EISS-2018企业信息安全峰会之上海站

"Face the challenge,Embrace the best practice"

November 30th,2018|SHANGHAI

2018年11月30日|上海

构筑金融云合规体系

招银云创

陈欣炜（KC）

安全加

目录


01
总体定义
合规的定义
金融云的定义
历史和由来
02
合规总览
金融云合规体系
总图
03
监管体系
金融云的监管组织，检查点和近期方向
04
合规检查
尽职检查
体系检查
监管检查
05
合规展望
195号文的影响
组织人员和工具

合规的定义

从法律名词延伸为安全名词

合规是指商业银行的经营活动与法律、规则和准则相一致。从巴塞尔银行监管委员会关于合规风险的界定来看，银行的合规特指**遵守法律、法规、监管规则或标准。**

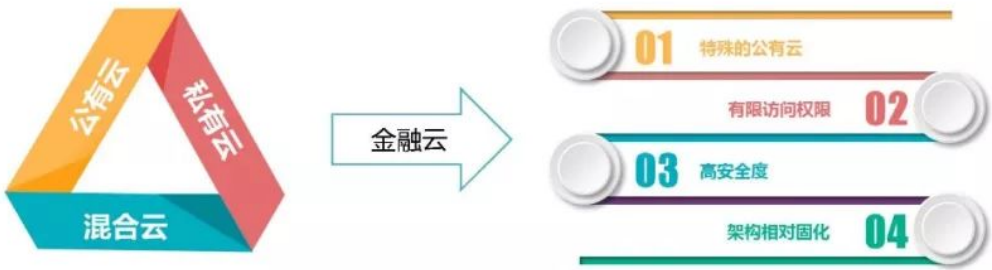
以上摘选自百度百科

《商业银行合规风险管理指引》对**合规的含义也进行了如下明确：“是指商业银行的经营活动与法律、规则和准则相一致。”**与银行经营业务相关的法律、规则及标准，包括诸如反洗钱、防止恐怖分子进行融资活动的相关规定、涉及银行经营的准则包括避免或减少利益冲突等问题、隐私、数据保护以及消费者信贷等方面的规定此外，依据监管部门或银行自身采取的不同监督管理模式，上述法律、规则及标准还可延伸至银行经营范围之外的法律、规则及准则，如劳动就业方面的法律法规及税法等。

金融云的定义

《可信金融云服务（银行类） 第1部分- 场景需求与总体框架》

3.5 行业云服务 community cloud
云服务仅由一组特定的云服务客户使用和共享的一种云部署模型。这组云服务客户的需求共享，彼此相关，且资源由组内云服务客户控制或云服务提供商控制。行业云可由行业内的一个或多个组织、第三方、或两者联合拥有、管理和运营。行业云局限于有共同关注点的行业内客户，这些共同关注点包括但不限于：业务需求、安全需求、政策符合性考虑等。
3.6 银行业行业云服务 banking cloud service
为银行这一类客户，提供的行业云服务。
3.7 金融行业云服务 financial industry cloud services
为银行、保险、证券、互联网金融等金融行业客户，提供的行业云服务。



信息化合规顶层演进

2003

《国家信息化领导小组关于加强信息安全保障工作的意见》
(中办发[2003]27号)

- 首次对我国网络安全提出设计，具有划时代意义
- 提出信息安全等级保护、密码技术、监控、应急、开发、人才、保障等要求

2005

国家信息化领导小组
《国家信息安全战略报告》
（2005年5月）

- 我国第一部真正意义的网络安全战略
- 确定了国家信息安全战略布局和长远规划

2012

国务院《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》

- 促进资源优化配置为着力点，加快建设下一代信息基础设施，推动信息化和工业化深度融合，构建现代信息技术产业体系，全面提高经济社会信息化发展水平

2014-

成立中央网络安全和信息化领导小组
《中华人民共和国网络安全法》
《国家网络空间安全战略》

- 网络强国顶层设计闭环
- 安全是发展的前提，发展是安全的保障，安全和发展要同步推进。
- 网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。

金融云合规总图


扩展合规
合规
强合规
SOC
ISO27017
C-STAR Certification
ISO27018
合规平台化
云自律
ISO27001
ISO22301
ISO20000
可信云
可信金融云
总行审计
银监局检查
网安检查
人行检查
云平台等保
多部门敏感数据检查
客户尽职检查
监管合规
安全体系合规
数据灾备合规
服务管理合规
其他合规

