ISO 17799 2005	COBIT 4.1	Sarbanes Oxley COSO	HIPAA Requirements	GLBA
Section: 4 Risk Assessment and Tr	eatment	· · · · · ·		
1.1	Plan and Organize:	- Risk Assessment	Security Standard:	ILB, Assess Risk
	- PO9 Assess and Manage IT Risks	- Objective Setting		ILD. Assess Plan
Assessing Security Risks	- PU9 Assess and Manage II HISKS	- Event Identification	a) 1. Risk Analysis (R)	
dentify, quantify, and prioritize risks against criteria		- Event delibilitation		
or risk acceptance relevant to the organization	Monitor and Evaluate:			
	- ME3 Ensure Regulatory Compliance			1
	- ME4 Provide IT Governance			
4.2	Plan and Organize:	- Risk Response	Security Standard:	ILC. Manage and Control Risk
Treating Security Risks	- PO9 Assess and Manage IT Risks	- Event Identification	a) 1. Risk Management (R)	
Determine risk treatment options: Apply appropriate			1	
controls, accept risks, avoid risks or transfer risk to	Monitor and Evaluate:			
other parties	- ME1 Monitor and Evaluate IT Performance			
ostor parties	- ME2 Monitor and Evaluate Internal Control			
Section: 5 Security Policy	- MEZ MONIOr and Evaluate Internal Control			
	Terror and terror		I	Territoria
5.1	Plan and Organize:	- Internal Environment	Security Standard:	I.A. Information Security Program
nformation Security Policy	- PO1 Define a Strategic IT Plan	- Objective Setting	a) 1. Sanction Policy (R)	I.B. Objectives
An information security policy document should be	- PO4 Define the IT Processes, Organization and	- Risk Assessment	a) 2. Assigned Security Responsibility (R)	ILA. Invoice Board of Directors
approved by management, and published and	Relationships			1
communicated to all employees and relevant	- PO6 Communicate Management Aims and Direction			
external parties. The information security policy	- PO7 Manage IT Human Resources			
should be reviewed at planned intervals				
and the same of th				
Cti C	- Cit			
Section: 6 Organization of Informat				
6.1	Deliver and Support:	- Internal Environment	Security Standard:	I.A. Information Security Program
Internal Organization	- DS5 Ensure Systems Security	- Control Activities	a) 1. Information System Activity Review (R)	I.B. Objectives
A management framework should be established to		- Information and Communication	a) 2. Assigned Security Responsibility (R)	II.A. Involve Board of Directors
initiate and control the implementation of information				ILC. Manage and Control Risk
security within the organization				ILF. Report to the Board
6.2	Discouration of the second	- Internal Environment	0	ILC, Manage and Control Risk
	Plan and Organize:	- Risk Assessment	Security Standard:	ILD. Oversee Service Provider
External Parties	- POB Manage Quality	- Fisk Assessment - Control Activities	b) 1. Written Contract or Other Arrangement (R)	Arrangements
To maintain the security of information and		- Information and Communication		Arrangements
information processing facilities that are accessed,	Deliver and Support:	- Monitoring		
processed, communicated to, or managed by	- DS1 Define and Manage Service Levels	- Monitoring		1
external parties	- DS2 Manage Third-Party Services			
	- DS5 Ensure Systems Security			
Section: 7 Asset Management				
- · ·	Plan and Organize:	- Control Activities	Physical Standard:	N/A
			d) 2. Device and Media Controls - Accountability (A)	
7.1	DOAD-1 II- IT D		u) z. Device and media doninois - Accountability (A)	
Responsibility for Assets	- PO4 Define the IT Processes, Organization and			
Responsibility for Assets All assets should be accounted for and have a	- PO4 Define the IT Processes, Organization and Relationships			
Responsibility for Assets All assets should be accounted for and have a nominated owner	Relationships			
Responsibility for Assets All assets should be accounted for and have a		- Risk Assessment	Security Standard:	N/A
Responsibility for Assets All assets should be accounted for and have a nominated owner	Relationships	- Risk Assessment - Event Identification	Security Standard: a) 1. Risk Analysis (R)	N/A
