1(main concepts of information security)

保护计算机硬件、软件和数据不被破坏、篡改和泄露。

2(Risk assessment)

（风险识别、风险分析、风险评估、风险处理、风险监测）Risk identification, risk analysis, risk assessment, risk treatment, risk monitoring.

3(Information security and functional security)

信息安全主要是关于信息的保护。功能安全主要关注系统功能的正确性和安全性**。**

4(Identification and authentication)

识别是确定用户的身份，身份验证是验证用户是否就是他所声称的那个人。

5(Access control in information systems)

防止非法的主体进入受保护的网络资源。

允许合法用户访问受保护的网络资源。

防止合法的用户对受保护的网络资源进行非授权的访问。

6(A cryptographic method to ensure information integrity)

哈希

7(Electronic signature. Public Key Infrastructure )

提供了验证身份、保护数据完整性和机密性的方法。

8(Static and dynamic integrity constraints)

静态约束: 隐式约束和显式约束

隐式约束：隐含于数据模型中的完整性约束

显式约束：隐式约束不能完全描述现实中的规定或约束

动态约束：反映数据库状态变迁的约束。

9（Firewall packet filtering rules）

允许或禁止特定的IP地址或IP地址范围访问网络。

允许或禁止特定的端口或端口范围通过。

允许或禁止特定的数据包类型通过，如HTTP、FTP或SMTP。

10（information availability approach）

用户模型法，用户调查法，专家评审法，观察法（User model method, user survey method, expert review method, observation method）

11（Anti-malware tools）

Comodo AEP，AVG，ESET NOD32 Antivirus

12（National policy in the field of information security）

网络安全法，个人信息保护法，密码管理法，网络安全等级保护制度（Network security Law, Personal Information Protection Law, password management law, network security level protection system）

14（Information security supervision）

完善法律法规，加强技术研发与创新，加强国际合作（Improve laws and regulations, strengthen technology research and development and innovation）

15（Protection of personal information.）

使用安全软件，将数据进行备份

19（Security system development life cycle）

安全需求进行分析和定义，进行安全编码，进行安全测试，安全部署和运维（Security requirements are analyzed and defined, securely coded, securely tested, securely deployed, and O&M）

20（Enterprise information security policy）

采用防火墙、对重要应用系统进行身份认证与访问控制；对数据进行加密存储与传输；

21（System security policy）

访问控制，防火墙配置，身份验证，权限管理，数据加密，数据备份与恢复

22（Risk management）

风险识别是风险管理的第一步，其目的是识别出可能对项目或组织产生负面影响的事件或情况。

风险评估是对识别出的风险进行量化和定性分析的过程。这包括评估风险的概率、影响程度以及可能对项目或组织目标造成的后果。

24（Security management model）

海因里希法则，冰山理论。