

安世加

AFSS-亚太金融安全峰会

护驾金融，安定民生

上海站 | 2021年7月23日





李扬，现任信也科技安全经理。从业以来，先后承担过安全运维，合规，研发角色。牵头多次顺利通过非银行支付机构支付业务设施技术，等级保护，PCI-DSS，ISO-27001认证。设计并落地移动条码支付系统，实时风控系统，4A系统。选择安全，从业安全，坚持安全，是金融安全行业的一线老兵。

个人背景

- 李扬，现任信也科技安全经理。
- 从业以来，先后承担过多项安全角色，如安全运维，安全合规，安全研发等。多次牵头顺利通过非银行支付机构支付业务设施技术，等级保护三级，PCI-DSS，ISO-27001认证。设计并落地移动条码支付系统，移动安全实时风控系统，移动环境检测系统等。
- 选择安全，从业安全，坚持安全，是金融安全行业的一线老兵。
- 声明：本次分享仅代表作者个人观点，与所就职的信也科技无关。

目录

1.安全合规的定位



2.安全合规的现在



3.安全合规的未来



4.总结

1.1.安全合规的定位—核心驱动力



1.2.安全合规的定位—回顾

起源

- 无明显标志性事件

雏形

- 监管
 - 2008年信息安全等级保护三级—专职安全管理员
- 增信
 - 信息安全管理体系认证—ISO27001等

爆发

- 2017年—网络安全法
- 2019年—App个人信息保护治理

1.3.安全合规的定位—工作界面



2.1.安全合规的现在—监管条线

行业	通用	行业自治	国外监管
<ul style="list-style-type: none">• 一行两会• 人民银行• 银行保险监督管理委员会• 证券业监督管理委员会• 卫生健康委员会•	<ul style="list-style-type: none">• 4部委• 12部委	<ul style="list-style-type: none">• 支付清算协会• 互联网金融协会• 互联网协会• 广告协会•	<ul style="list-style-type: none">• SOX• HFCA-外国公司问责法

2.2.安全合规的现在—监管态势

《App违法违规收集使用个人信息行为认定方法》

国务院新闻办公室网站 www.scio.gov.cn 2019-12-20 来源：中国网信网

国家互联网信息办公室秘书局

工业和信息化部办公厅

公安部办公厅

国家市场监督管理总局办公厅

网络安全审查办法

2020年04月27日 12:00

来源：中国网信网



【打印】 【纠错】

国家互联网信息办公室
中华人民共和国国家发展和改革委员会
中华人民共和国工业和信息化部
中华人民共和国公安部
中华人民共和国国家安全部
中华人民共和国财政部
中华人民共和国商务部
中国人民银行
国家市场监督管理总局
国家广播电视总局
国家保密局
国家密码管理局

令

2.3.安全合规的现在—合规要点



2.4.安全合规的现在—权力来源

从属

安全

合规

法务

信息技术

研发

运维

.....