Responsibility for Assets All assets should be accounted for and have a nonimaled owner 7.2 Information Classification	Relationships Plan and Organize:			N/A
Responsibility for Assets All assets should be accounted for and have a norminated owner 7.2 Information Classification Information should be classified to indicate the need,	Relationships Plan and Organize: - PO2 Define the Information Architecture		a) 1. Risk Analysis (R)	N/A
Responsibility for Assets All assets should be accounted for and have a norminated owner 7.2 Information Classification Information should be classified to indicate the need,	Plan and Organize: - POZ Define the Information Architecture - PO9 Assess and Manage IT Risks		a) 1. Risk Analysis (R)	N/A
Responsibility for Assets 41 assets should be accounted for and have a rominated owner 7. Information Classification rformation should be classified to indicate the need,	Pelationahips Plan and Organize: - POZ Define the information Architecture - PO9 Assess and Manage IT Risks Deliver and Support:		a) 1. Risk Analysis (R)	N/A
Responsibility for Assets Al assets should be accounted for and have a nonmated owner 7.2 information Classification information Classification information classified to indicate the need, priorities and expected degree of protection	Pelationahips Plan and Organize: - PCQ Define the information Architecture - PO9 Assess and Manage IT Risks Deliver and Support: - ISSS Ensure Systems Security		a) 1. Risk Analysis (R)	N/A
Responsibility for Assets At assets about be accounted for and have a command dense 7.2 Information Classification information should be classified to indicate the need, priorities and expected degree of protection Section: 8 Human Resources Secur	Plan and Organize: - POZ Defins the information Architecture - POZ Defins the information Architecture - POZ Resease and Marriage IT Risks Deliver and Support: - USS Ensure Systems Security Type Ty	- Event Identification	a) 1. Risk Analysis (R) a) 1. Risk Management (R)	
Responsibility for Assets of assets about be accounted for and have a command center 7.2 from mormation Classification reformation classification reformation should be classified to indicate the need, increase and expected degree of protection Section: 8 Human Resources Secur	Plan and Organize: - PCC Dates the Information Architecture - PCO Assess and Marriage IT Risks Deliver and Support: - DSS Ensure Systems Security Ly Plan and Organize:	- Event Identification	a) 1. Risk Analysis (R) a) 1. Risk Management (R) Security Standard:	N/A ILC. Manage and Control Risk
Responsibility for Assets All assets shoulds be accounted for and have a mornisate owner 7.2 Information Classification for induction inducts the need, promotes and expected degree of protection Section: 8 Human Resources Secur 8.1	Plan and Organize: - POZ Defins the information Architecture - POZ Defins the information Architecture - POZ Resease and Marriage IT Risks Deliver and Support: - USS Ensure Systems Security Type Ty	- Event Identification - Internal Environment - Control Activities	a) 1. Risk Analysis (R) a) 1. Risk Management (R) Security Standard: a) 1. Sanction Polcy (R)	
Responsibility for Assets All assets about be accounted for and have a command owner 7.2 Information Classification information should be classified to indicate the need, promises and expected degree of protection Section: 8 Human Resources Secur 8.1 Prior to Employment	Plan and Organize: - PCC Dates the Information Architecture - PCO Assess and Marriage IT Risks Deliver and Support: - DSS Ensure Systems Security Ly Plan and Organize:	- Event Identification	a) 1. Risk Analysis (R) a) 1. Risk Management (R) Security Standard:	
Responsibility for Assets All assets shoulds excounted for and have a nonmand coner 12 Information Classification retromation should be classified to indicate the need, promotes and expected degree of protection Section: 8 Human Resources Secur 8.1 Prior to Employment 1 on source that employees, contractors, and third resources and remojoves, contractors, and third	Plan and Organize: - PCC Dates the Information Architecture - PCO Assess and Marriage IT Risks Deliver and Support: - DSS Ensure Systems Security Ly Plan and Organize:	- Event Identification - Internal Environment - Control Activities	a) 1. Risk Analysis (R) a) 1. Risk Management (R) Security Standard: a) 1. Sanction Polcy (R)	
