第四章 法律、法规和合规性

4.1 法律的分类

4.1.1 刑法

- 刑法是法律体系的基石，刑法非常严肃，卷入其中需请求律师帮助

4.1.2 民法

- 民法是法律体系的大部分，用于维护社会秩序
- 民法和刑法的主要差异在于执行方式，刑法是政府通过执法调查员和检察官对犯罪人采取的措施，民法是受到冤枉的人得到法律建议，政府在纠纷和争论过程中不站在任何一方
- 行政法:行政机构要求众多的机构对保证政府功能的有效性担负广泛的责任

4.2 法律

4.2.1 计算机犯罪

- 计算机诈骗和滥用法案：用于跨越州边界的计算机犯罪，避免违反州的权利和践踏宪法
- CFAA修正案(1994年)
    i. 可能造成计算机系统损害的、生成任何类型恶意代码的行为是不合法的
    ii. 修改CFAA，包含了所有被用于州间贸易的计算机，而不只是包含联邦利益的计算系统
    iii. 允许关押犯人，不管他们是否造成实际的损坏
    iv. 为计算受害者提供民事诉讼的法律权利，受到的损失可以申请减轻和补偿
- 计算机安全法案(1987年)：为所有的联邦机构设置了安全要求基准
- 美国国家信息基础设施保护法案(1996)：扩展了计算机诈骗和滥用法案的保护范围，增加新的领域
- 文书精简法案(1995年)：要求机构在请求大多数类型的公共信息之前，必须获得美国行政管理和预算局的批准
- 政府信息安全改革法案(2000年)：修正了美国法典，从而实施额外的信息安全策略和措施
- 美国联邦信息安全管理法案：要求联邦机构实施一个信息安全项目
    i. 定期评估风险

ii. 基于风险评估的策略和程序，在成本和效益的原则下，把信息安全风险降低到一个可接受级别
iii. 下级计划为网络、设施、信息系统和信息系统集群提供恰当的信息安全
iv. 提供安全意识培训
v. 定期测试和评估安全策略、程序、时间和安全控制的 有效性
vi. 规划、实施、评估和记录补救措施
vii. 制定对信息安全事件监测、报告和响应的流程
viii. 制定计划和程序来确保支撑着组织运营和资产信息的系统持续运行

4.2.2 知识产权

- 版本和数字千禧年版权法案
  i. 版权法只保护计算机软件的内在表达方式，也就是实际的源代码，不保护软件背后的思想和过程
  ii. 版权法保护时间：最后一位创作者死后70年
  iii. DMCA还限制了当网络服务提供商的线路被犯罪用来违反版权法时应承担的责任
- 商标：商标是单词、口语和标志语
  i. 商标不需要正式注册，公众活动期间使用商标，就会获得相关商标法保护,TM符号
  ii. 正式承认商标，在美国专利局和商标局进行注册，注册后得到R符号表示
- 专利权：保护发明者的知识产权，提供20年的保护
- 专利权的要求:
  i. 发明必须是新的
  ii. 发明必须是有用的
  iii. 发明不是显而易见的
- 商业秘密：保存生产过程的秘密
- 版权和专利的缺点
  i. 版权和专利申请时，要求公开透露发明细节
  ii. 版权和专利都提供有限时间的保护
- 许可证
  i. 合同许可证
  ii. 收缩性薄膜包装许可证协议，撕开封装软件包的收缩薄膜包装就承认了合同条款
  iii. 单击包装许可证协议，单击一个按钮，表示已阅读协议条款并且同意遵守这些条款
  iv. 云服务许可条款，屏幕上简单闪现法律条款供检阅

4.2.3 进口/出口

- 计算机出口控制
- 加密产品出口控制

4.2.4 隐私

- 美国隐私法
  i. 隐私法案(1974):严格限制美国联邦政府机构在没有当事人书面同意的情况下，向他人或其他机构泄露隐私信息的能力
  ii. 电子通信 隐私法案(1986)个人电子隐私的侵犯是犯罪行为
  iii. 执法通信协助法案(1994) 无论采用怎样的技术，所有通信运营商都需要允许持有适当法院判决的执法人员进行窃听
  iv. 经济和专有信息保护法案(1996) 窃取经济信息的行为视为针对行业或公司的间谍行为
  v. 健康保险流通与责任法案(1996) 规定要求医院、医师、保险公司和其他处理或存储个人医疗隐私信息的组织采取严格的安全措施
  vi. 2009关于经济和临床健康的卫生信息技术法案 引入泄密通告需求，泄密影响 超过500人，需通知卫生和人力服务部的部长和媒体
  vii. 儿童联机隐私保护法案(1998年) 对关心孩子和有意收集孩子信息的网站提出要求 网站必须发送隐私通知，清楚说明收集信息的类型和用途 必须向父母提供机会，复查任何从他们的孩子那里收集到的信息，并可以永久删除这些信息 孩子年龄小于13岁，收集信息前，必须获得负责的允许
  viii. Gramm-Leach-blilry法案(1999年) 对银行、保险公司和贷款提供商受到对他们所能体统的服务和相互共享的信息严格限制
  ix. 美国爱国者法案（2001年）官方对个人的一揽子授权，政府可监视此人的所有通信、ISP可以自愿的向政府提供大范围的信息
  x. 子女教育权和隐私法案，赋予18岁以上的学生和未成年学生父母的确定隐私权
  xi. 身份偷窃和冒用阻止法案
- 欧盟隐私法，在欧洲进行商业活动的美国公司必须遵守7项处理个人信息要求
  i. 通知
  ii. 选择：信息用于其他目的或第三方共享，他们必须允许个人决定退出，敏感信息必须采取决定参加的策略
  iii. 向前传递：企业只可能与其他遵守安全避难所原则的企业共享时数据
  iv. 访问：个人必须被授权访问任何包含其个人信息的数据
  v. 安全：必须采取适当的机制保护数据，以防止丢失、滥用和未授权的公开
  vi. 数据完整性：企业必须采取措施，确保他们所维护信息的可靠性
  vii. 实施：企业必须为个人提供争论解决办法，想管理机构提供证明，表明遵守安全避难所规定

4.3 合规性

- 组织受到各种法律约束以及来自监管机构或合同义务的强制合规

4.4 合同和采购