

# ABC College High Level IT Security Risk Matrix

© 2007 iSecure Solutions

Information Security Governance & Infrastructure Components

Level Of Risk - Numerical Values			
Description	Color	Value	Risk
relevant or the significance of a control failure is not minimal risk potential	White	0	N/A
or the significance of a control elevated risk potential	Green	1	LOW
or the significance of a control extensive risk potential	Yellow	2	MED
or the implications of a control	Red	3	HIGH

RISK FACTORS		Factor Weight
F1	Customer Information - Confidentiality	0.26
F2	Improper/Incorrect Transactional Data - Integrity	0.16
F3	Infrastructure Stability/ Change Control/ Business Continuity/ Physical - (Availability)	0.11
F4	Alumni/Student Organizational Confidence - Reputation	0.26
F5	Regulatory Compliance - Legal	0.10
F6	Operational Systems Reliance	0.06
F7	Fraud / Data Breach - Financial Loss	0.05

ASSESSMENT AREA	RISK		CONTROL PROCESS	Regulatory Compliance Requirement		Risk Factors							Relative Risk Factor	Risk Factor Avg	High Risk Factor	GLBA Risk Factor	GLBA High Risk Factor
	CATEGORY	FUNCTION		GLBA - FTC Enforcement	State Data Breach Notification Laws	F1	F2	F3	F4	F5	F6	F7					
General Information Security Objectives	Management Oversight & Governance	Information Security Program / Information Security Plan	Development and Management	X		2	0	1	2	3	0	1	1.50	1.338	1.870	3.000	3.000
		Implementation		X		3	0	1	2	3	1	2	1.87			3.000	
		Security Steering Committee	Implementation			2	0	0	2	2	1	0	1.30			2.000	
		Information Security Policies	Development and Management	X	X	1	2	2	2	2	1	2	1.68			2.000	
		Implementation		X	X	1	2	2	2	2	1	2	1.68			2.000	
	Vendor Management	Implementation			X		0	0	0	0	0	0	0.00	0.000			
	Information Security Administrative Controls	Information Security Incident Response Plan	Development and Management	X	X	1	1	2	2	3	0	1	1.51	1.573	2.500	3.000	3.000
		Implementation		X	X	2	1	3	3	3	0	2	2.19			3.000	
		Information Security Risk Assessment	Development and Management	X		0	0	0	0	1	0	0	0.10			1.000	
		Implementation		X		1	0	0	0	1	0	0	0.36			1.000	
		Information Security Awareness, Education and Training Program	Development and Management	X		2	2	0	2	3	1	1	1.77			3.000	
		Implementation		X		3	3	0	3	3	1	2	2.50			3.000	
		Configuration Management	Development and Management	*		2	1	2	1	1	1	1	1.37			2.000	
		Implementation		*		3	2	3	1	2	1	1	2.00			3.000	
	Information Security System Administration	Development and Management	X		2	2	2	1	1	1	2	1.58	2.000				
	Implementation		X		2	2	2	2	2	2	2	2.00	2.000				
	Retention of Data and Output	Development and Management	X		3	0	1	2	2	1	1	1.72	3.000				
	Implementation		X		3	0	1	2	2	1	2	1.77	3.000				
	Information Security Technical Controls	Network Perimeter Security	Implementation	X		2	2	1	2	2	2	2	1.89	0.923	1.890	2.000	2.000
		Virus and Malware Protection	Implementation	*		1	0	2	1	1	1	0				1.000	
		Data Encryption	Implementation	X	X	2	0	0	2	2	0	2	1.34			2.000	
		Monitoring and Logging	Implementation	X		2	1	0	0	1	0	2	0.88			2.000	
		Physical Security / Environmental	Implementation	X		1	0	0	0	1	0	1	0.41			1.000	
		Vulnerability Assessments	Implementation	X		2	0	1	1	1	0	0	0.99			2.000	
		Backup / Recovery	Implementation			1	1	1	1	1	1	0	0.95			1.000	
	Software Development Life Cycle	Application Development	Development and Management			1	1	0	0	0	0	1	0.47	0.523	0.940	1.000	2.000
		Implementation				2	2	0	0	0	0	2	0.94			2.000	
		Commercial Off-The-Shelf (COTS) System Deployment	Development and Management			0	0	0	0	0	0	0	0.00			0.000	
Implementation					1	1	1	0	1	0	1	0.68	1.000				

\* = Although not specifically mentioned as a required control, this controls necessary as per 314.3(b)(2) - Protect against any anticipated threats or hazards to the security and integrity of customer information

### Ratings Factors / Descriptions

No written InfoSec Program

No InfoSec Program implementation process or staff assignments

ITC and Council reporting by IT management

ITC Approval and may ask Council approval as appropriate

Have partial set of InfoSec policies. Must create end user awareness.

It was determined that major applications with GLBA data are not outsourced

Informal, undocumented procedures and email trails.

Informal, undocumented procedures and email trails.

GLBA IT Risk assessment outsourced to external vendor Q2 2006

GLBA IT Risk assessment performed Q4 2006 - Q2-2007 by iSecure

User awareness program planning process started.

No user awareness program currently in place'

Partial implementation of process and procedures.

Partial implementation of process and procedures.

Windows user authentication and access controls

Windows user authentication and access controls implemented

Not Implemented

Not Implemented

Controls implemented and tested

Controls implemented and tested

Minimal implementations

Controls implemented

Controls implemented

External vendor assessments performed

Controls implemented

Control development process begun

Controls not implemented

Control development process begun

Controls not implemented