Third Party Security Review Process v2.1

Rev. 05/30/18

Table of Contents

Version Control 2
Introduction 4
Purpose 4
Process Description 4
Initiation 4
Information Gathering 5
Acceptance of Documentation 5
Information Review 5
Review Time 6
Determine Compliance 6

Introduction

The Information Security Program recognizes that the University's information assets are critical and important to the University's operations and delivery of services. It is the responsibility of all users to ensure the security of information assets and to protect them in a manner that reduces the risk of unauthorized information disclosure, modification, or destruction, whether accidental or intentional.

Therefore, The Information Security Program has adopted a risk management approach to identify, assess and determine appropriate mitigation of vulnerabilities and threats that can adversely impact the University's information assets. This approach has been deployed through the Process called Third Party Security Review.

The Third Party Security Review Process is part of the landscape of processes which the Governance Risk and Compliance Management Group (GRC), a group of Information Protection and Security and Information Security Office (IPS/ISO) Division of OIT, has established to ensure that appropriate security controls are implemented over the University's information assets in order to protect the confidentiality, integrity and availability of data.

Purpose

The purpose of this document is to outline the overall Third Party Security Review Process. This Process will analyze, identify, assess and provide recommendations and possible mitigation actions for vulnerabilities and threats that may be associated with an application, service, solution or product to be acquired by the University.

Process Description

Initiation

The Third Party Security Review Process starts with a necessity of a Unit or School to acquire a product, software or service offered by a third party that needs to use, process, transmit, store or reproduce Rutgers University's data. Procurement Services addresses this necessity by identifying the different options and vendors in the market.

As data protection is critical to fulfill Rutgers University's policies, the Procurement Department must initiate this Process since they can determine if the service or product offered will include the processing of University data. Therefore, Procurement Services must ask the business requester to complete the Third Party Security Review Questionnaire.

The Information Security Third Party Questionnaire is the main document the IPS Department uses to evaluate if the security controls provided by the vendor are appropriate based on best business practices and the Rutgers Information Classification Policy 70.1.2.

Information Gathering

Once the requester receives the Questionnaire, he/she must complete the general information section on the Questionnaire; provide an explanation of the business need; provide the proposal from the vendor; and provide any documentation that he/she considers appropriate. Once completed, the requester shall send the vendor the Questionnaire to fill out the specific questions about the security controls of the product or service being offered.

Once all information requested is complete, the requester or Procurement Services must send the Questionnaire and additional documentation directly to the mailing list security_reviews@email.rutgers.edu. This mailing list will be reviewed by one of the two teams under the IPS Department: Governance Risk and Compliance Group (GRC) Group or the Cybersecurity Defense Services Group (CDS). The designated group to perform the review will depend on the Rutgers University unit/school requesting the product/service.

The GRC Group will process requests sent by the Rutgers Biomedical and Health Sciences (RBHS) schools and units or departments identified as covered components under the HIPAA Regulation. A more detailed explanation of these covered components can be found in the Hybrid Entity Declaration Policy - 100.1.12. The CDS Group will process all other departments of Rutgers University.

From this point on, this document only reflects the Third Party Review Process that the GRC Group follows. The CDS Group follows another sub-process.

Acceptance of Documentation

The request will be processed only if it meets the following requirements:

- The Questionnaire must be fully completed.
- The Questionnaire must be filled out by the Requester and the Vendor, according to the Questionnaire's instructions.
- The "Classification of data" field must be filled out only by the Requester.
- Documentation considered relevant to respond to any of the questions must be attached to the Questionnaire.
- The Cloud Security Alliance Questionnaire (CSA) is the only questionnaire that can be sent in place of the Information Security Third Party Questionnaire. A HITRUST certification letter also may be accepted in place of completing the questionnaire.

Information Review

The GRC Group will review the information provided by the School/Unit representative to ensure:

- The Questionnaire and information provided is complete.

- There is a clear understanding of the product or service.

The GRC Group will conduct further research if required.

The review will be based upon the ISO 27002:2013 Security Control Clauses such as:

- Information Security Policies
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development and Maintenance
- Supplier Relationships
- Information Security Incident Management
- Business Continuity Management
- Compliance

Review Time

If the Questionnaire does not fulfill the previous requirements, the request under the Third Party Security Review Process will not be considered, and the requester will need to resubmit the request.

If the Questionnaire meets the previous requirements and no questions are raised by the GRC Group, a final response will be sent to the requester within seven (7) business days from the date of receiving the Questionnaire.

If required, a meeting or conference calls will be scheduled with the appropriate parties to gather additional information and/or clarify questions.

Determine Compliance

For each area that is not in compliance with the ISO 27002 requirement, applicable regulation, University policy or security best practices, the GRC Group will identify potential remediation options.

Final Response

The GRC Group will prepare a Final Response with the recommendations/remediation plans based upon the identified risks associated to the review. The Final Response will be sent via e-mail to the Requester and the Procurement Analyst in charge of the request.

The Final Response will include the following sections:

1. Overview
2. Review Summary
3. Approval
4. Risks Identified / Remediation Actions / Recommendations

Follow Up

It is the responsibility of the Requester or the Business Process Owner to implement and periodically communicate the status of agreed upon remediation noted in the report.

The GRC Group can be contacted to provide guidance on remediation steps on an as needed basis.

Documentation

All documentation received and reports issued as part of the operation of this Process are stored in the Rutgers University's learning and collaboration management system (SAKAI).

Workflow of the Process

This process is depicted in the workflow diagram file Third Party Security Review Process Workflow Diagram–2.0.