Responsibility for Assets All assets about be accounted for and have a command owner 7.2 Information Classification information should be classified to indicate the need, priorities and expected degree of protection Section: 8 Human Resources Secur 8.1 To ensure that employees, contractors, and their to ensure that employees, contractors, and their to ensure that employees, contractors, and their dary users understand responsibilities, and are	Plan and Organize: - POC Burins the information Architecture - POD Assess and Manage IT Risks Deliver and Support: - DOS Exams Systems Security Y Plan and Organize: - POT Manage IT Human Resources Deliver and Support:	- Event Identification - Internal Environment - Control Activities	a) 1. Risk Aralysis (R) a) 1. Risk Management (R) Security Standard: a) 1. Sanction Policy (R) a) 3. Authorization and/or Supervision (A) a) 3. Workforce (Sanance Procedure (A)	
Responsibility for Assets All assets shoulds be accounted for and have a nonmande owner 122 Information Classification Tromation invald be classified to indicate the need, promotes and expected degree of protection Section: 8 Human Resources Secur 8.1 Prior to Employment 10 neares that employees, contractors, and third party users understand responsibilities, and are subtlete for the rice of the section of the security of the security of the section of the security of the s	Palationahips Plan and Organize: -POE Dries the information Anchéedure -POE Assess and Marriage IT Rieks Deliver and Support: -DOE Assess and Marriage IT Rieks Poliver and Organize: -POT Marage IT Human Resources Deliver and Organize: -POT Marage IT Human Resources Deliver and Support: -DOE IZ Marriage the Physical Environment	- Event Identification - Internal Environment - Control Activities - Information and Communication	a) 1. Risk Aralysis (R) a) 1. Risk Management (R) Security Standard: a) 1. Sanction Policy (R) a) 3. Authorization ander Supervision (A) a) 3. Workbore Cleanance Poosudure (A) a) 5. Security Remindes (A)	ILC. Manage and Control Risk
Responsibility for Assets Al assets should be accounted for and have a commanded owner 1.2 1.2 1.2 1.2 1.3 1.2 1.3 1.3 1.3 1.4 1.5 1.5 1.5 1.5 1.5 1.5 1.5 1.5 1.5 1.5	Plan and Organize: - PCQ Define the information Architecture - PCQ Enter and Support: - PCQ Enter and Support: - PCSE Enter Systems Security IV Plan and Organize: - PCV Manage if Human Resources Deliver and Support: - LOSX Manage the Physical Environment Plan and Organize: - PCY Manage in Physical Environment	- Event Identification - Internal Engineerit - Control Adminis - Information and Communication - Internal Engineerit - Internal En	a) 1. Risk Aralysis (R) a) 1. Risk Management (R) Security Standard: a) 1. Sanction Peloy (R) a) 3. Authorization and or Supervision (A) a) 3. Workforce Clearance Procedure (A) a) 5. Security Reminders (A) Security Reminders (A)	
Reponsibility for Assets all assets should be accorded for and have a normated owner. 2 nformation Classification 72 nformation Classification 73 normation Classification 74 normation and be classified to indicate the need, normation and expected degree of protection Section: 8 Human Resources Secur 3.1 7-Prior to Employment 7-In ormate that employees, contractors, and third surphy users understand responsibilities, and are tutted for their owner. 3.2 During Employment	Palationahips Plan and Organize: -POE Dries the information Anchéedure -POE Assess and Marriage IT Rieks Deliver and Support: -DOE Assess and Marriage IT Rieks Poliver and Organize: -POT Marage IT Human Resources Deliver and Organize: -POT Marage IT Human Resources Deliver and Support: -DOE IZ Marriage the Physical Environment	- Event Identification - Internal Environment - Cornio Activities - Information and Communication - Internal Environment - Cornio Activities	a) 1. Risk Aralysis (R) a) 1. Risk Management (R) Security Standard: a) 1. Sanction Policy (R) a) 3. Authorization ander Supervision (A) a) 3. Workbore Cleanance Poosudure (A) a) 5. Security Remindes (A)	ILC, Manage and Control Risk
