

Stop, Drop, and Roll: Prevent and Douse Cyber Incidents

Cedric Bennett, Information Security Director
Stanford University (Emeritus)

Susan A. Blair, Privacy Officer
University of Florida

Kathleen Roberts, Principal
iSecure Solutions

October 24, 2007



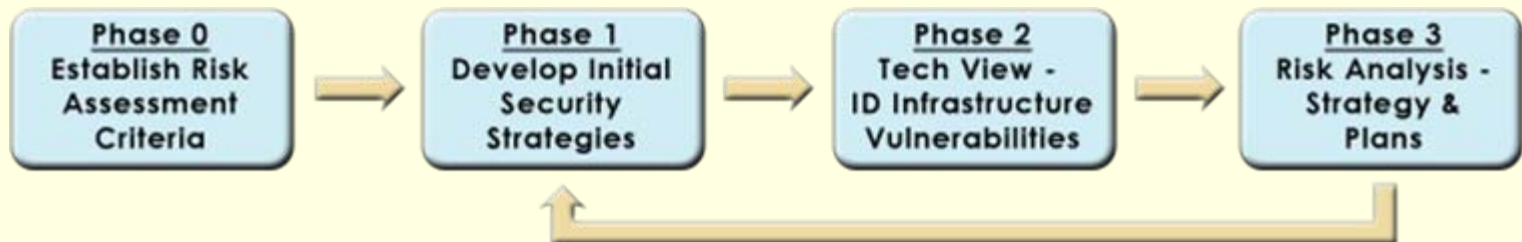
Risk Assessment

...on the ground

Kathleen Roberts

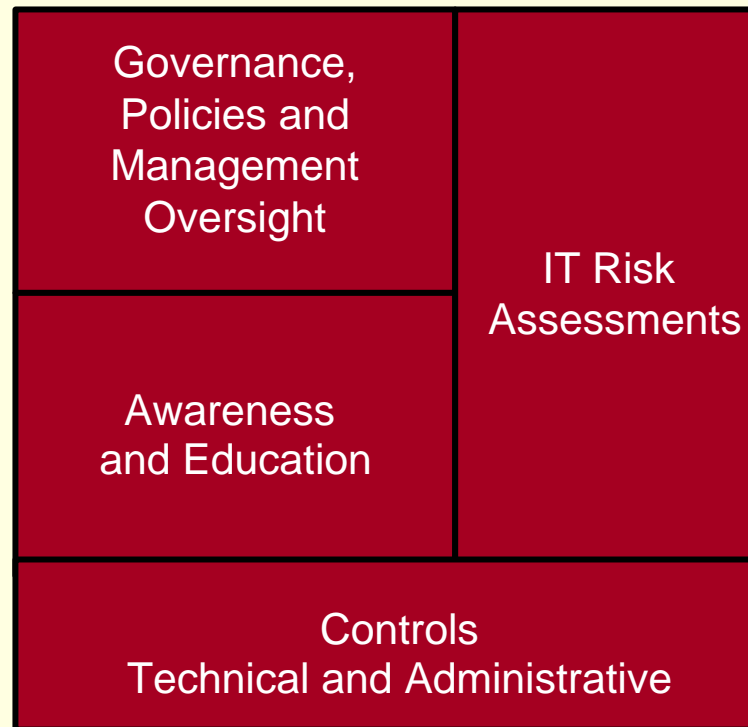
Risk Assessment Framework

- Phase 1 – Phase 2 – Phase 3
 - Have choices
 - May proceed with an institutional application of all phases
 - May focus on one or two specific areas identified by the first phase
 - May skip the rest of the process and begin to apply mitigation programs
 - Downside
 - May not be as complete as following complete process



Security Program Framework

All four components are required by security standards, best practices and regulatory compliance.



