

Introduction:

The Information Risk Assessment/Business Impact Analysis process at the College will bring forward the information security risks that a department faces while engaging in its primary mission of providing services to the students and/or community. Departments will benefit from this process by becoming aware of the critical information resources that are used and by developing solutions to remove or reduce the impact of an outage on the functioning of the department. LCC has becoming increasing reliant on the technology infrastructure to perform daily tasks and it is important for the college to recognize the impact to business operations.

This procedure will detail the steps that will be followed to complete a yearly Information Risk Assessment. The Information Risk Assessment documents will be completed by each department or groups of departments by the first of each calendar year. The Information Risk Assessment documents will outline the recommendations for security improvements for the upcoming year and will outline the resource requirements needed to complete the projects.

Responsibility:

The Director of Information Security is responsible for the implementation and monitoring of the Information Risk Assessment process.

Scope:

All Department and Divisional offices must complete the Information Risk Assessment (IRA) procedure to provide the college with information about the risks that it faces and also the value of information resources in the delivery of services within the department.

General:

The Information Risk Assessment will be started at the department level and once completed, the document will be sent to the Information Security Office and to the Division Office. The Division Office will then summarize or combine the Department Information Risk Assessment documents for inclusion in the budget development process.

1. Selection of Department IRA team and team leader
 - a. The Department Chair is required to select a person to be the Department IRA Leader. This person will be the driver behind the process within the department and will be the point of contact for both the Divisional Office and the Information Security Team during the process.
 - b. The Department IRA Leader will be required to attend an introductory meeting to be trained in the Information Risk Assessment procedure.

- c. The Department Chair is required to select a team of 3 to 6 people that will make up the Department IRA team. This team will be required to participate in the Information Risk Assessment Determination and Solution Sessions. The team members should be well versed in the operations of the department.
2. Preparation
 - a. An Information Risk Assessment Guide will be provided to give a detailed outline of the information that will be gathered and the steps needed to complete the assessment.
 - b. The Department Risk Contact will schedule a 3 Hour IRA Determination session with the Department IRA team and if needed a member of the College Information Security Team.
 - c. The Department Risk Contact will schedule a 2 Hour IRA Solution Session with the Department IRA team and a member of the College Information Security Team.
3. Information Risk Assessment Determination Session
 - a. The session will define the departments Information Assets and prioritize how important they are to the operation of the department.
 - b. The session will define the risks (threats) to the Department and its information assets and prioritize those risks.
 - c. The session will reference which risks are associated with what information asset.
4. Information Risk Assessment Solution Session.
 - a. Look at the risks associated with the most critical systems and develop solutions that either provide additional protections or to allow for faster recovery of service.
 - b. Develop cost and justification statements for the resources needed to implement the solutions. These will be forwarded as part of the budget process for resource allocation.
5. Reporting
 - a. The completed Risk Assessment/Business Impact Analysis for a department will be forwarded to the Division office and to the Director of Information Security.
 - b. The reports will be retained and monitored by the Information Security office to look for trends and provide insight to the leadership team on shared solutions to departmental risks.

The Information Risk Assessment/Business Impact Analysis process produces information that is to be considered confidential to the College. All reports and working documents should not be stored in public work spaces or left for public review.