Responsibility for Assets 1.2 1.2 1.3 1.3 1.4 1.5 1.5 1.5 1.5 1.5 1.5 1.5	Plan and Organize: - PCQ Define the information Architecture - PCQ Enter the information Architecture - PCQ Assess and Marrage IT flisks Deliver and Support: - LOSS Ensure Systems Securely IY Plan and Organize: - PCY Manage IT Human Resources Deliver and Support: - LOS1 Namage IT Human Resources PRI nand Organize: - PCY Manage IT Human Resources	- Event Identification - Internal Engineerit - Control Adminis - Information and Communication - Internal Engineerit - Internal En	a) 1. Risk Aralysis (R) a) 1. Risk Management (R) Security Standard: a) 1. Sanction Peloy (R) a) 3. Authorization and or Supervision (A) a) 3. Workforce Clearance Procedure (A) a) 5. Security Reminders (A) Security Reminders (A)	ILC, Manage and Control Risk
Responsibility for Assets All assets should be accounted for and have a mornisate owner 7.2 Information Classification The accounted for and have a processor of the accounted for any formation and any formation and any formation and any formation and approach and approach and approach and approach and approach and approach and any formation and any for	Palationaripies Plan and Organize: -POE Dates the information Architecture -POE Assess and Marriage IT Risks Deliver and Support: -DOS Assess and Marriage IT Risks Poliver and Organize: -POT Manage IT Human Resources Deliver and Support: -DOS IZ Marriage the Physical Environment Plan and Organize: -POT Wanage IT Human Resources Deliver and Support: -DOS Manage IT Human Resources Deliver and Support:	- Event Identification - Internal Environment - Cornio Activities - Information and Communication - Internal Environment - Cornio Activities	a) 1. Risk Aralysis (R) a) 1. Risk Management (R) Security Standard: a) 1. Sanction Peloy (R) a) 3. Authorization and or Supervision (A) a) 3. Workforce Clearance Procedure (A) a) 5. Security Reminders (A) Security Reminders (A)	ILC. Manage and Control Risk
Responsibility for Assets Al assets should be accounted for and have a command owner 1.2 1.2 1.2 1.3 1.3 1.2 1.4 1.5 1.5 1.5 1.5 1.5 1.5 1.6 1.6 1.6 1.6 1.6 1.6 1.6 1.6 1.6 1.6	Plan and Organize: - PCQ Define the information Architecture - PCQ Enter the information Architecture - PCQ Assess and Marrage IT flisks Deliver and Support: - LOSS Ensure Systems Securely IY Plan and Organize: - PCY Manage IT Human Resources Deliver and Support: - LOS1 Namage IT Human Resources PRI nand Organize: - PCY Manage IT Human Resources	- Event Identification - Internal Environment - Cornio Activities - Information and Communication - Internal Environment - Cornio Activities	a) 1. Risk Aralysis (R) a) 1. Risk Management (R) Security Standard: a) 1. Sanction Peloy (R) a) 3. Authorization and or Supervision (A) a) 3. Workforce Clearance Procedure (A) a) 5. Security Reminders (A) Security Reminders (A)	ILC. Manage and Control Risk
Responsibility for Assets All assets should be accounted for and have a mornisate owner 7.2 Information Classification The accounted for and have a processor of the accounted for any formation and any formation and any formation and any formation and approach and approach and approach and approach and approach and approach and any formation and any for	Palationaripies Plan and Organize: -POE Dates the information Architecture -POE Assess and Marriage IT Risks Deliver and Support: -DOS Assess and Marriage IT Risks Poliver and Organize: -POT Manage IT Human Resources Deliver and Support: -DOS IZ Marriage the Physical Environment Plan and Organize: -POT Wanage IT Human Resources Deliver and Support: -DOS Manage IT Human Resources Deliver and Support:	- Event Identification - Internal Environment - Cornio Activities - Information and Communication - Internal Environment - Cornio Activities	a) 1. Risk Aralysis (R) a) 1. Risk Management (R) Security Standard: a) 1. Sanction Peloy (R) a) 3. Authorization and or Supervision (A) a) 3. Workforce Clearance Procedure (A) a) 5. Security Reminders (A) Security Reminders (A)	ILC, Manage and Control Risk