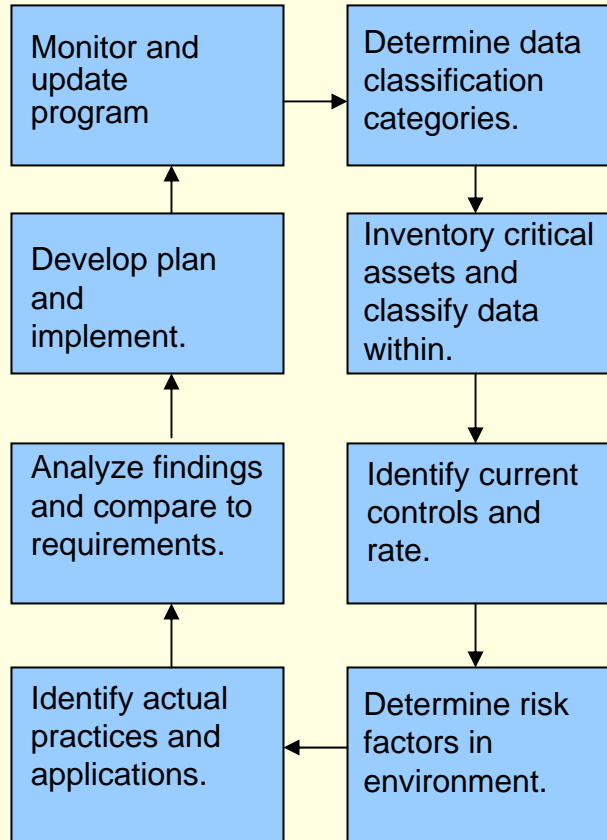
IT Risk Assessment Process

10. Monitor, evaluate and adjust security program every 1-3 years.

9. Implement plan with corrective actions required for compliance and to mitigate risks.

8. Develop remediation plan to address each of the risks uncovered.

7. Compare findings to regulatory and best practice standards. Analyze gaps, create and prioritize recommendations.



6. Identify overall institution and dept. practices and applications using survey tool and interview session.

1. Select appropriate data classification categories.
2. Identify and document critical assets.
3. Classify data within those assets.
4. Identify and inventory current controls in place. Determine implementation stage.
5. Establish initial risk factors for institution. Prioritize and assign weighting.

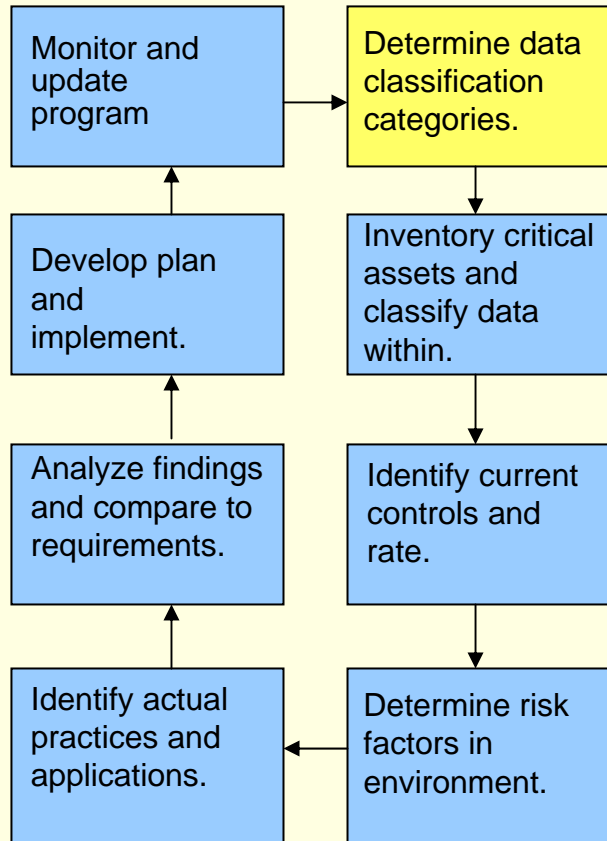
IT Risk Assessment Process

10. Monitor, evaluate and adjust security program every 1-3 years.

9. Implement plan with corrective actions required for compliance and to mitigate risks.

8. Develop remediation plan to address each of the risks uncovered.

7. Compare findings to regulatory and best practice standards. Analyze gaps, create and prioritize recommendations.



1. Select appropriate data classification categories.

2. Identify and document critical assets.

3. Classify data within those assets.

4. Identify and inventory current controls in place. Determine implementation stage.

5. Establish initial risk factors for institution. Prioritize and assign weighting.

6. Identify overall institution and dept. practices and applications using survey tool and interview session.

Step 1: Select Data Classification Categories

Categories Criteria	Most Critical / Restricted <i>Highest Sensitivity</i>	Critical / Sensitive <i>Moderate Sensitivity</i>	Least Critical / Public <i>Lowest Sensitivity</i>
Legal Requirements	Protection of data is required by law	Contractual obligation to protect the data	None
Reputational Risk	High	Medium	Low
Other Institutional Risks	Information that provides access to physical or virtual resources	Smaller subsets of "Most Critical" data perhaps at a dept level	None
Examples of Data	<ul style="list-style-type: none"> ■ Non Public Personal Information which includes SSN, credit card, financial account info, medical info, etc. of students, donors, alumni ■ Password Files, Building-Key Information, Physical Plant Details ■ Proprietary Management Information ■ Confidential Research Information 	<ul style="list-style-type: none"> ■ Information that is not Most Critical ■ Research details that are not Most Critical ■ Financial transactions that are not Most Critical 	<ul style="list-style-type: none"> ■ Campus directory ■ Campus maps ■ Institutional public data

