"Face the challenge, Embrace the best practice"

EISS - 2019 企业信息安全峰会 ②深圳站 2019.8.16



从隐私保护建设看安全管理



预设背景

多样 的业务

数十个App

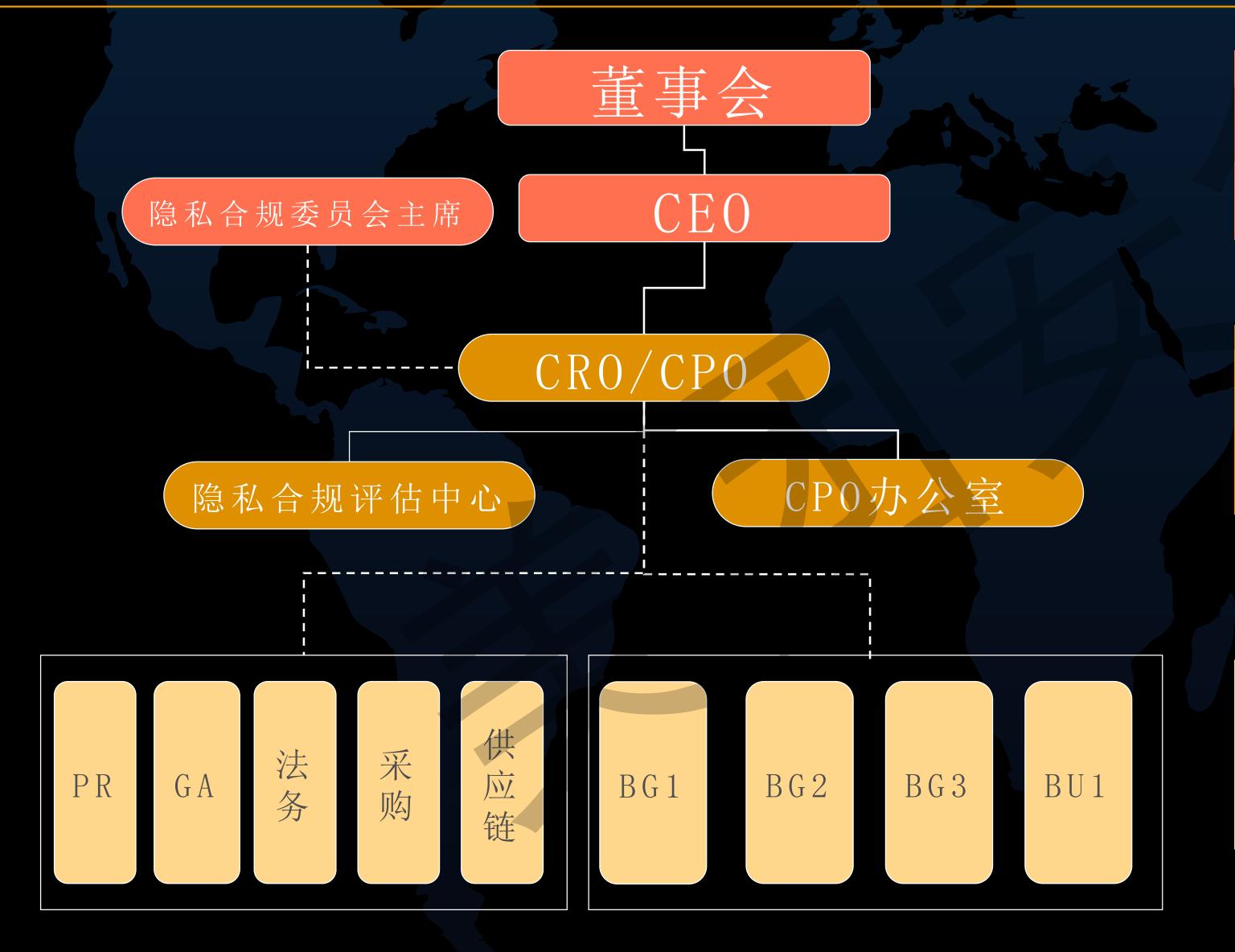
全球业 务部署 全栈并发数亿

几十万的 Server OS

数万 的雇员 理解安管



治理架构



策略制定:

刷脸,增值,提供服务

执行落地:

经营主体,准入,税务及服务成本,危机处理

执行落地:

能力建设,ROI控制



技术体系

用户可见的数据保护说 隐私通知 隐私保护门户 隐私政策 数据主体请求 用户体验 明和可以自助使用的个 数据滥用报告 透明度报告 数据泄露通知 人数据管理功能 联通隐私保护技术栈与 Privacy by Privacy by 使能机制 PIA DPIA 用户体验功能 default design 隐私控制API 用户同意管理 用户诊断日志 隐私dashboard 等价类匿名 差分隐私 Data masking 关键技术 Location Anti-ID 随机化 fingerprinting privacy 同态加密 基于属性的加密 秘钥管理 默认加密



工程能力

DPO 团队 多部门会议形成的 checklist及评估结 果

从系统中获取的脱 敏样本数据 dashboard+子业务 详情报告 (基于日志分析)

RD

手工填写的接口文档

版本匹配的自动生成的文档 成的文档 (DevOps)

灰度发布时匹配的 隐私验证数据

隐私技术团队

各类手工截图

离线测试工具

集成到发布/自动 部署平台的用户测 数据呈现

救火状态

可分析状态

可循环状态



常见的实践



基于发布平台和部署平台的App检测能力

- 权限使用的检测与验证
- · SDK的发现及动态验证



隐私政策的治理

- 版本管理
- Privacy Notice管理
- 同意管理



