1. 信息安全：就是要保护信息免受威胁的影响，从而确保业务的连续性，缩减业务风险，最大化投资收益并充分把握业务机会。
2. 信息安全事件：是指系统、服务或网络的一种可识别的状态的发生，它可能是对信息安全策略的违反或防护措施的失效，或是和安全关联的一个先前未知的状态。
3. 信息安全事故：一个信息安全事故由单个的或一系列的有害或意外信息安全事件组成，它们具有损害业务运作和威胁信息安全的极大的可能性。
4. 方针：管理层正式发布的总体意图与方向。
5. 风险：就是指信息资产遭受损坏并给企业带来负面影响的潜在可能性。
6. 风险分析：系统地使用信息以识别来源和估计风险。
7. 风险评价：将估计的风险与既定的风险准则进行比较以确定重要风险的过程。
8. 风险评估：风险分析和风险评价的全过程。
9. 风险管理：指导和控制一个组织的风险的协调的活动。
10. 风险处置：选择和实施措施以改变风险的过程。
11. 风险管理：以可接受的代价，识别、控制、减少或消除可能影响信息系统的安全风险的过程。
12. 资产：任何对组织具有价值的东西，包括计算机硬件、通信设施、建筑物、数据库、文档信息、软件、信息服务和人员等。
13. 弱点：也被称作漏洞或脆弱性，即资产或资产组中存在的可被威胁利用的缺点，弱点一旦被利用，就可能对资产造成损害。
14. 威胁：非预期事件地潜在原因，这些事件可能对系统或组织造成损害。
15. 脆弱性：可能被一个或多个威胁利用的一个或一组资产的弱点。
16. 可能性：对威胁发生几率（Probability）或频率（Frequency）的定性描述
17. 影响：后果（Consequence），意外事件发生给组织带来的直接或间接的损失或伤害。
18. 安全措施：控制措施（control）或对策（countermeasure），即通过防范威胁、减少弱点、限制意外事件带来影响等途径来消减风险的机制、方法和措施。
19. 残留风险：在实施安全措施之后仍然存在的风险。
20. 安全保护能力：系统能够抵御威胁、发现安全事件以及在系统遭到损害后能够恢复先前状态等的程度。
21. 定量风险评估：试图从数字上对安全风险进行分析评估的一种方法。
22. 定性风险评估：凭借分析者的经验和直觉，或者业界的标准和惯例，为风险管理诸要素的大小或高低程度定性分级。
23. 等级保护:信息系统安全等级保护是指对信息安全实行等级化保护和等级化管理。
24. COBIT：(Control Objectives for Information and related Technology) 是目前国际上通用的信息系统审计的标准，由信息系统审计与控制协会在1996年公布。这是一个在国际上公认的、权威的安全与信息技术管理和控制的标准，它在商业风险、控制需要和技术问题之间架起了一座桥梁，以满足管理的多方面需要。
25. PDCA:分别为（plan、do、check、action）计划、实施、监控、改进。
26. CIA:分别为（Confidentiality、Integrity、Availability）保密性、完整性、可用性
27. 可用性：确保授权用户在需要时可以访问信息并使用相关信息资产。
28. 完整性：保护信息和信息的处理方法准确而完整。
29. 机密性：确保只有经过授权的人才能访问信息。
30. 业务连续性计划：在业务中断后恢复业务流程所需步骤的计划。
31. CMM:（Capability Maturity Model）是指“能力成熟度模型”，是对于[软件](http://baike.baidu.com/view/37.htm" \t "_blank)组织在定义、实施、度量、控制和改善其[软件过程](http://baike.baidu.com/view/2207.htm" \t "_blank)的实践中各个发展阶段的描述。
32. IT服务管理：是一种以流程为导向、以客户为中心的方法。它通过整合IT服务与企业业务，提高了企业的IT服务提供和服务支持的能力和水平。
33. ITIL:一套详细描述最佳IT服务管理的丛书，信息服务管理实施上的业界标准，可简单概括为六大模块、十个流程。
34. 降低风险：实施有效控制，将风险降低到可接受的程度，实际上就是力图减小威胁发生的可能性和带来的影响。
35. 规避风险（Avoid Risk）： 或者Rejecting Risk。有时候，组织可以选择放弃某些可能引来风险的业务或资产，以此规避风险。例如，将重要的计算机系统与互联网隔离，使其免遭来自外部网络的攻击。
36. 转嫁风险（Transfer Risk）：也称作Risk Assignment。将风险全部或者部分地转移到其他责任方，例如购买商业保险。
37. 接受风险（Accept Risk）： 在实施了其他风险应对措施之后，对于残留的风险，组织可以选择接受，即所谓的无作为。
38. 审核：为获得审核证据并对体系进行客观评价，以确定满足审核准则的程度所进行的系统的、独立的并形成文件的检查过程。
39. PCI-DSS: (Payment Card Industry (PCI) Data Security Standard), 第三方支付行业(支付卡行业PCI)数据安全标准，PCI DSS对于支付网关的安全方面作出标准的要求，其中包括安全管理、策略、过程、网络体系结构、软件设计的要求的列表等，全面保障交易安全。
40. 数据资产：存在于电子媒介中的各种数据和资料，包括源代码、数据文件、系统文件 等，也包括文档文件例如合同、策略方针、企业文件、重要商业结果。
41. 软件资产：应用软件，系统软件，开发工具，公用程序
42. 实物资产：计算机和通信设备，磁介质，电源和空调等技术性设备，家具，场所
43. 人员资产：承担特定职能和责任的人员
44. 服务资产：计算和通信服务，其他技术性服务， 例如供暖、照明、水电、UPS等
45. 组织形象与声誉：企业形象，客户关系等，属于无形资产
46. ISO27001认证过程