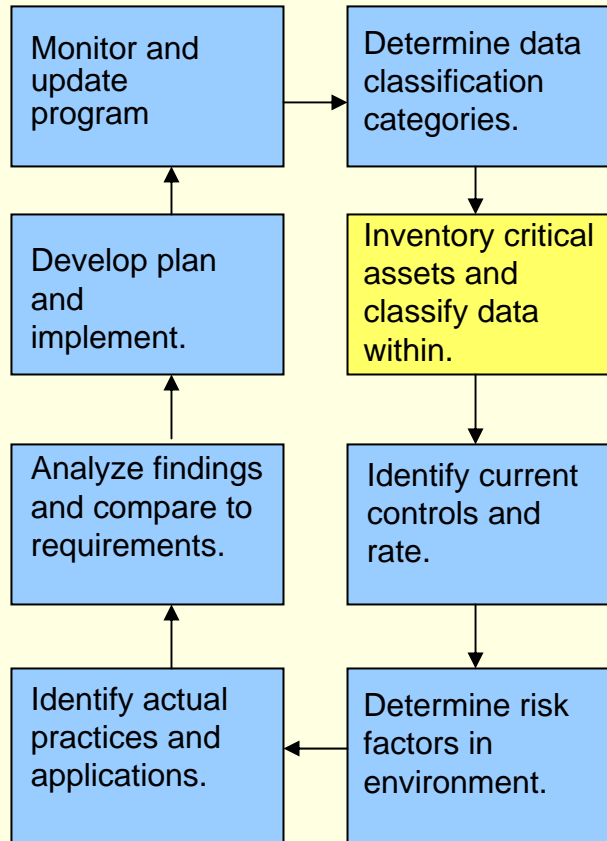
IT Risk Assessment Process

10. Monitor, evaluate and adjust security program every 1-3 years.

9. Implement plan with corrective actions required for compliance and to mitigate risks.

8. Develop remediation plan to address each of the risks uncovered.

7. Compare findings to regulatory and best practice standards. Analyze gaps, create and prioritize recommendations.



6. Identify overall institution and dept. practices and applications using survey tool and interview session.

1. Select appropriate data classification categories.

2. Identify and document critical assets.

3. Classify data within those assets.

4. Identify and inventory current controls in place. Determine implementation stage.

5. Establish initial risk factors for institution. Prioritize and assign weighting.

Step 2 & 3: Critical Asset Inventory

Critical Function	App Name	Data Class Category	Elements (Data Categories)	App Systems	Hardware	Dept.	Info Users	Critical Knowledge
Financial Aid	FinAid	Restricted	Name, Address, SSN, Salary, Tax	Fin Svrs	HP /Linux	Fin. Aid, Admissions, Bus. Office	Individuals	Individuals
Donors	AlumFin Plan	Restricted	Name, Address, SSN, Bank Account #,	App Svrs	HP /Unix	Development, Bus. Office	Individuals	Individuals
Student Records	Central-Grades	Restricted	Student Name, ID, SSN, Grades	Central Grading Svrs	HP	Registrar	Individuals	Individuals
Human Resources Employee Info	HRSys	Restricted	Name, Employee ID, SSN, Salary, Appraisal Rating	HR Svrs	Sun	HR	Individuals	Individuals

