# Introduction

To protect IT assets and data in an effective manner, an agency must identify necessary security controls in the planning phase of new development and maintenance efforts. These security controls must be accounted for in project budgets and schedules. Business and technical leaders can influence a system?s IT security risks, corresponding controls, and cost. This is accomplished by planning early for the type and sensitivity of data involved, the profiles of allowed users, and the architecture of the application and IT infrastructure.

# Purpose

This IT Security Checklist provides a structured and uniform method to help agency business and technical leaders:

1. Understand the controls needed to comply with the IT security standards based on the system?s data, users and architecture.
2. Finalize the cost, resource, and schedule estimates of the security controls for inclusion in agency budgets and schedules.
3. Anticipate the user?s experience to obtain security credentials and access the system.
4. Conduct a management discussion on the above to optimize system value, cost, security, and the user experience.

# Using the IT Security Checklist

This IT Security Checklist is used as required in Section 1.5(3) of the IT security standards. The IT Security Checklist is completed by applicable technical groups in the agency including the IT security staff. It is discussed and agreed upon by the business sponsor with the IT security and technology leadership.

The IT Security Checklist contains three sections:
*Section 1 - Agency and System Characteristics*
This section identifies the main characteristics of the agency and system that affect IT security risk and corresponding controls.
*Section 2 ? Agency wide IT Security Controls That Protect the System Under Review*
This section surfaces security controls that protect agency wide IT infrastructure and all systems, as it pertains to the system under review. Update Section 2 when significant changes are made to the Agency?s IT infrastructure or organizational security practices.
*Section 3 - System Specific Security Controls*

This section surfaces security controls that protect the specific application, system, or IT infrastructure under review. Complete Section 3 for each application/system in the planning stage for new development and maintenance.
Agencies shall take steps to provide sufficient controls in every IT Security Functional Area.

**Section 1 - Agency and System Characteristics**

| ***Instructions: This section describes the system-related information used to characterize the spe application/system and IT operational environment. For the IT application/system environment u please identify the following:*** | |
|---|---|
| 1. Application/System Name: | |
| 2. Application/System purpose or mission: | |
| 3. How important is the system to the user organization?s mission. | |
| 4. What information is generated by, consumed by, presented by, processes on, stored in, and retrieved by the system? | |
| 5. How important is the information to the user organization?s mission? | |
| 6. Where specifically is the information processed and stored? (such as a data center, laptop, etc.) | |
| 7. What is the potential negative impact on the organization if the information is disclosed to unauthorized personnel? | |
| 8. Users of the system: (May include the identification of the roles or classes of users such as but not limited to:<br>a. Administrator.<br>b. Internal Users.<br>c. External Users. | |
| 9. Hardware: (such as mainframe, server, etc.) | |
| 10. Software: (such as operating system, RDBMS, Java Runtime engine, browser, etc.): | |
| 11. System interfaces: | |
| 12. Operational Protocols: (such as TCP/IP, VOIP, SSL, etc) | |
| 13. Port Use Requirements: | |
| 14. Physical security environment of the IT system: | |

| ***Instructions: This section is designed to help you determine whether your agency has a high, m reliance on Information Technology (IT).***<br><br>***Scoring: very low = 0; low = 1; medium = 2; high = 3; very high = 4*** | |
|---|---|
| **State Agency Characteristics AND RELIANCE ON IT** | **SCORE** |
| 15. Annual budget of the entire agency: Less than $10 million = very low<br>$10 million to $100 million = low<br>$100 million to $250 million = medium<br>$250 million to $500 million = high<br>More than $500 million = very high | |

| | |
|---|---|
| 16. Number of employees: Less than 50 employees = very low<br>50 to 100 employees = low<br>100 to 1,000 employees = medium<br>1,000 to 5,000 employees = high<br>more than 5,000 employees = very high | |
| 17. Dependence upon information technology systems and the Internet to offer services to customer, outreach programs, conduct research, and support services | |
| 18. Value of agency?s intellectual property stored or transmitted in electronic form | |
| 19. Impact of major system downtime on operations | |
| 20. Degree of change within agency (expansions, reorganizations, etc.) | |
| 21. Impact to your agency?s operations from an Internet outage | |
| 22. Dependency on multi-site operations | |
| 23. Plans for multi-site operations (e.g. outsourced business functions, multiple locations, new collaborations) | |
| 24. Potential impact to national or critical IT infrastructure in case of outage, interruption, or compromise to your systems | |
| 25. Stakeholder and customer sensitivity to security and privacy | |
| 26. Level of regulation regarding security and privacy (e.g. HIPAA, FERPA, GLBA, Sarbanes-Oxley, PCI DSS, other applicable federal or state laws or regulations) | |
| 27. Negative impact on reputation of a security incident (negative press, political pressure, etc.) > | |
| 28. Extent of operations dependent upon third parties (contractors, business partners, suppliers) | |
| 29. Does your agency have business programs in a politically sensitive area that may make it a target of a violent physical or cyber attack from any groups? | |

