ISAC Information Security Program Prioritization Results - FY11 Q1-Q2

Project Info						Rankings	
Row	Project	Project Description	Institutional Impact	Size	Priority	Score	Rank
1	Annual PII Audit & Review	Via the data steward's conduct scans for Personally Identifiable Information, document results and encrypt personal computers, per the University's PII Policies.	A reduction of PII on workstations, and encryption of PII on workstations reduces the risk of data breaches due to theft or malware.	Large	M	Active	
2	Annual PCI Compliance	Annual compliance with PCI is mandated by industry regulation. Loyola must attest, yearly, that it is compliant against all controls.	Reduces the risk of a data breach of credit card information.	Medium	M	Active	
3	Annual Security Assessment	Annual security assessment against information systems and processes. External vendors will test the security of defined systems to determine if weaknesses exists.	Reduction of overall security risk to the tested systems and processes.	Medium	M	Active	
4	LOCUS Security Audit (Deloitte)	An annual audit of LOCUS account profiles is mandated by the annual Deloitte Financial audit. Review of all business users access to the LOCUS system to ensure that the LOCUS administrative users have appropriate access based on their job function.	This audit will ensure that users do not have more access than is appropriate for their role. Reduces potential data exposure and misuse.	Medium	M	Active	
5	Enterprise Disk Encryption	Implementation and upgrade from existing whole disk encryption solution to an enterprise management solution. This allows ITS administrators enhanced functionality over the encryption product.	Continued risk reduction and information protection of the initial PII program encryption. Additional benefits of improved asset identification and tracking.	Large	A	Active	
6	Protection of Data Exchange	Ensure that confidential data is transmitted according to an established PII policies. Train business users on proper methods for transmitting confidential data and the policies that govern these rules.	By training all end users we can raise the awareness and executing our PII policies. A failure to do this could cause an accidental voluntarily leak of PII during the normal course of business.	Small	A	298	1
7	Online Information Protection	Ensure that online transactions of confidential data are digitally signed and encrypted through any ecommerce systems.	By utilizing digital signatures and encryption a recipient can understand with certainty the source and validity of the data received.	Medium	A	281	2
8	Improved Malware Defenses	Deter the execution of malicious programs from running on the network through the use of policy and technical controls. Regularly monitor for next generation malware and incorporate protections.	Loyola workstations are regularly infected with spyware, trojans and other "data compromising" malware. Lowering the rate of infection would reduce the risk of a breach on the network while also increasing user productivity.	Large	A	279	3
9	Data Leak Prevention	Evaluate and determine how to prevent confidential information from accidentally leaving the organization. Monitor network resources to determine if a potential leak is occurring.	Systems would need to be implemented to scan for sensitive data. This will be centered around Loyola Protected data and the systems that store them. This will reduce the risk of an accidental loss of sensitive data.	Medium	B	266	4
10	Validate Data Input	Create and execute a standard to define the proper 'secure development' practices to protect against known web attacks.	Ensuring all input is 'scrubbed' is a defensive measure to protect a system from behaving in an unexpected manner. This will prevent against popular attacks which can compromise confidential data stored in backend databases.	Small	B	265	5
11	Record Retention	Consolidate existing University record retention policies under a single framework and implement these policies as appropriate throughout the University.	Storage requirements for data are not currently understood University wide. Additionally, these requirements are necessary for certain systems, such as Enterprise Content Management. Protecting our records will reduce the risk of accidental exposure.	Large	B	264	6
12	Network Security Management	Ensure the security of systems and applications on the network and protect against threats. This involves a review of the network security architecture and developing a framework with which to implement future security architecture.	Will harden the network from attack, and thus reduce the risk of systems connected to the network.	X-Large	B	261	7
13	Information Security Awareness	Define a formal security awareness program that will educate the university on appropriate security topics, such as policies and procedures. This will include regulatory requirements, proper use of systems and the method for engaging the UISO to report items of suspect.	In order for policies to be effective all employees must understand the policies and their responsibilities. Additionally, all employees will understand how and when to contact the UISO to report suspicious activity.	Large	B	258	8