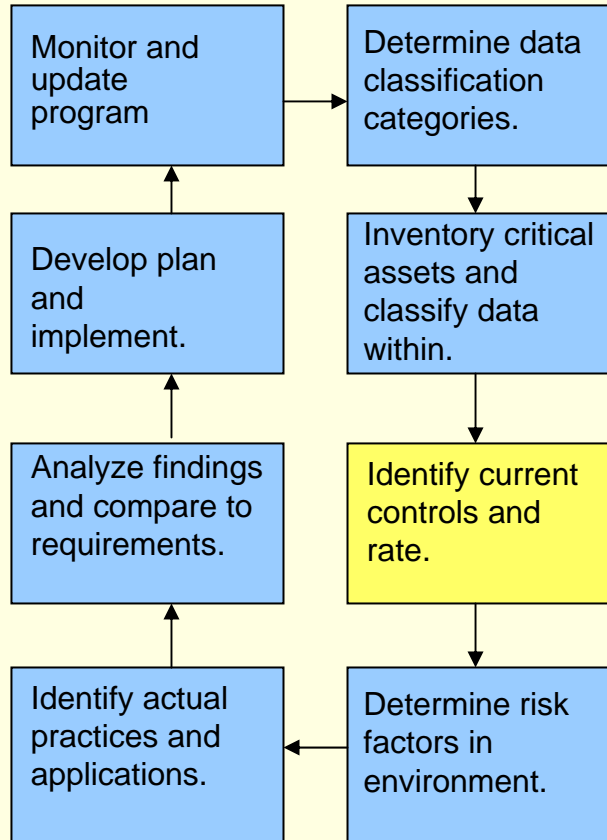
IT Risk Assessment Process

10. Monitor, evaluate and adjust security program every 1-3 years.

9. Implement plan with corrective actions required for compliance and to mitigate risks.

8. Develop remediation plan to address each of the risks uncovered.

7. Compare findings to regulatory and best practice standards. Analyze gaps, create and prioritize recommendations.



6. Identify overall institution and dept. practices and applications using survey tool and interview session.

1. Select appropriate data classification categories.

2. Identify and document critical assets.

3. Classify data within those assets.

4. Identify and inventory current controls in place. Determine implementation stage.

5. Establish initial risk factors for institution. Prioritize and assign weighting.

Step 4: Inventory Safeguards and Determine Effectiveness Level

Risk Area (as defined by Standard)	Functional Area	Control Area	Control Objectives (Admin, Technical)	Gap	Design	Implement	Test
Information Security Governance	Policies and Procedures	Create / Implement / Approval /	Written Information Security Policy Exists, etc.			X X X	
Information Security	Operations	Develop / Implement / Monitor	Procedures to ensure timely maintenance of user accts.	X	X X		
Information Security	CSIRT	Develop / Implement	Create Security Incident Response Plan	X X			
Information Security	CSIRT	Manage Notification & Escalation	Develop Notification Plan	X X			

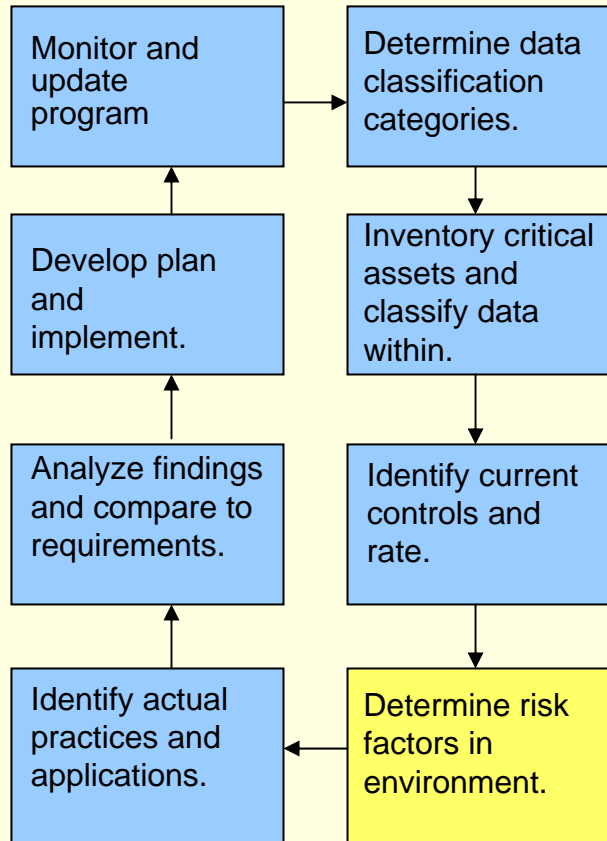
IT Risk Assessment Process

10. Monitor, evaluate and adjust security program every 1-3 years.

9. Implement plan with corrective actions required for compliance and to mitigate risks.

8. Develop remediation plan to address each of the risks uncovered.

7. Compare findings to regulatory and best practice standards. Analyze gaps, create and prioritize recommendations.



6. Identify overall institution and dept. practices and applications using survey tool and interview session.

1. Select appropriate data classification categories.

2. Identify and document critical assets.

3. Classify data within those assets.

4. Identify and inventory current controls in place. Determine implementation stage.

5. Establish initial risk factors for institution. Prioritize and assign weighting.

Step 5: Create Initial Risk Factors

	<i>Risk Factors</i>
F1	Customer Information - Confidentiality
F2	Improper or Incorrect Transaction Data - Integrity
F3	Infrastructure Stability / Change Control / Business Continuity / Physical - Availability
F4	Donors / Alumni / Students - Reputation
F5	Regulatory Compliance - Legal
F6	Fraud / Data Breach / Financial Loss

Step 5: Prioritize Risks Using Weightings

	<i>Risk Factors</i>	<i>Weighting</i>
F1	Customer Information - Confidentiality	0.25
F2	Improper or Incorrect Transaction Data - Integrity	0.10
F3	Infrastructure Stability / Change Control / Business Continuity / Physical - Availability	0.20
F4	Donors / Alumni / Students - Reputation	0.25
F5	Regulatory Compliance - Legal	0.10
F6	Fraud / Data Breach / Financial Loss	0.10