**Section 2 ? Agency-wide IT Security Controls That Protect the System Under Review**

| | |
|---|---|
| ***Instructions: Use the tables below to analyze agency IT development and maintenance projects f<br>each functional area of the IT security standards. If a section of the Standard is not fully satisfied<br>project, list the additional control(s) necessary to comply and the associated cost, resources, an<br>estimates for each control.***<br><br>***Update Section 2 when significant changes are made to the agency?s IT infrastructure or organi<br>practices.***<br>***For Example:*** | |
| ***4.4 Secure Data Transfer*** | |
| ***Are the requirements in this section currently satisfied for this project?*** | ***Yes No N/A*** |

***Additional controls and estimates:***

**1. Encrypt Category 3 data in transit to cities.**

- ***Cost: $5,000; Schedule: 2 weeks; Resources: 1 developer, 1 server certificate***

**2. Encrypt Category 4 data in transit to the federal government.**

- ***Cost: $3,000; Schedule: 1 week; Resources: 1 developer, 1 server certificate***

| | |
|---|---|
| ***Estimated Cost:*** | ***$8,000*** |

**3 Physical and Environmental Protection**

*3.1 Facilities*

Controls related to physical access to systems as well as safeguards against threats to the environment operates.

| | |
|---|---|
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |

**5 Network Security**

Controls related to the system/applications specific connection to the network.

*5.1 Secure Segmentation*

| | |
|---|---|
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |

*5.2 Restricted Services*

| | |
|---|---|
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |

*5.3 External Connections*

| | |
|---|---|
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |

*5.4 Wireless Connections*

| | |
|---|---|
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |

*5.5 Security Patch Management*

| | |
|---|---|
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |

*5.6 System Vulnerabilities*

| | |
|---|---|
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |

| | |
|---|---|
| **Estimated Cost:** | |
| *5.7 Malicious Software Protection* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| *5.8 Mobile Computing* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| **8 Operations Management**<br>Controls related to IT functions and processes that affect the ongoing operations and maintenance of a<br><br>*8.1 Change Management* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| *8.2 Asset Management* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| *8.3 Media Handling and Disposal* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |

| | |
|---|---|
| *8.4 Data and Program Backup* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| **9 Electronic Commerce**<br>Related to the risk of using the Internet and other electronic transactions to conduct transactions for stat<br>public entities, citizens, and businesses. | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| **11 Incident Response**<br>Controls related to the effectiveness of the detection, isolation, eradication, and recovery phases of secu | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |

**Section 3 - System Specific Security Controls**

| |
|---|
| ***Instructions: This section surfaces security controls that protect the specific application or syst*** |
| ***Complete Section 3 for each application/system in the planning stage for new development and*** |
| **4 Data Security**<br>Controls related to the inherent value of the type data handled by a system, and its potential for harm if<br><br>*4.1 Data Classification* ? Check below the Data Category(ies) relevant to the information impacted by th |

| | |
|---|---|
| **Category 1 ? Public:** Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls. | |
| **Category 2 ? Sensitive:** Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested. | |
| **Category 3 ? Confidential:** Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:<br>a. Personal information about individuals, regardless of how that information is obtained.<br>b. Information concerning employee payroll and personnel records.<br>c. Information regarding IT infrastructure and security of computer and telecommunications systems. | |
| **Category 4 ? Confidential with special handling;** Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:<br>a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.<br>b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions. | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |

| | |
|---|---|
| *4.2 Data Sharing* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| *4.3 Secure Management and Encryption of Data* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| *4.4 Secure Data Transfer* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |

| | |
|---|---|
| Additional controls and estimates: | |
| **Estimated Cost:** | |

**5 Network Security**
Controls related to the system/applications specific connection to the network.

*5.1 Secure Segmentation*

| | |
|---|---|
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |

**6 Access Security**
Controls related to user account management and logical access controls.

*6.1 Access Management*

| | |
|---|---|
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |

*6.2 Password Requirements*

| | |
|---|---|
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |

*6.3 Authentication*
Describe the level of authentication required, the anticipated user experience and the impact on custom system users:

| | |
|---|---|
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| Declare the Authentication Type(s) used by checking the box(es) below: | |
| **Anonymous**<br>No specific network or application level security requirements. | |
| **Type 1 - External**<br>Access to category 1 data, if authenticated (not anonymous), requires authentication via the SecureAccess® Washington infrastructure (OCIO Identity Management User Authentication Standards 7/10/2008) with the following controls:<br>• Requires UserID and hardened passwords as defined in Section 6.2(4).<br>• Password expiration period not to exceed 24 months. | |