监管体系

强监管型

银监发2014年187号文：非驻场集中式外包风险管理的通知
银监发2013年5号文：信息科技外包风险监管指引
银监办发2008年53号文：中国银行业监督管理委员会办公厅关于印发《银行业重要信息系统突发事件应急管理规范（试行）》的通知
银监办发2014年272号文：中国银监会办公厅关于开展银行业金融机构信息科技非驻场集中式外包监管评估工作的通知
银监办发2010年294号文：中国银监会办公厅关于转发加强信息安全管理体系认证安全管理的通知
银监发2009年19号文：中国银监会关于印发《商业银行信息科技风险管理指引》的通知
银监发2011年104号文：中国银监会关于印发商业银行业务连续性监管指引的通知
银发2017年20号文：中国人民银行关于发布《中小银行信息系统托管维护服务规范》行业标准的通知
银发2018年195号文：中国人民银行关于发布实施金融行业标准规范云计算技术金融应用的通知

监管体系

监管型

银监办发2010年114号：中国银行业监督管理委员会办公厅关于印发商业银行数据中心监管指引的通知

银监发2014年39号文：关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见

银监发2016年12号文：商业银行内部审计指引

银监发2018年9号文：中国银监会关于印发银行业金融机构从业人员行为管理指引的通知

其他银监会和人行相关发文.....

跨部门监管型

工网安函2018年883号文：关于开展2018年互联网接入服务企业信息安全监督检查工作的通知

工信部网安2017年281号文：公共互联网网络安全突发事件应急预案

工信部11号令：通信网络安全防护管理办法

工信部24号令：电信和互联网用户个人信息保护规定

法释2017年10号：最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释

其他相关法律法规.....

监管体系

体系型

顶层体系

习近平：实施国家大数据战略加快建设数字中国

习近平总书记在网络安全和信息化工作座谈会上的讲话

引领网信事业发展的思想指南——习近平总书记关于网络安全和信息化工作重要论述综述

习近平：中央网络安全和信息化领导小组第一次会议重要讲话

国办函2O12年102号：国务院办公厅关于开展重点领域网络与信息安全检查行动的通知

国务院关于促进云计算创新发展培育信息产业新业态的意见

其他总书记、网信委及国务院等意见.....

法律体系

网络安全法

欧盟GDPR

.....

标准体系

JRT系列标准

可信金融云相关标准

ISO20000族

ISO27001族

ISO22301

CSA CSTAR族

其他相关标准.....

审计体系

美国AICPA SOC

德国C5数据保护

新加坡MTCS

.....

合规检查——尽职检查、体系检查和监管检查

A 访谈+检查表+证据复核

B 访谈+检查表+证据复核+技术复核

C 访谈+检查表+证据复核+技术复核+多方验证

合规检查——尽职检查

检查依据

银监发2014年187号文：非驻场集中式外包风险管理的通知

银监发2013年5号文：信息科技外包风险监管指引

其他

检查源

各银监局、各政策性银行、国有商业银行、股份制商业银行、金融资产管理公司、储蓄银行、各省级农村信用联社，银监会直接监管的信托公司、企业集团财务公司、金融租赁公司

检查对象

外包服务商不在银行业金融机构提供现场服务，或外包的关键基础设施和信息系统不在银行业金融机构产权场所，由银行业金融机构以租用设施或购买服务资源的方式获得，主要由外包服务商运维，并且外包服务商同时为3家（含）以上银行业金融机构或其他机构提供服务的外包方式。信息科技非驻场集中式外包服务商分为银行类机构和社会类机构两类，银行类机构是指依法设立的由银监会监管的银行业金融机构，其他属于社会类机构。

合规检查——尽职检查要点

第二十八条 对重要的服务提供商，银行业金融机构在与其**签订合同前**应当深入开展尽职调查，必要时可聘请第三方机构协助调查。

第二十九条 银行业金融机构在尽职调查时应当关注服务提供商的**技术和行业经验**，包括但不限于：服务能力和支持技术、服务经验、服务人员技能、市场评价、监管评价等。

第三十条 银行业金融机构在尽职调查时应当关注服务提供商的**内部控制和管理能力**，包括但不限于：内部控制机制和管理流程的完善程度、内部控制技术和工具等。

第三十一条 银行业金融机构在尽职调查时应当关注服务提供商的**持续经营状况**，包括但不限于：从业时间、市场地位及发展趋势、资金的安全性、近期盈利情况等。

第三十二条 对于关联外包，银行业金融机构不得因关联关系而降低对服务提供商的要求，应当在尽职调查阶段详细分析服务提供商**技术、内控和管理水平**，确认其有足够能力实施外包服务、处理突发事件等。