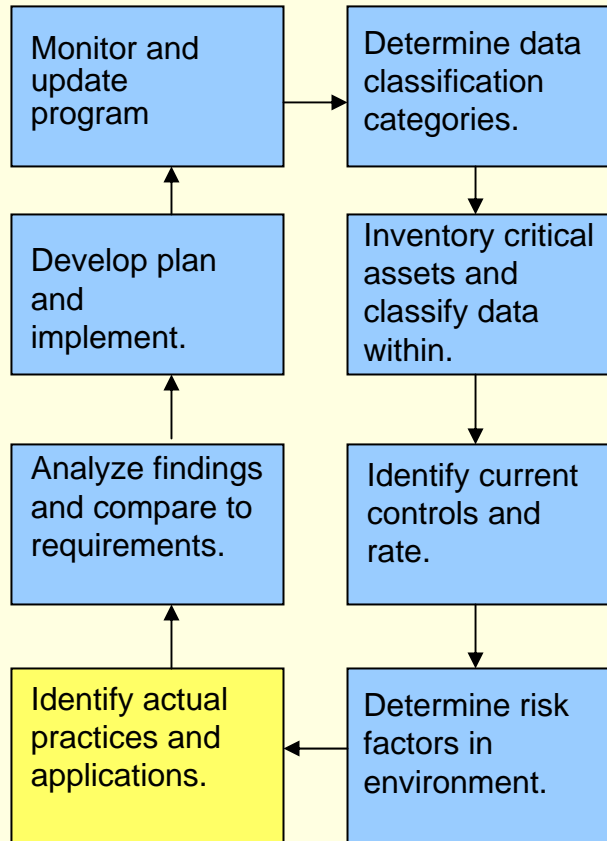
IT Risk Assessment Process

10. Monitor, evaluate and adjust security program every 1-3 years.

9. Implement plan with corrective actions required for compliance and to mitigate risks.

8. Develop remediation plan to address each of the risks uncovered.

7. Compare findings to regulatory and best practice standards. Analyze gaps, create and prioritize recommendations.



6. Identify overall institution and dept. practices and applications using survey tool and interview session.

1. Select appropriate data classification categories.

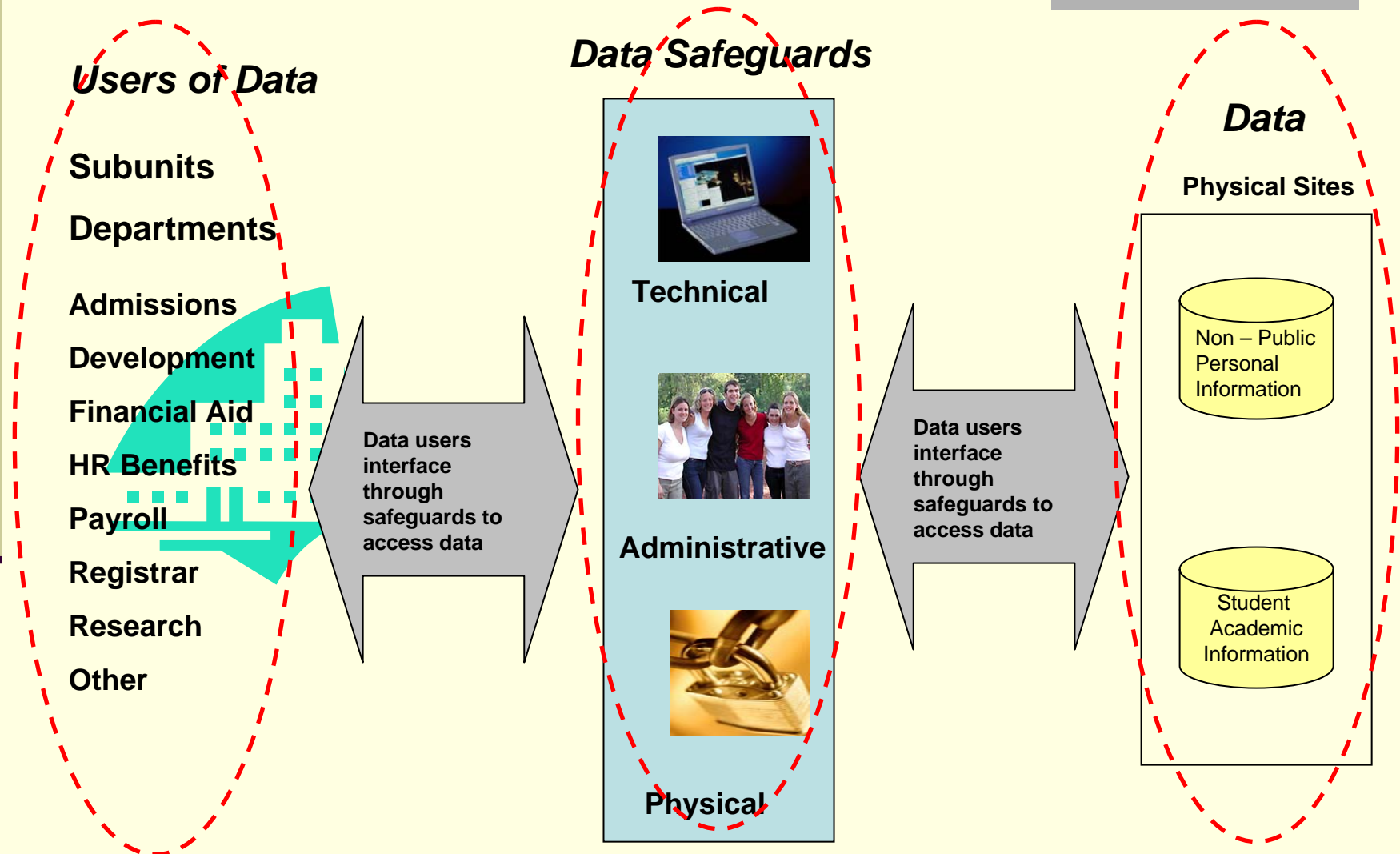
2. Identify and document critical assets.