Responsibility for Assets 1.2 1.2 1.3 1.3 1.4 1.5 1.5 1.5 1.5 1.5 1.5 1.5	Palationaripies Plan and Organize: -POE Dates the information Architecture -POE Assess and Marriage IT Risks Deliver and Support: -DOS Assess and Marriage IT Risks Poliver and Organize: -POT Manage IT Human Resources Deliver and Support: -DOS IZ Marriage the Physical Environment Plan and Organize: -POT Wanage IT Human Resources Deliver and Support: -DOS Manage IT Human Resources Deliver and Support:	- Event Identification - Internal Environment - Cornio Activities - Information and Communication - Internal Environment - Cornio Activities	a) 1. Risk Aralysis (R) a) 1. Risk Management (R) Security Standard: a) 1. Sanction Peloy (R) a) 3. Authorization and or Supervision (A) a) 3. Workforce Clearance Procedure (A) a) 5. Security Reminders (A) Security Reminders (A)	ILC, Manage and Control Risk
Responsibility for Assets 1.2 1.3 1.3 1.4 1.5 1.5 1.5 1.5 1.5 1.5 1.5	Palationaripies Plan and Organize: -POE Dates the information Architecture -POE Assess and Marriage IT Risks Deliver and Support: -DOS Assess and Marriage IT Risks Poliver and Organize: -POT Manage IT Human Resources Deliver and Support: -DOS IZ Marriage the Physical Environment Plan and Organize: -POT Wanage IT Human Resources Deliver and Support: -DOS Manage IT Human Resources Deliver and Support:	- Event Identification - Internal Environment - Cornio Activities - Information and Communication - Internal Environment - Cornio Activities	a) 1. Risk Aralysis (R) a) 1. Risk Management (R) Security Standard: a) 1. Sanction Peloy (R) a) 3. Authorization and or Supervision (A) a) 3. Workforce Clearance Procedure (A) a) 5. Security Reminders (A) Security Reminders (A)	ILC, Manage and Control Risk
Responsibility for Assets a lessed should be accounted for and have a command owner 12 Information Classification To a more and the classification of the common of the common of the classification of the classificati	Plan and Organize: - POS Defins the information Architecture - POS Defines the information Architecture - POS Defines and Martinger IT Maks Deliver and Support: - LOSS Ensume Systems Security Y Plan and Organize: - POT Marage IT Human Resources Deliver and Support: - LOST Stanger IT Human Resources Deliver and Organize: - POT Marage IT Human Resources Deliver and Support: - LOST Defines IT Human Resources Deliver and Support: - LOST Educate and Train Users Plan and Organize:	- Event Identification - Internal Environment - Control Adminis - Information and Communication - Internal Environment - Control Adminis - Information and Communication - Internal Environment - Information and Communication	a) 1. Risk Management (R) Security Standard: a) 1. Sanction Policy (R) a) 3. Authorization and or Supervision (A) a) 3. Workforce Clearance Procedure (A) a) 3. Workforce Clearance Procedure (A) a) 5. Security Memmides (A) Security Standard: a) 5. Security Permides (A) Security Standard:	BLC. Manage and Control Risk BLC. Manage and Control Risk
Responsibility for Assets 3.1 assets should be accounted for and have a command context. 2.2 information Classification information Classification information should be classified to indicate the need, monitors and expected degree of protection. Section: 8 Human Resources Secur 3.1 Prior to Employment to emane that employees, contractors, and find anyly users understand responsibilities, and are unable to the security of the contractors of the context of the conte	Plan and Organize: - PCQ Define the information Architecture - PCQ Forest and Marrage IT Risks Deliver and Support: - LOSS Ensure Systems Securely IY Plan and Organize: - PCY Manage IT Human Resources Deliver and Support: - LOSI Naturage the Physical Environment