

**Office of the State Controller**

Self-Assessment of Internal Controls

**Computer Security Cycle**

Objectives and Risks

Agency \_\_\_\_\_

Year-End \_\_\_\_\_

<u>Objectives</u>	<u>Risks</u>
Definition and communication of organizational structure, policies and procedures.	<ul style="list-style-type: none"> <li>• Control may be superficial, inconsistently followed or subject to override or circumvention.</li> <li>• Segregation of incompatible duties.</li> <li>• Opportunities to perpetrate and conceal fraud may exist if personnel have direct or indirect access to assets.</li> </ul>
Management and user involvement and approval.	<ul style="list-style-type: none"> <li>• Personnel may not fully understand users' needs or the accounting aspects of the systems; systems may be developed that perform improper calculation, prepare erroneous reports or cause other processing errors.</li> <li>• Systems may be designed with inadequate control in the application programs.</li> <li>• User control may be incomplete or ineffectual as a result of poor knowledge of the system and the processing functions performed by the application programs.</li> </ul>
Restricted access to application system documentation.	<ul style="list-style-type: none"> <li>• Unauthorized persons may obtain detailed knowledge of applications and use that knowledge to perpetrate irregularities.</li> </ul>

<p>Authorization and approval of systems changes.</p>	<ul style="list-style-type: none"> <li>• Personnel may make systems changes that do not conform to users' needs resulting in processing errors.</li> <li>• Unauthorized program modifications may be implemented to perpetrate and conceal fraud.</li> </ul>
<p>Monitoring integrity of master files.</p>	<ul style="list-style-type: none"> <li>• Master files may contain erroneous data that cause errors in all transactions using those data.</li> <li>• Master file data may be altered to allow the processing of fraudulent transactions.</li> <li>• Master file data may be altered prior to the preparation of statements or confirmation.</li> </ul>
<p>Verifying accuracy of output.</p>	<ul style="list-style-type: none"> <li>• Unauthorized or fraudulent transactions introduced during processing may not be detected.</li> </ul>

**Office of the State Controller**  
Self-Assessment of Internal Controls  
**Computer Security Cycle**  
Control Policies and Procedures

Agency \_\_\_\_\_

Year-End \_\_\_\_\_

**Bolded questions identify critical controls. A critical control is a control that will prevent or detect an error in the event that all other controls fail.**

**A. Control Activities / Information and Communication:**

Yes No N/A

- |      |      |      |   |
|------|------|------|---|
| ____ | ____ | ____ | 1. Is there a formal organizational chart which identifies the individuals responsible for the:   |
| ____ | ____ | ____ | a. Computer systems?  |
| ____ | ____ | ____ | b. Computer security?   |
| ____ | ____ | ____ | 2. Has management considered the appropriate segregation of duties among personnel involved in the IT security function?  |
| ____ | ____ | ____ | 3. Have roles and responsibilities been clearly defined and communicated?   |
| ____ | ____ | ____ | 4. Is the financial system's business owner management appropriately included in the design of the IT security function from a data ownership?  |
| ____ | ____ | ____ | 5. Does management have a controlled process in place to update the security policy and procedure documentation on a periodic basis?  |
| ____ | ____ | ____ | <b>6. Is a formal documented security administration process in place to ensure that all applications access, including restricted access to financial applications, is approved?</b> |
| ____ | ____ | ____ | 7. Has management implemented a formal process for changing financial data file permissions?  |
| ____ | ____ | ____ | 8. Has management implemented a formal security administration process for granting, changing and removing direct access to financial data?   |
| ____ | ____ | ____ | <b>9. Does management periodically review monitoring reports to identify potential unauthorized activity?</b>   |

10. When an employee or contractor is terminated, are the following precautions implemented immediately:
- \_\_\_ \_\_\_ \_\_\_            a. The employee or contractor is denied access to the equipment?
- \_\_\_ \_\_\_ \_\_\_            b. The employee or contractor is denied access to any data, program listing, etc.?
- \_\_\_ \_\_\_ \_\_\_            c. All other employees are informed of the employee's termination?
- \_\_\_ \_\_\_ \_\_\_            d. The employee or contractor's user-id and password are deleted from the computer system?
- \_\_\_ \_\_\_ \_\_\_            11. Is there a time out/screen saver and/or log off function, which will protect a terminal if left unattended?
- \_\_\_ \_\_\_ \_\_\_            12. Does a login name and a password uniquely identify users when they sign on to the system (e.g. no group users IDs)?
- \_\_\_ \_\_\_ \_\_\_            13. If an employee incorrectly enters their password three times in a row, does the computer system deny them access to the computer system until reset by the system administrator?
- \_\_\_ \_\_\_ \_\_\_            14. Do all PCs under control of the agency use a recognized anti-virus (A/V) or end-point security program? Does the agency run the A/V program on a regular schedule?
- \_\_\_ \_\_\_ \_\_\_            15. Does the agency have a firewall established for their LAN or for individual workstations?
- \_\_\_ \_\_\_ \_\_\_            16. Is there a written disaster recovery (DR) plan?
- \_\_\_ \_\_\_ \_\_\_            17. **Does the DR plan include identification of the following?**
- \_\_\_ \_\_\_ \_\_\_                a. **Critical applications?**
- \_\_\_ \_\_\_ \_\_\_                b. **Staff responsibilities?**
- \_\_\_ \_\_\_ \_\_\_                c. **Steps for recovery of the system?**
- \_\_\_ \_\_\_ \_\_\_                d. **Computer equipment needed for temporary processing?**
- \_\_\_ \_\_\_ \_\_\_                e. **Business location(s) that could be used to process critical applications in the event of an emergency?**
- \_\_\_ \_\_\_ \_\_\_            18. **Has the agency taken steps to prevent and minimize potential damage and interruption through the use of data and program backup procedures, including off-site storage of backup data as well as environmental controls, staff training and hardware maintenance and management?**

\_\_\_ \_\_\_ \_\_\_ 19. Are there provisions for retaining and/or copying master files, and is there practical means of reconstructing a damaged or destroyed file?

**B. Monitoring:**

\_\_\_ \_\_\_ \_\_\_ 20. **Does the agency monitor information systems access, investigate apparent violations, and take appropriate remedial and disciplinary action?**

\_\_\_ \_\_\_ \_\_\_ 21. **Does the department or management balance control totals generated during computer processing with those originally established and reconcile all discrepancies?**