Project Management Security Checklist

Initiating

Business Owner	Identifies the Data Steward and Security Liaison.
Project Manager	Adds Data Steward and Security Liaison to the Stakeholder Registry.
Project Manager	Adds Business Owner's responsibilities to the RACI.
Business Owner	Identifies the data's classification.
Business Owner	Requests "initial" data access from the Data Steward.
Data Steward	Authorizes "initial" data access.

Planning

Business Owner	Includes security contract language—if the information system is pre-purchase.

Executing

Technical SME	Ensures USC's Minimum Security Controls are in place.
Technical SME	Ensures compliance security controls are in place (if applicable).
Technical SME	Performs a credentialed vulnerability scan.
Technical SME	Resolves all "Critical" vulnerabilities identified during the vulnerability scan.
Technical SME	Informs the Business Owner that Minimum Security Controls (and other required security controls) are in place.
Business Owner	Requests authorization with the "Data Steward Authorization Memo."
Data Steward	Authorizes "on going" data use access.

No.	Responsible	Task	Phase	Description
1	Business Owner	Identifies the Data Steward and Security Liaison.	Initiating	The Data Steward & Security Liaison are two key security roles. Data Stewards are responsible for making security decisions regarding access to the data under their charge (UNIV 1.5). Security Liaisons are an organization's point-of-contact with the UISO. IT 3.0 states, "Security Liaison[s] will remain knowledgeable about current security issues, Information Security Program requirements, and the unit's IT assets." Data Stewards make security decisions. They should know about projects that affect their data and any related security issues. Typically, a Security Liaison will not have decision making authority. But, Liaison's report annual compliance to the UISO and need to know about projects and risks in their departments.
2	Project Manager	Adds Data Steward and Security Liaison to the Stakeholder Registry.	Initiating	
3	Project Manager	Adds Business Owner's responsibilities to the RACI.	Initiating	
4	Business Owner	Identifies the data's classification.	Initiating	Classifying data and identifying compliance requirements are essential in selecting security controls. The classification level determines the security controls that the OU must apply. The Business Owner will identify the data's classification using the State of South Carolina's Data Classification Scheme. They will also identify any regulatory compliance requirements that must be met.
5	Business Owner	Identifies laws, regulations, and security standards that apply.	Initiating	
6	Business Owner	Requests "initial" data access from the Data Steward.	Initiating	
7	Data Steward	Authorizes "initial" data access.	Initiating	
8	Business Owner	Includes security contract language—if the information system is pre-purchase.	Planning	Security contract language includes clauses to use in service agreements. The language covers how providers should protect and use sensitive data.
9	Technical SME	Ensures USC's Minimum Security Controls are in place.	Executing	
10	Technical SME	Ensures compliance security controls are in place (if applicable).	Executing	At a minimum, information systems must meet the minimum security standards detailed on security.sc.edu. The Organizational Unit is responsible for implementing security controls, and they will attest if the information system meets controls. If the information system falls under regulatory compliance, such as PCI DSS, they must also attest that they meet required security controls.
11	Technical SME	Performs a credentialed vulnerability scan.	Executing	Vulnerability scans assess an information system for weaknesses. They determine if and where a system can be exploited. The UISO can perform a vulnerability scan. The Technical SME can request a scan through ServiceNow.
12	Technical SME	Resolves all "Critical" vulnerabilities identified during the vulnerability scan.	Executing	
13	Technical SME	Informs the Business Owner that Minimum Security Controls (and other required security controls) are in place.	Executing	
14	Business Owner	Requests authorization with the "Data Steward Authorization Memo."	Executing	The memo presents a summary of key information security areas for an information system. It provides information on topics, such as data sensitivity and security compliance. It also describes how the project meets information security requirements and addresses vulnerabilities. For Data Stewards, this information them make an informed, risk-based decision regarding data access.
15	Data Steward	Authorizes "on going" data use access.	Executing	

Authorization Memo—USC Information Systems

1 The **Business Owner** identifies the Data Steward and Liaison. *The Liaison is copied.

2 The **Data Steward** approves data access.

3 The **Business Owner** identifies the data's classification as well as laws, regulations, or standards.

4 The **Business Owner** attests that the project meets security requirements.

5 The **Business Owner** also attests that the vulnerability scan shows no critical flaws.

ISPS and MSS are required for all Information Systems

Date: [Date]
To: [Data Steward]
From: [Business Owner] 1

Subject: Authorization Request & Information Security Compliance Status for [Project]

This letter presents a summary of key information security topics and how [Project] meets security requirements. As the Data Steward, this information will help you make an informed, risk-based decision regarding data access.[1]

Please review the summary and the attestation of requirements presented. If you approve data access, please send an email with your decision to [BusinessOwner@mailbox.sc.edu]. 2

Security Summary & Attestation

- **Data classification.** [Project] stores [student records], which are classified "[Restricted]."[2] If restricted information is inappropriately altered, or is subject to unauthorized access, use or disclosure, significant loss including statutory penalties will occur. 3
- **Laws, Regulations, and Minimum Security Standards.** [Project] must comply with the following:
  - FERPA: The use of student records must align with the Family Educational Rights and Privacy Act of 1974 (FERPA).
  - ISPS: As a state agency, the University must follow the State of South Carolina's Information Security and Privacy Standards (ISPS).
  - Minimum Security Standards (MSS): The MSS are a select set of prioritized security controls. These controls represent essential protections that University systems and organizations must have in place. 4

As [Business Owner], I attest that this project complies with laws, regulations, and Minimum Security Standards. This project also completed a vulnerability scan, and no critical 5 vulnerabilities exist. Note that the requirements are not independently verified. If you would like verification, please submit a verification request to the University Information Security Office.

If you have any questions about this request, please email me at [BusinessOwner@mailbox.sc.edu].

cc: Audit & Advisory Services
Chief Information Security Officer
Security Liaison

---

[1] University Policy UNIV 1.50, Data Steward Responsibilities
[2] Classification is set by the State of South Carolina's Data Classification Schema