3. Classify data within those assets.

4. Identify and inventory current controls in place. Determine implementation stage.

5. Establish initial risk factors for institution. Prioritize and assign weighting.

Step 6: Conduct Risk Assessment Interview Session with Selected Departments



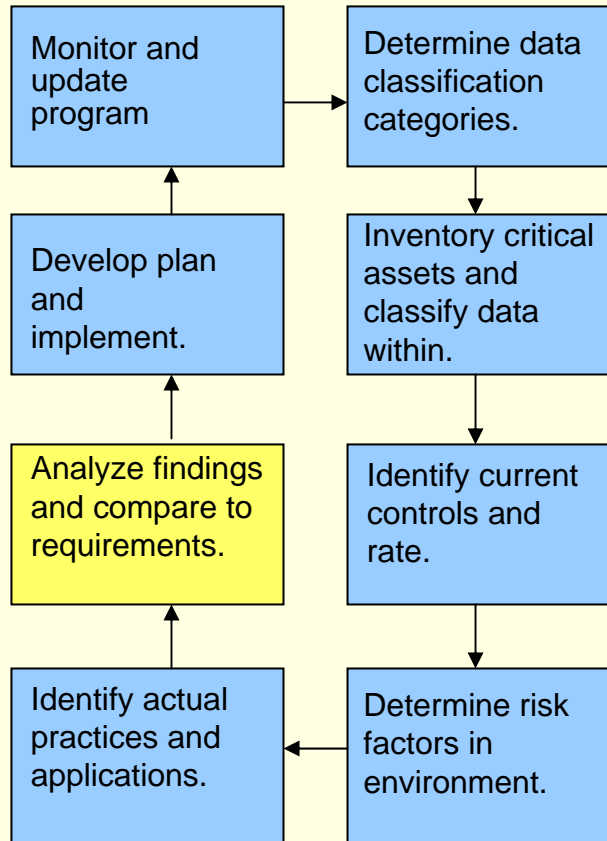
IT Risk Assessment Process

10. Monitor, evaluate and adjust security program every 1-3 years.

9. Implement plan with corrective actions required for compliance and to mitigate risks.

8. Develop remediation plan to address each of the risks uncovered.

7. Compare findings to regulatory and best practice standards. Analyze gaps, create and prioritize recommendations.



6. Identify overall institution and dept. practices and applications using survey tool and interview session.

1. Select appropriate data classification categories.

2. Identify and document critical assets.

3. Classify data within those assets.

4. Identify and inventory current controls in place. Determine implementation stage.

5. Establish initial risk factors for institution. Prioritize and assign weighting.

Step 7: Analyze Findings, Conduct Analysis and Determine Gaps

Level Of Risk - Numerical Values			
	<u>Color</u>	<u>Range</u>	<u>Risk</u>
Level 0 - Functional control area is not relevant or the significance of a control failure is not relevant	White	0	N/A
Level 1 - Functional control area poses a minimal risk potential or the significance of a control failure is minor	Green	1	LOW
Level 2 - Functional control area poses an elevated risk potential or the significance of a control failure is considerable	Yellow	2	MED
Level 3 - Functional control area poses an extensive risk potential or the implications of a control failure are severe.	Red	3	HIGH

Step 7: Analyze Findings, Conduct Analysis and Determine Gaps

Risk Category	Risk Functional Area	Control Process Area	Regulatory Requirement and Standards	Risk Factors F1 to F8	Relative Risk Factors	Aver. Risk Factors	High Risk Factor
Mgmt Oversight & Governance	Info Security Program / Plan	Development and Mgmt / Implement	GLBA / HIPAA / ISO 17799	0-1-2-3 times weight	0 – 3.0	Math. Average	High Score for Category
Mgmt Oversight & Governance	Security Steering Committee	Implement	GLBA / HIPAA / ISO 17799	0-1-2-3 times weight	0 – 3.0	Math. Average	High Score for Category
Mgmt Oversight & Governance	Info Security Policies	Development and Mgmt / Implement	GLBA / HIPAA / ISO 17799	0-1-2-3 times weight	0 – 3.0	Math. Average	High Score for Category
Information Security Admin Controls	Info Security Incident Response Plan	Development and Mgmt / Implement	GLBA / HIPAA / ISO 17799	0-1-2-3 times weight	0 – 3.0	Math. Average	High Score for Category

Step 7: Analyze Findings, Conduct Analysis and Determine Gaps

ABC College High Level IT Security Risk Matrix
Information Security Governance & Infrastructure Components