第三十三条 对于外包服务提供商为同业托管机构的情况，银行业金融机构可参照本节内容对其进行管理。

合规检查——尽职检查方式

有框架，无套路

序号	客户名	检查方式	检查依据	备注
1	某银行	现场+表单	CSA STAR+27001+等保+2013年5号文+2014年187号文	
2	某银行	现场+表单	2013年5号文+2014年187号文	
3	某银行	现场+表单+采信	等保	
4	某银行	现场+表单	2013年5号文+2014年187号文	
5	某银行	现场+表单	审计+等保+27001	
6	某银行	现场+表单	审计+等保+27001+22301+2013年5号文+2014年187号文	
7	某银行	现场+表单	27017+27001+等保+2013年5号文+2014年187号文	
8	某银行	现场+表单	2013年5号文+2014年187号文	
9	某银行	现场+表单	2013年5号文+2014年187号文	
10	某银行	表单+采信	2013年5号文+2014年187号文	

合规检查——尽职检查基本要求

银行业金融机构应当对重要的非驻场外包服务进行实地检查。实地检查原则上一年不少于一次，检查结果作为外包服务提供商项目考核及准入的重要指标。

（一）外包服务商对**本机构与其他机构**的**设施、系统和数据**是否有**明确、清晰的边界**；

（二）外包服务商是否有**管理制度和技术措施**保障本机构**数据**的**完整性和保密性**；

（三）外包服务商对涉及本机构的服务器、存储、网络设备、操作系统、数据库、中间件**等**软硬件基础设施是否具有**最高访问权限**；

（四）外包服务商是否拥有或可能拥有**业务系统**的最高**管理权限**，外包服务商是否拥有或可能拥有业务系统的访问权限，是否能够**浏览、获取客户敏感信息**；

（五）外包服务商是否有完善的**灾难恢复设施和应急管理体系**，对关键基础设施和信息系统运行是否有**业务连续性**安排；

（六）外包服务商是否知晓并遵从了**银行业相关监管法规**要求。

银行业金融机构可以**委托第三方机构**开展尽职调查，或者**采信**其他银行业金融机构对同一外包服务商6个月内的尽职调查结果。

银行业金融机构可以**采信**监管机构对外包服务商在12个月内的评估或审计结果，不再重复安排外部评估或审计。

在外包合同签订前至少**20**个工作日向银监会或其派出机构对非驻场集中式外包活动进行报告，报告内容应当包括**尽职调查报告和风险评估报告**。

合规展望——政策收紧、人员组织和合规平台化

银发【2018】195号《金融行业标准规范云计算技术金融应用》带来的挑战

JRT 0166-2018 技术架构
JRT 0167-2018 安全技术要求
JRT 0168-2018 容灾

合规人员组织和架构

合规展望——处罚案例

网络安全法施行3个月内处罚案例

7月：汕头网警支队办理首宗适用《网络安全法》行政案件，警告处罚并责令其改正

7月：山西忻州市某省直事业单位网站不履行网络安全保护义务被处罚，行政警告处罚并责令其改正

7月：四川宜宾市翠屏区教师培训与教育研究中心网站被黑，翠屏区教师培训与教育研究中心处一万元罚款，对法人代表唐某某处五千元罚款。

7月：安徽铜陵网警依法查处违反《网络安全法》全省第一案，金某处以行政拘留十日的处罚

8月：重庆市首页科技发展有限公司未依法留存网络日志，警告处罚，并责令限期十五日内进行整改

8月：宿迁网警成功查处全省首例违反《网络安全法》接入违规网站案

8月：58同城、赶集网等因违法违规发布“大棚房”租售信息被约谈

8月：哈尔滨市警方依法查处黑龙江省首宗违反《网络安全法》案件，责令方正县政府农业技术推广中心立即整改，并给予2万元罚款的处罚

8月：网信办《网络安全法》处罚第一案，BOSS直聘网站立即整改

8月：腾讯微信、新浪微博、百度贴吧涉嫌违反《网络安全法》被立案调查

8月：安徽网警依法查处一起违反网络安全等级保护制度案件，怀远县教师进修学校处以一万五千元罚款，对负有直接责任的副校长处以五千元罚款。

8月：淘宝网、同花顺金融网、蘑菇街互动网等5家网站被责令限期整改

9月：国内首例高校违法案例诞生，因未落实等保制度致学生信息泄露，淮南职业技术学院被责令立即整改

9月：广东网络安全执法：阿里云等四家企业被查

Thanks