| | |
|---|---|
| **Type 2 - External**<br>Access to category 2 data or a single category 3 record belonging to the individual requires authentication via the SecureAccess® Washington infrastructure (OCIO Identity Management User Authentication Standards 7/10/2008) with the following controls:<br><br>• Requires UserID and hardened passwords as defined in Section 6.2(4).<br>• Password expiration period not to exceed 24 months. | |
| **Type 3 - External**<br>Access to category 3 data or a single category 4 record belonging to the individual requires authentication via the SecureAccess® Washington infrastructure (OCIO Identity Management User Authentication Standards 7/10/2008) with the following controls:<br><br>• Requires hardened password as defined in Section 6.2(4).<br>• Password expiration period not to exceed 13 months.<br>• Requires multi-factor authentication supported by SecureAccess® Washington. | |
| **Type 4 - External**<br>Access to category 4 information requires multi-factor authentication via the SecureAccess® Washington or Transact? Washington infrastructure (OCIO Identity Management User Authentication Standards 7/10/2008) with the following controls:<br><br>• Requires two-factor authentication using hardware or software tokens or digital certificates.<br>• Requires that the individual prove through a secure, encrypted authentication protocol that the individual controls the token by first unlocking the token with a password, PIN or biometric and in a secure authentication protocol to establish two factors of authentication using a hardware or software token or digital certificate. | |
| **Type 5 - External**<br>Employee and contractor access to agency resources or the SGN via common remote access methods requires two-factor authentication with the following controls:<br><br>• Requires that the individual prove through a secure, encrypted authentication protocol that the individual controls a hardware or software token by first unlocking the token with a password, PIN or biometric and in a secure authentication protocol to establish two factors of authentication. | |

| | |
|---|---|
| **Type 6 - External**<br>Authenticated access that does not meet the criteria outlined in the OCIO Identity Management User Authentication Standards 7/10/2008 requires the following minimum controls:<br><br>• Requires a hardened password as defined in Section 6.2(4) or stronger authentication.<br>• Password expiration not to exceed 120 days.<br>• Additional controls documented in the agency IT Security Program | |
| **Type 7 ? Internal**<br>Access to category 4 data and below requires authentication via the Enterprise Active Directory infrastructure (OCIO Identity Management User Authentication Standards 7/10/2008) with the following controls:<br><br>• Requires UserID and hardened passwords as defined in Section 6.2(5).<br>• Password expiration period not to exceed 120 days. | |
| **Type 8 - Internal**<br>Access to system administration functions requires the following controls:<br><br>• Requires a discrete account used only for interactive system administration functions.<br>• Where passwords are employed as an authentication factor:<br>  ○ Requires a hardened password as defined in Section 6.2(5) with an extended password length of 16 characters.<br>  ○ Password expiration period not to exceed 60 days. | |
| **Type 9 - Internal**<br>Accounts used for system service, daemon or application execution (service accounts) require documentation in the agency security program and the following controls:<br><br>• Requires a discrete account used only for the defined privileged functions, and never used by an individual.<br>• Requires a hardened password as defined in Section 6.2(5) with an extended password length of 20 characters.<br>• Password expiration requirements must be documented in the agency security program.<br>• The principle of least privilege must be employed when determining access requirements for the account. | |

| | |
|---|---|
| **Type 10 ? Internal**<br>Authenticated access that does not meet the criteria outlined in the OCIO Identity Management User Authentication Standards 7/10/2008 requires the following minimum controls:<br>• Requires a hardened password as defined in Section 6.2(5) or stronger authentication.<br>• Password expiration not to exceed 120 days.<br>• Additional controls documented in the agency IT Security Program. | |

| | |
|---|---|
| *6.4 Remote Access* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| **7 Application Security**<br>Controls related to the design, development, deployment, and ongoing maintenance of applications. | |
| *7.1 Planning and Analysis* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| *7.2 Application Development* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| *7.3 Application Maintenance* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| *7.4 Vulnerability Prevention* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| *7.5 Application Service Providers* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| **10 Security Monitoring and Logging**<br>Controls related to monitoring processes and mechanisms for assessing ongoing compliance with security requirements, as well as capture of data for reconstruction of security-relevant events. | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |
| Additional controls and estimates: | |
| **Estimated Cost:** | |
| *10.3 Intrusion Detection and Prevention* | |
| Are the requirements in this section currently satisfied for this project? | Yes No N/A |

| Additional controls and estimates: | |
|---|---|
| **Estimated Cost:** | |
| **Total Estimated Cost:** | |

**Source URL:** https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets-0