ISO 17799 2005	COBIT 4.1	Sarbanes Oxley COSO	HIPAA Requirements	GLBA
Section: 4 Risk Assessment and Treatment				
4.1 **Assessing Security Risks** Identify, quantify, and prioritize risks against criteria for risk acceptance relevant to the organization	**Plan and Organize:** - PO9 Assess and Manage IT Risks **Monitor and Evaluate:** - ME3 Ensure Regulatory Compliance - ME4 Provide IT Governance	- Risk Assessment - Objective Setting - Event Identification	**Security Standard:** a) 1. Risk Analysis (R)	II.B. Assess Risk
4.2 **Treating Security Risks** Determine risk treatment options: Apply appropriate controls, accept risks, avoid risks or transfer risk to other parties	**Plan and Organize:** - PO9 Assess and Manage IT Risks **Monitor and Evaluate:** - ME1 Monitor and Evaluate IT Performance - ME2 Monitor and Evaluate Internal Control	- Risk Response - Event Identification	**Security Standard:** a) 1. Risk Management (R)	II.C. Manage and Control Risk
Section: 5 Security Policy				
5.1 **Information Security Policy** An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties. The information security policy should be reviewed at planned intervals	**Plan and Organize:** - PO1 Define a Strategic IT Plan - PO4 Define the IT Processes, Organization and Relationships - PO6 Communicate Management Aims and Direction - PO7 Manage IT Human Resources	- Internal Environment - Objective Setting - Risk Assessment	**Security Standard:** a) 1. Sanction Policy (R) a) 2. Assigned Security Responsibility (R)	II.A. Information Security Program II.B. Objectives II.A. Invoice Board of Directors
Section: 6 Organization of Information Security				
6.1 **Internal Organization** A management framework should be established to initiate and control the implementation of information security within the organization	**Deliver and Support:** - DS5 Ensure Systems Security	- Internal Environment - Control Activities - Information and Communication	**Security Standard:** a) 1. Information System Activity Review (R) a) 2. Assigned Security Responsibility (R)	II.A. Information Security Program II.B. Objectives II.A. Involve Board of Directors II.C. Manage and Control Risk II.F. Report to the Board
6.2 **External Parties** To maintain the security of information and information processing facilities that are accessed, processed, communicated to, or managed by external parties	**Plan and Organize:** - PO8 Manage Quality **Deliver and Support:** - DS1 Define and Manage Service Levels - DS2 Manage Third-Party Services - DS5 Ensure Systems Security	- Internal Environment - Risk Assessment - Control Activities - Information and Communication - Monitoring	**Security Standard:** b) 1. Written Contract or Other Arrangement (R)	II.C. Manage and Control Risk II.D.Oversee Service Provider Arrangements
Section: 7 Asset Management				
7.1 **Responsibility for Assets** All assets should be accounted for and have a nominated owner	**Plan and Organize:** - PO4 Define the IT Processes, Organization and Relationships	- Control Activities	**Physical Standard:** d) 2. Device and Media Controls - Accountability (A)	N/A
7.2 **Information Classification** Information should be classified to indicate the need, priorities and expected degree of protection	**Plan and Organize:** - PO2 Define the Information Architecture - PO9 Assess and Manage IT Risks **Deliver and Support:** - DS5 Ensure Systems Security	- Risk Assessment - Event Identification	**Security Standard:** a) 1. Risk Analysis (R) a) 1. Risk Management (R)	N/A
Section: 8 Human Resources Security				
8.1 **Prior to Employment** To ensure that employees, contractors, and third party users understand responsibilities, and are suitable for their roles	**Plan and Organize:** - PO7 Manage IT Human Resources **Deliver and Support:** - DS12 Manage the Physical Environment	- Internal Environment - Control Activities - Information and Communication	**Security Standard:** a) 1. Sanction Policy (R) a) 3. Authorization and/or Supervision (A) a) 3. Workforce Clearance Procedure (A) a) 5. Security Reminders (A)	II.C. Manage and Control Risk
8.2 **During Employment** To ensure that employees, contractors and third party users are aware of information security threats and concerns, and are equipped to support security policy in the course of their normal work	**Plan and Organize:** - PO7 Manage IT Human Resources **Deliver and Support:** - DS7 Educate and Train Users	- Internal Environment - Control Activities - Information and Communication	**Security Standard:** a) 5. Security Reminders (A)	II.C. Manage and Control Risk
8.3 **Termination or Change of Employment** To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner	**Plan and Organize:** - PO4 Define the IT Processes, Organization and Relationships - PO7 Manage IT Human Resources	N/A	**Security Standard:** a) 3. Termination Procedures (A)	N/A
Section: 9 Physical and Environmental Security				