业属性和内部职责划分的不同 ，导致企业开源软件维护主体相关规则差异较大。
- 45%的被调研企业秉持**谁先引入谁负责**的原则； 28%的被调研企业按**部门职责**进行划分； 15%的企业**谁使用谁负责**； 12%的企业由**技术委员会评估**确定。

OSGMM2.0

2024年中国企业开源治理全景观察

OSGMM2024-各领域关键活动实践情况

持续跟踪

Q:在引入开源软件后，会对哪些信息进行持续跟踪?（多选）

- **洞察：** 开源软件安全漏洞问题所带来的负面影响更为直接，我国大部分企业明显更重视开源软件安全，并对开源漏洞信息和版本进行持续跟踪。
- 约**100%**的被调研企业在引入开源软件后，**对开源漏洞信息**进行持续跟踪；**78%**的企业会进行**开源许可证跟踪**；75%的企业进行版本跟踪；21%的企业进行社区基本情况的跟踪。

退出管理

Q:决定不再使用某种开源软件，对于软件退出的依据是？（多选）

- **洞察：** 我国企业对于开源软件安全风险问题已有较高程度认知。
- **100%**的被调研企业在面临严重**安全问题**时进行软件退出操作； 50%的被调研企业在面临法律合规红线时，进行软件的退出管理；48%的企业当开源软件不满足业务场景时会进行退出规划；24%的企业因开源软件更新频次过低或版本过老而进行退出规划。

OSGMM2.0

2024年中国企业开源治理全景观察

OSGMM2024-各领域关键活动实践情况

存量管理

Q:针对内部所有存量开源软件的管理措施是？

- **洞察：** 我国企业开源治理工作开展较晚 ，存量开源软件量级较大 ， 因此对于存量软件的全量、周期性管理存在一定困难。
- 超过**60%**的企业仅在新增的安全事件、生态变化等外部因素触发时针对存量开源软件进行**非周期检查**；约28%的企业对存量开源软件的安全合规性与依赖情况进行周期性分析检查； 12%的企业不针对存量开源软件进行检查。

第三方管理

Q:如何确保软件供应商遵循企业的开源软件治理要求？（多选）

- **洞察：**我国企业对于第三方软件管理的重视程度存在不足，同时缺乏开源合规相关专业人员 ，难以规范审查第三方软件中专有代码、开源代码的交互方式是否合规。
- 超过**80%**的企业通过**合同义务**来规范软件供应商，以确保其遵循企业的开源软件治理要求； 23%的企业通过交付时检查组件清单/分发说明确保供应商遵守要求； 8%的企业要求供应商提供第三方检测报告。

OSGMM2.0

2024年中国企业开源治理全景观察

垂直行业比较

开源治理成熟度高水位线图提供了基线 ，用于比较企业在各项治理指标中的实践能力和水平。成熟度级别代表了参与企业各项能力水准 ，具有基础执行能力被指定为“第1级” ，具有统一组织规划的执行能力被指定为“第2级” ，具备自动化的执行能力被指定为“第3级”。

水位线通常表示成熟度 ，如3级的水位线高 ，2级的水位线较低。如上图所示 ，所有参与本次调研的企业 ，在 “管理制度”、“存量软件管理”、“开发测试”、“软件测评”等指标下的能力较之于其他项下的能力稍强一些。