ISAC Information Security Program Prioritization Results - FY11 Q1-Q2

Project Info						Rankings	
Row	**Project**	**Project Description**	**Institutional Impact**	**Size**	**Priority**	**Score**	**Rank**
14	Information Security Responsibilities	Define the responsibilities relating to information security roles. This does not only pertain to the UISO, but also to the day to day management of our assets. This should be defined within the information security policy. Communicate this authority throughout the University in order to raise awareness.	Without a clear delineation of roles and responsibilities it is possible that security incidents might not be appropriately reported, triaged or handled.	Small	B	257	9
15	Improved Account Termination Process	Expand on the existing process for the termination of user accounts to include systems other than LOCUS. Additional high risk systems will be identified to automatically terminate user access upon an employee ending their engagement with Loyola.	The existing termination process is manual for any systems outside of LOCUS. Managers must know who to contact to remove access to previous employees. This may allow ex-employees to continue to retain access to systems without authorization.	Large	B	255	10
16	Formalized Asset Management	Determine all assets owned by Loyola and ensure that identification and maintenance is done in an automated fashion. All assets (systems, databases, software, services, etc) should have an owner associated to them to ensure proper responsibility of maintenance of that asset is being accounted for.	Asset management will allow for system classification and owner identification. Confidential data should reside on assets with the appropriate strict security controls. Systems without confidential data do not need the same level of security.	X-Large	C	236	11
17	Security Program for Non Standard Systems	Develop a plan to identify any non-standard system (non-ITS managed) and determine a set of operational guidelines and procedures to appropriately secure those systems, based on the assets risk classification.	Many systems currently exist on the network that are not governed under the same security framework. Some of these systems contain large amounts of PII and are high risk. This project will help reduce the risk of these systems by providing a governance methodology for security standardization.	Medium	C	227	12
18	Remote Access Assessment	Review all systems available to the public and ensure that the access methods to these systems are appropriately secured.	By allowing an insecure method of remote access to a system the University risks that system being compromised by an external threat. All systems that require remote access should be secured according to a defined standard.	Small	C	221	13
19	Network Segmentation Strategy	The network will be broken up into logical segments that contain similar data classifications. Access between networks will be restricted as appropriate.	This item was defined as a critical risk item (level 4) in the 2009 security assessment. Without a proper segmentation scheme a malicious user on the network could gain unauthorized access to information systems.	Large	C	218	14
20	Disaster Recovery & Business Continuity Planning	A business continuity and disaster recovery plan should be developed that includes: Business Impact Analysis based on key stakeholders, identification of appropriate systems, development of recovery time objectives to meet the needs of the business and system recovery procedures.	Operating without a BC/DR plan puts the organization at risk as a result of a disaster. An organization could suffer a severe loss if a disaster recovery plan is not developed based on the needs of the business. Additionally, a BC/DR plan will not be executed appropriately without the business driving its development.	Large	C	217	15
21	Sanitation of Test Data	Test environments should not contain "live" data from the production environments. A policy will be created that requires the analysis of any test systems that might contain Loyola Protected Data. Additionally, a review will be conducted against all test environments that contain Loyola Protected Data.	Traditionally, test environments do not contain the same level of security controls as production environments. However, test environments tend to have a replica of the same data as production environments. Data exposure could occur if these test systems are not properly sanitized or secured.	X-Small	C	210	16
22	Time Synchronization Improvements	All clocks on all information systems (server, network, appliance, workstation, etc) will be synchronized to a common source. The UISO will audit a sample of systems annually to determine if system clocks are synchronized.	Each information system contains an internal clock. In order for effective forensic analysis to occur over the network it is imperative all clocks remain in-sync in order to determine a sequence of interesting events.	X-Small	C	206	17