Queens College
Information Technology Services
Cybersecurity Office

RISK ACCEPTANCE FORM

This form is used to justify a risk acceptance of a known deficiency. The system/project manager is responsible for writing the justification and the compensating control. It is required that a compensating control be defined to obtain full approval for a risk acceptance. A form must be completed for each NIST 800-53 Control and all fields must be completed.

1. NIST 800-53 Control Family Deficiency:

Access Control

a. NIST 800-53 Control Deficiency:

2. Description of the Deficiency:

3. Justification for Risk Acceptance

4. Description of the Compensating Control that will be put in place:

5. Additional Remarks:

System/Project Owner:	Date:
Department Chair:	Date:
Dean of School:	Date:
ITS Chief Information Security Officer:	Date:
Provost:	Date:
Chief Information Officer:	Date
President:	Date
Risk Acceptance Expiration	Date:

Instructions for Risk Acceptance Forms

- *NIST 800-53 Control Family Deficiency:*
  - *Display the appropriate National Institute of Standards and Technology (NIST) control family associated to the deficiency. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*
- *NIST 800-53 Control Deficiency:*
  - *Display the appropriate National Institute of Standards and Technology (NIST) control associated to the deficiency. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*
- *Description of the Deficiency:*
  - *Provide a summary of the overall deficiency.*
- *Justification for a Risk Acceptance:*
  - *Justify why a Risk Acceptance is requested versus remediating the deficiency.*
- *Describe the Compensating Control that will be put in place:*
  - *To obtain a Risk Acceptance for a deficiency, a compensating control must be put in place. A very detailed description must be provided, in writing, and the approving individuals on the form are accepting the compensating control.*
- *Additional Remarks*
  - *Provide any other comments and supporting material needed for the Risk Acceptance.*
- *Approvals*
  - *System/Project Owner*
  - *Department Chair*
  - *Dean of School*
  - *Chief Information Security Officer*
  - *Provost*
  - *Chief Information Officer*
  - *President*
- *Risk Acceptance Expiration Date:*
  - *Cannot Exceed 1 year from the CISO's approval date.*

NIST 800-53 Control Families

NIST SP 800-53 has more than 1,000 controls across 20 distinct control 'families'. Families include a range of controls relating to their specific area. For example, the 'Access Control' family contains security and privacy controls relating to device and user access to the system.

The 20 NIST SP 800-53 control families are:

Access Control

The Access Control family contains controls that cover access to systems, networks, and devices. Controls provide guidance on the implementation of access policies, account management, and topics like user privileges. The controls aim to lower the risk of unapproved access to a range of systems, devices, or networks.

Awareness and Training

The Awareness and Training family of controls helps to ensure users of information systems are adequately trained to identify threats. A particular focus is improving awareness of different operational risks and threats to privacy or system security. Requirements around the creation of training policy, records, and feedback helps to fine-tune the organization's approach to cybersecurity training.

Audit and Accountability

The Audit and Accountability family of controls provides guidance on procedures for event logging and auditing. Controls cover the baseline content of audit records, the capacity of log storage, and the process for monitoring and reviewing logs. Log audits are an important part of identifying the cause of breaches or system issues, and are a tool for accountability.

Assessment, Authorization and Monitoring

The Assessment, Authorization and Monitoring family focuses on the continuous monitoring and improvement of security and privacy controls. It covers the creation of an assessment plan and the delegation of the team to carry out control assessment. Controls also cover the creation of a plan of action and milestones (POAM), an integral document for identifying and fixing vulnerabilities or weaknesses.

Configuration Management

The Configuration Management family contains controls focusing on the configuration of software and devices on the network. Controls cover the creation of a configuration policy, the creation of a baseline configuration of the system, and the management of unauthorized configuration or devices. Configuration controls lower the risk of unauthorized hardware or software being installed on the system, or vulnerabilities caused by changes to settings.

Contingency Planning

The Contingency Planning family contains controls to prepare organizations for system failures and breaches. Controls cover the planning for alternative processing or storage sites and the creation of system backups to help mitigate system downtime. Other controls focus on contingency planning, including training and plan testing. This family of controls is important for mitigating the damage from a system outage or network breach, establishing clear plans to restore normal operation.

Identification and Authentication

The Identification and Authentication family contains controls for the reliable identification of users and devices. Different controls focus on different elements of safe user or device authentication. Controls strengthen user management policies, lowering the risk of unauthorized access to the system.

Incident Response

The Incident Response family contains controls for all aspects of responding to a serious incident. This includes training and planning for potential incidents, as well as plans for actively monitoring and responding to incidents as they occur. Enhanced controls cover specific types of incidents that distinct organizations might face. Incidents may include data breaches, breakdowns in the supply chain, public relations damage, or malicious code in the system.

Maintenance

The Maintenance family of controls deals with all elements of system maintenance, including software updates, logging, and inspection tools. It covers the need for timely maintenance to lower the risk of operational outages, and outlines policy and the management of maintenance personnel.

Media Protection

The Media Protection family of controls covers the use, storage and safe destruction of media and files in the organization. Established policies and procedures help to lower the risk of information breaches and leaks.

Physical and Environmental Protection

The Physical and Environmental Protection family of controls covers physical access to devices and facilities, and the mitigation of threats to facilities. Controls cover policies for physical access to system controls, including monitoring access and visitors, as well as the monitoring of devices and assets. Other controls cover responses to physical threats, such as emergency lighting or power and the relocation to alternative facilities.

Planning

The Planning family of controls covers privacy and system security plans (SSPs), including system architecture, management processes, and the setting of baseline system settings.

Program Management

The Program Management family of controls covers all elements of the management of an information system, including a variety of processes, programs, and plans. This includes an information security program plan, risk management strategy, and critical infrastructure plan.

Personnel Security

The Personnel Security family of controls covers different policies and procedures around the management of personnel. This includes the process for terminating personnel contracts and the relative risk of each position to information security.

Personally Identifiable Information (PII) Processing and Transparency

The PII Processing and Transparency family of controls helps to safeguard sensitive data, focusing on consent and privacy. Organizations can lower the risk of data breaches by properly managing personally identifiable information.

Risk Assessment

The Risk Assessment family of controls focuses on the assessment of system vulnerabilities and relevant risk. Controls cover the development of risk response procedures, and the use of vulnerability monitoring tools and processes.

System and Services Acquisition

The System and Services Acquisition family of controls includes the allocation of resources and the creation of system development life cycles. Controls help organizations create a safe acquisition process for new systems and devices, safeguarding the integrity of the wider system and data. Controls also cover the development and testing process for new systems, including developer training and security processes.

System and Communications Protection

The System and Communications Protection family of controls covers the protection of system boundaries and the safe management of collaborative devices. Controls provide in-depth guidance on set-up and ongoing management of systems, including access, partitions, and usage restrictions.

System and Information Integrity

The System and Information Integrity family of controls focuses on maintaining the integrity of the information system. Controls cover topics like protection from malicious code and spam, and procedures for ongoing system-wide monitoring.

Supply Chain Risk Management

The Supply Chain Risk Management family of controls covers policies and procedures to counter risks in the supply chain. This includes processes to assess and manage suppliers, and the inspection of supply chain systems and components.