汇报线

CTO

CSO

CIO

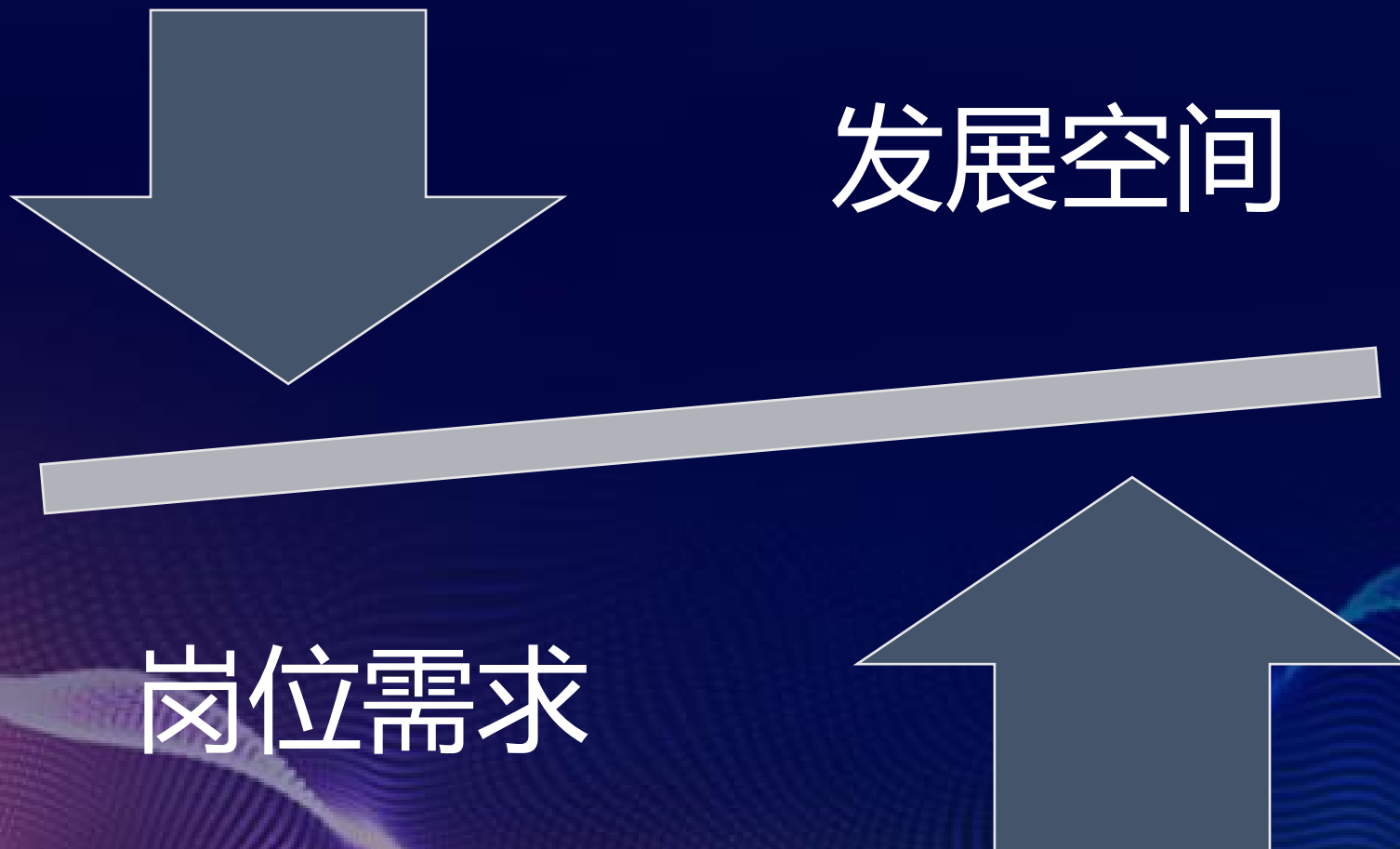
CCO

总监

经理

.....