Level Of Risk - Numerical Values				
	Description	Color	Value	Risk
Level 0	Control area is not relevant	White	0	N/A
Level 1	Control area poses a minimal risk potential	Green	1	LOW
Level 2	Control area poses an elevated risk potential	Yellow	2	MED
Level 3	Control area poses an extensive risk potential	Red	3	HIGH

RISK FACTORS		Factor Weight
F1	Customer Information - Confidentiality	0.20
F2	Improper/incorrect Transactional Data - Integrity	0.15
F3	Infrastructure Stability/ Change Control/ Business Continuity/ Physical - (Availability)	0.10
F4	Alumni/Student Organizational Confidence and Reputation	0.25
F6	Regulatory Compliance - Legal	0.10
F8	Operational Systems Reliance and Capability	0.15
F7	Fraud / Data Breach - Financial Loss	0.05

ASSESS- MENT AREA	RISK		CONTROL PROCESS	Regulatory Compliance Requirement		Risk Factors							Relative Risk Factor	Risk Factor Avg	High Risk Factor
	CATEGORY	FUNCTION		GLBA - FTC Enforcement	ISO 17799	F1	F2	F3	F4	F5	F6	F7			
Management Oversight & Governance	Information Security Program / Information Security Plan	Development and Management	X		2	0	1	2	3	0	1	1.35	1.276	1.750	
		Implementation	X		3	0	1	2	3	1	2	1.75			
	Security Steering Committee	Implementation			2	0	0	2	2	1	0	1.25			
	Information Security Policies	Development and Management	X	X	1	2	2	2	2	1	2	1.85			
		Implementation	X	X	1	2	2	2	2	1	2	1.85			
Vendor Management	Implementation	X		0	0	0	0	0	0	0	0.00				
	Information Security Incident Response Plan	Development and Management	X	X	1	1	2	2	3	0	1	1.40			
		Implementation	X	X	2	1	3	3	3	0	2	2.00			

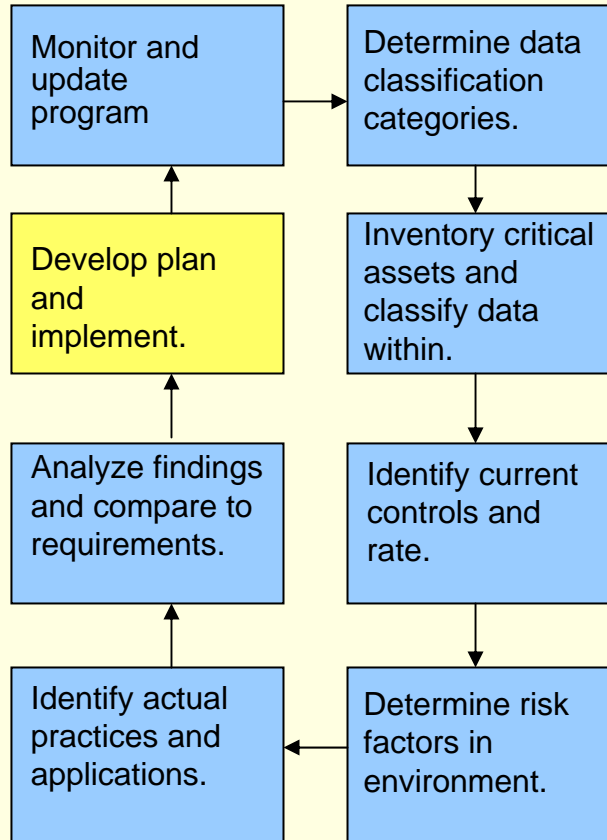
IT Risk Assessment Process

10. Monitor, evaluate and adjust security program every 1-3 years.

9. Implement plan with corrective actions required for compliance and to mitigate risks.

8. Develop remediation plan to address each of the risks uncovered.

7. Compare findings to regulatory and best practice standards. Analyze gaps, create and prioritize recommendations.



6. Identify overall institution and dept. practices and applications using survey tool and interview session.

1. Select appropriate data classification categories.
2. Identify and document critical assets.
3. Classify data within those assets.
4. Identify and inventory current controls in place. Determine implementation stage.
5. Establish initial risk factors for institution. Prioritize and assign weighting.

Sample Customized Scorecard

Rule No.	Type	IT Risk Assessment Selected Controls	Rating
1	Governance	Information Security Plan	Adequate
2		Security Program Monitoring and Adjustments	Not Adequate
3		Safeguards Coordinator	Adequate
4		Periodic Risk Assessments	Adequate
5		Information Security Training and Awareness	Adequate
7		Administrative, Technical and Physical Control Implementation	Not Adequate
8		Third Party Service Providers	Not Conclusive
9		Third Party Service Provider Contract Enforcement of Objectives	Not Conclusive
6	Administrative	Employee Training	Adequate
10		Periodic Update and Testing of Program's Key Controls	Adequate
11		Limit Access Using Segregation of Duties, Dual Controls, Background Checks	Adequate
12		Information Security Incident Response Program	Not Adequate
13	Administrative & Technical	Records & Storage Media Destruction - Policies & Procedures	Not Adequate
14		Access Controls to NPPI Systems	Not Adequate
17		Physical Access Controls to Business Records and Computer Systems with NPPI	Not Conclusive
15	Technical	Monitor Systems and Procedures to Detect Unauthorized Access	Adequate
16		Secure Data Transmission - Encryption	Not Adequate
8 out of 17 = 47% Compliant			