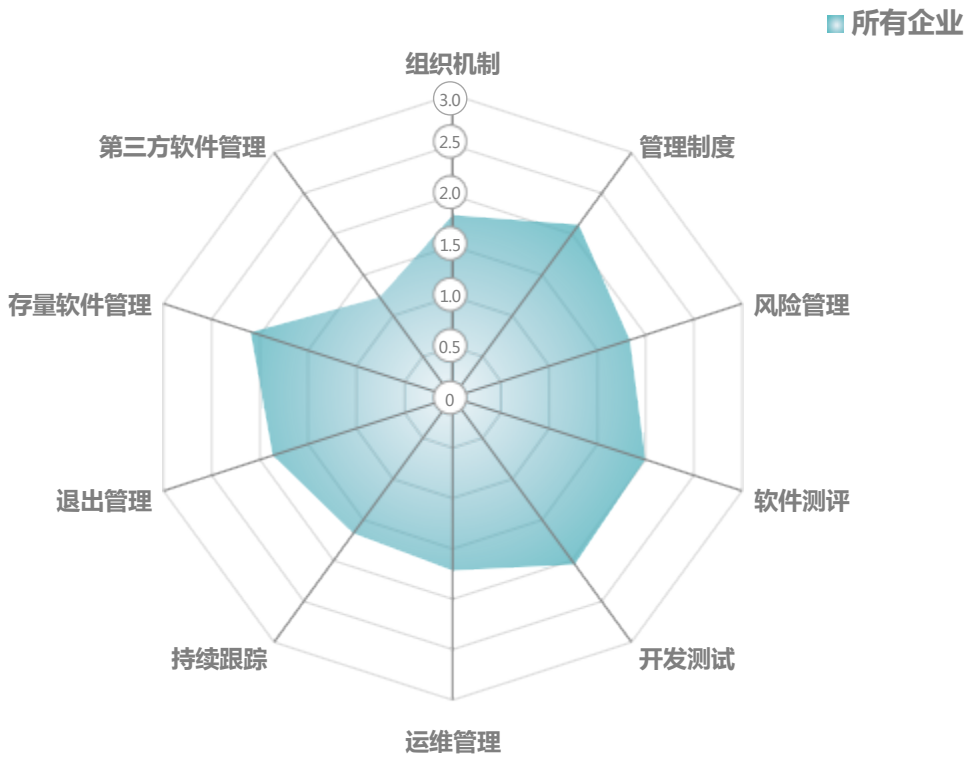

图6 OSGMM所有参与企业各项实践能力情况

OSGMM2.0

2024年中国企业开源治理全景观察

金融行业和通信行业

根据调研结果显示 ，金融和通信行业在开源软件治理方面存在不同的侧重点和成熟度水平 。 由于各自不同的特性和需求 ，它们在开源软件治理的侧重点和成熟度方面存在差异。

- 通信行业强调供应链管理和第三方软件管理。
- 金融行业则受到监管指引和法规要求的推动 ，更注重安全性和数据保护。

通信行业

通信行业通常具备更加完善的供应链管理措施 。通信行业中涉及到硬件设备和网络基础设施等复杂组件的供应链 ，促使通信企业在开源软件治理中更加重视第三方软件管理。 这使得通信行业在第三方软件的评估、 审查和