2.5.安全合规的现在—招聘



2.6.安全合规的现在—复杂的合规链



2.7.安全合规的现在—工作现状

<徒手合规>

摸底基本靠聊,

寻人基本靠吼,

统计基本靠表,

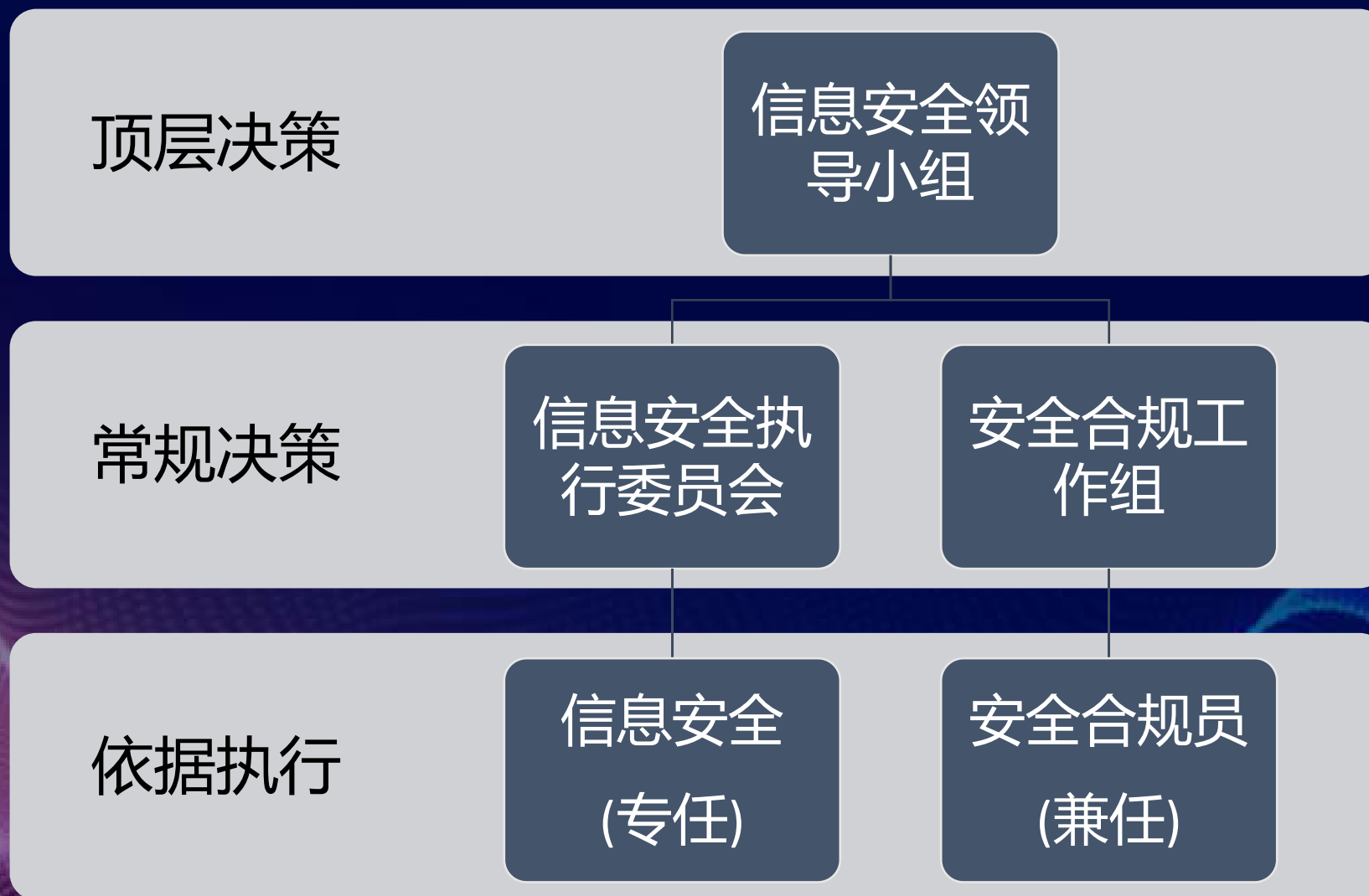
通知老是延迟,

差距基本靠猜,

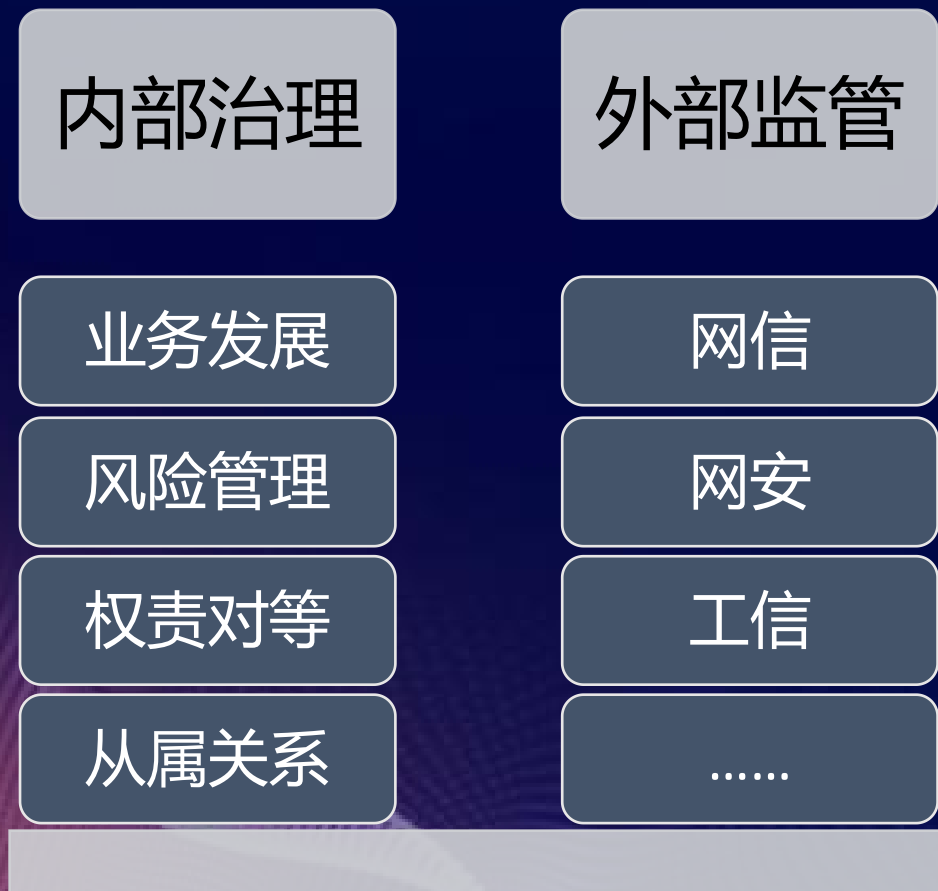
整改基本靠关。

可这样能够应对当前甚至未来的数字化挑战么？

2.8.安全合规的现在—虚拟组织架构



3.1.安全合规的未来—分分合合



3.2.安全合规的未来—安全vs合规

技术



法律

安世加

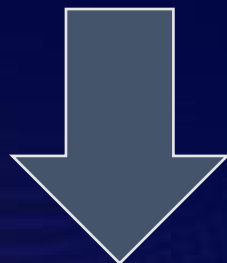
3.3.安全合规的未来—岗位价值均值回归

本科 绿牌专业	2020 年	2019 年	2018 年
信息安全	★	★	★
软件工程	★	★	★
信息工程	★	★	

*麦可思,《2020年中国大学生就业报告》



红利期



回归期

第二十八条 证券基金经营机构应当制定合规负责人与合规管理人员的薪酬管理制度。合规负责人工作称职的,其年度薪酬收入总额在公司高级管理人员年度薪酬收入总额中的排名不得低于中位数;合规管理人员工作称职的,其年度薪酬收入总额不得低于公司同级别人员的平均水平。