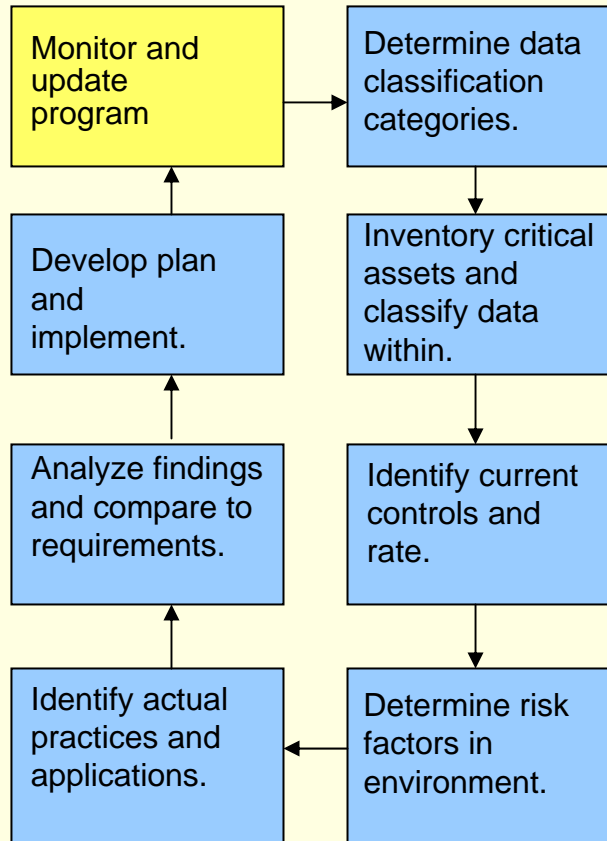
IT Risk Assessment Process

10. Monitor, evaluate and adjust security program every 1-3 years.

9. Implement plan with corrective actions required for compliance and to mitigate risks.

8. Develop remediation plan to address each of the risks uncovered.

7. Compare findings to regulatory and best practice standards. Analyze gaps, create and prioritize recommendations.



6. Identify overall institution and dept. practices and applications using survey tool and interview session.

1. Select appropriate data classification categories.

2. Identify and document critical assets.

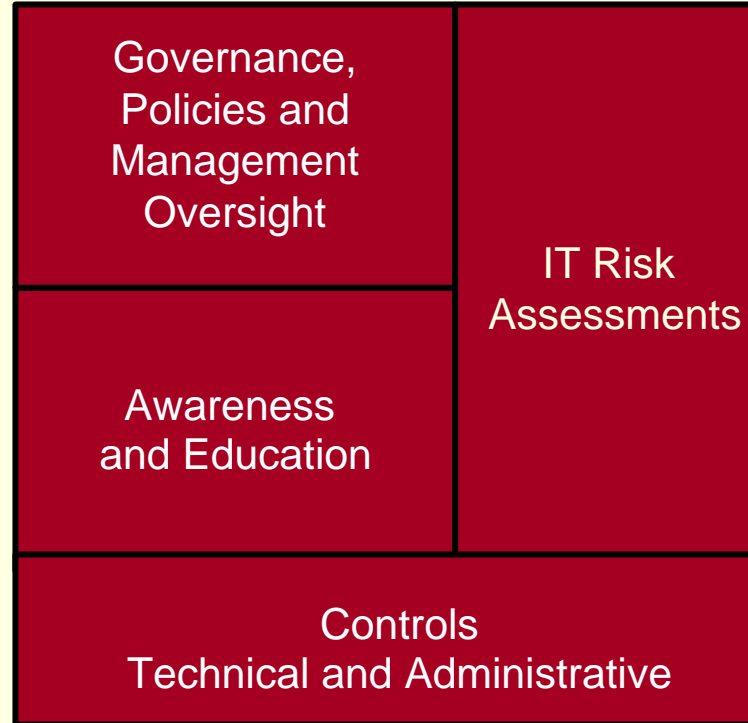
3. Classify data within those assets.

4. Identify and inventory current controls in place. Determine implementation stage.

5. Establish initial risk factors for institution. Prioritize and assign weighting.

Security Program Framework

All four components are required by security standards, best practices and regulatory compliance.



Contact Information

■ Kathleen Roberts

■ Email

- kathleen@isecuresolutions.com

■ Web

- www.isecuresolutions.com

■ Phone

- 215 641-1396 (office)
- 215 353-1902 (cell)