Plan and Organize: - PCY Manage IT Human Resources Deliver and Support: - PCY Manage IT Human Resources Deliver and Support: - PCY Manage IT Human Resources Deliver and Organize: - PCY Manage IT Human Resources Deliver and Organize: - PCY Deliver But Train Users	- Event Identification - Internal Environment - Control Adminis - Information and Communication - Internal Environment - Control Adminis - Information and Communication - Internal Environment - Information and Communication	a) 1. Risk Aralysis (R) a) 1. Risk Management (R) Security Standard: a) 1. Sanction Pelory (R) a) 3. Authorization andro Supervision (A) a) 3. Workforce Cleanance Procedure (A) a) 5. Security Perminders (A) Security Standard: a) 5. Security Perminders (A)	BLC. Manage and Control Risk BLC. Manage and Control Risk
Responsibility for Assets all assets shoulds accounted for and have a normalized owner 22 Information Classification 12 Information and the classified in indicate the need, increased and expected degree of protection Section: 8 Human Resources Secur 3.1 Prior to Employment 10 onsure that employees, contractors, and third barry users understand responsibilities, and are understand and expensibilities and fred for name, and are equipped to support security collect in the contraction of the normal work. 3.3 Termination or Change of Employment for nonuse that employees, contractors and find	Plan and Organize: - PO2 Defins the information Architecture - PO2 Defines the information Architecture - PO3 Defines and Martinger IT Maks Deliver and Support: - LOSS Expurise Systems Security Y Plan and Organize: - PO7 Wanage in Human Resources Deliver and Support: - LOS12 Martinger IT Human Resources Deliver and Organize: - POF Undruger IT Human Resources Deliver and Train Users Deliver and Support: - LOST Educate and Train Users Plan and Organize: - PO4 Defines the IT Processes, Organization and Relationships	- Event Identification - Internal Environment - Control Adminis - Information and Communication - Internal Environment - Control Adminis - Information and Communication - Internal Environment - Information and Communication	a) 1. Risk Management (R) Security Standard: a) 1. Sanction Policy (R) a) 3. Authorization and or Supervision (A) a) 3. Workforce Clearance Procedure (A) a) 3. Workforce Clearance Procedure (A) a) 5. Security Memmides (A) Security Standard: a) 5. Security Permides (A) Security Standard:	BLC. Manage and Control Risk BLC. Manage and Control Risk
Responsibility for Assets 3.1 assets should be accounted for and have a command context. 2.2 information Classification information Classification information should be classified to indicate the need, monitors and expected degree of protection. Section: 8 Human Resources Secur 3.1 Prior to Employment to emane that employees, contractors, and find anyly users understand responsibilities, and are unable to the security of the contractors of the context of the conte	Plan and Organize: - PCQ Define the information Architecture - PCQ Forest and Marrage IT Risks Deliver and Support: - LOSS Ensure Systems Securely IY Plan and Organize: - PCY Manage IT Human Resources Deliver and Support: - LOSI Naturage the Physical Environment Plan and Organize: - PCY Manage IT Human Resources Deliver and Support: - PCY Manage IT Human Resources Deliver and Support: - PCY Manage IT Human Resources Deliver and Organize: - PCY Manage IT Human Resources Deliver and Organize: - PCY Deliver But Train Users	- Event Identification - Internal Environment - Control Adminis - Information and Communication - Internal Environment - Control Adminis - Information and Communication - Internal Environment - Information and Communication	a) 1. Risk Management (R) Security Standard: a) 1. Sanction Policy (R) a) 3. Authorization and or Supervision (A) a) 3. Workforce Clearance Procedure (A) a) 3. Workforce Clearance Procedure (A) a) 5. Security Memmides (A) Security Standard: a) 5. Security Permides (A) Security Standard:	BLC. Manage and Control Risk BLC. Manage and Control Risk