*证券监督管理委员会,《证券公司和证券投资基金管理公司合规管理办法》

3.4.安全合规的未来—战略思考



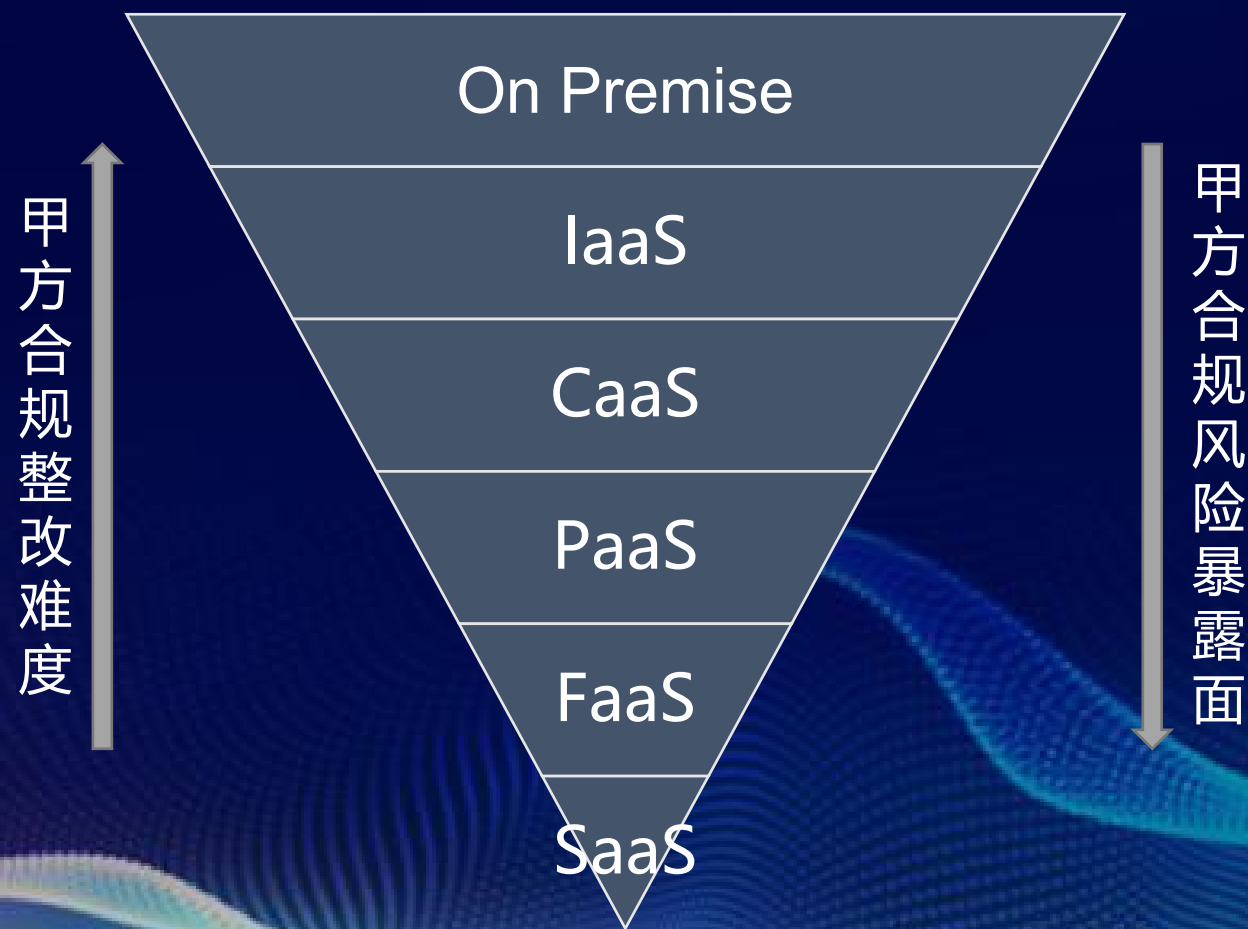
3.5.安全合规的未来—战术思考

- 标准化

- 设计安全-SecurityByDesign
 - 安全合规评审
- 默认安全-SecurityByDefault
 - CIS, 安全组件库等
- 安全即服务-SecurityAsAService
 - KMS, MFA, CAS等
- 云

- 自动化

- 安全合规度量
 - 合规是安全方面最易量化的切入点



4. 总结



个人微信一多多交流



安世加

安世加专注于安全行业，通过互联网平台、线下沙龙、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站：

<https://www.anshijia.net.cn>

微信公众号：asjeiss



安世加