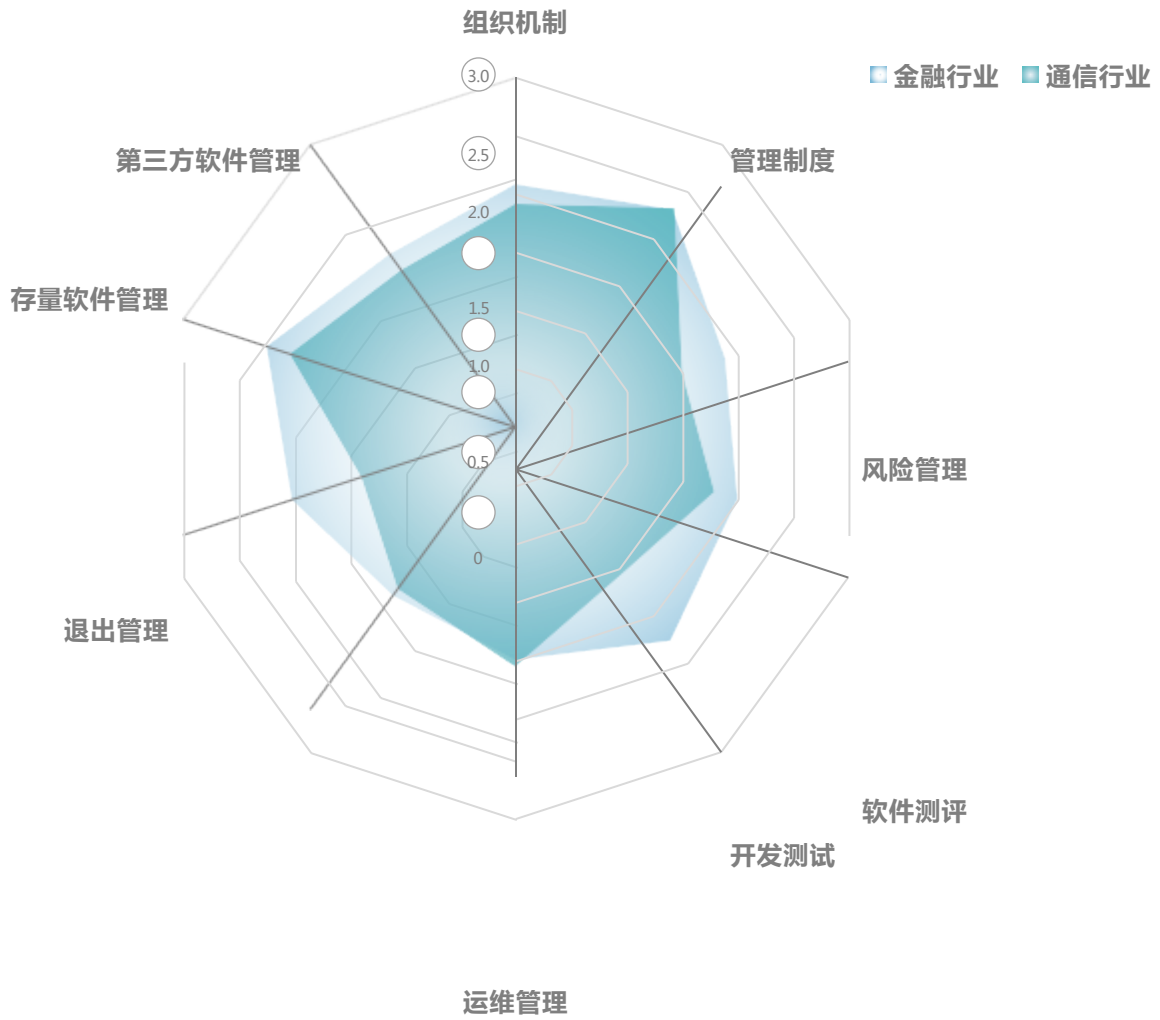

图7 OSGMM金融和通信行业参与企业各项实践能力情况

OSGMM2.0

2024年中国企业开源治理全景观察

金融行业和通信行业

金融行业

- **监管指引和法规要求**

金融行业受到监管机构的严格监管和法规要求。例如，人民银行发布的《关于规范金融业开源技术应用与发展的意见》为金融企业提供了具体的指导和规范，推动金融业开展开源治理活动。这使得金融行业在风险管理、软件测评和退出管理等方面处于领先地位。

- **安全性要求和数据保护**

金融行业对安全性和数据保护通常具有更高的要求。金融业务涉及敏感客户数据和金融交易信息，故对于开源软件的安全性和合规性关注度更高。基于此，金融行业在开源软件治理中可能更加注重安全漏洞管理、漏洞修

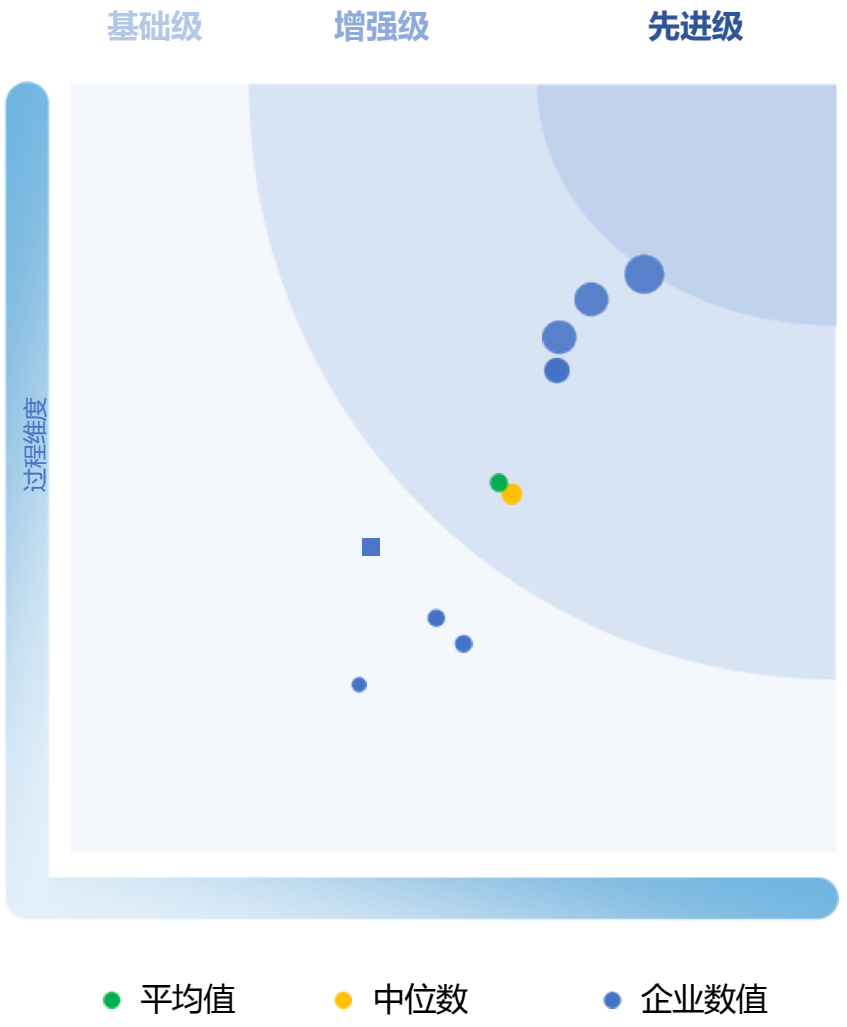

图8 金融行业部分企业OSGMM能力（圆圈大小代表企业规模）