



# Compliance Component

## DEFINITION

<i>Name</i>	Separation of duties
<i>Description</i>	Separation of duties is an organizational principle, which specifies that functions are assigned in a manner so that no one individual can control every activity in an end-to-end process.
<i>Rationale</i>	Provides process integrity while maintaining proper security and quality controls.
<i>Benefits</i>	<ul style="list-style-type: none"> <li>• Having different staff engaged within an end-to-end process is a common, sensible business practice that ensures consistent and successful execution of the process.</li> <li>• Effective separation of duties provides for a system of checks and balances when following the general principles below:             <ul style="list-style-type: none"> <li>• Separate system ownership from the system certification/accreditation process</li> <li>• Separate system administration from system auditing.</li> <li>• Separate operational responsibility from record keeping responsibility</li> </ul> </li> <li>• Helps ensure “the fox isn’t guarding the henhouse”</li> </ul> <p>NOTE: Adhering to these principles may not be possible due to resource limitations or other considerations. In these cases, the risk resulting from inadequate separation of duties should be assessed to ensure that the level of exposure is acceptable to an agency or division management.</p>

## ASSOCIATED ARCHITECTURE LEVELS

<i>List the Domain Name</i>	Security
<i>List the Discipline Name</i>	Management Controls
<i>List the Technology Area Name</i>	Personnel Security
<i>List Product Component Name</i>	

## COMPLIANCE COMPONENT TYPE

<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	

## COMPLIANCE DETAIL

<i>State the Guideline, Standard or Legislation</i>	<p>Separation-of-duties must be established and documented in order that an individual not have access to more than one critical task as identified by management. Examples of tasks that should be performed by different individuals:</p> <ul style="list-style-type: none"> <li>• Development</li> </ul>
---	---

	<ul style="list-style-type: none"> <li>• Testing</li> <li>• Administration (e.g. database, systems, network, etc.)</li> <li>• Physical security</li> <li>• IT security</li> </ul> <p>An audit policy should be established to ensure compliance with the separation-of-duties policy.</p>			
<i>Document Source Reference #</i>	International Standard, ISO/IEC 17799, Information Technology—Code of Practice for Information Security Management.			
<b>Standard Agency</b>				
<i>Name</i>	Applying Security Practices to Justice Information Sharing			
	<table border="1"> <tr> <td style="text-align: center;"><i>Website</i></td> <td><a href="http://it.ojp.gov/documents/asp/disciplines/index.htm">http://it.ojp.gov/documents/asp/disciplines/index.htm</a></td> </tr> </table>	<i>Website</i>	<a href="http://it.ojp.gov/documents/asp/disciplines/index.htm">http://it.ojp.gov/documents/asp/disciplines/index.htm</a>	
<i>Website</i>	<a href="http://it.ojp.gov/documents/asp/disciplines/index.htm">http://it.ojp.gov/documents/asp/disciplines/index.htm</a>			
<i>Contact Information</i>				
<b>Government Body</b>				
<i>Name</i>	<table border="1"> <tr> <td>International Standard, ISO/IEC 17799, Information Technology—Code of Practice for Information Security Management. NIST SP800-12 An Introduction to Computer Security: The NIST Handbook.</td> <td style="text-align: center;"><i>Website</i></td> <td> <a href="http://www.iso17799software.com">http://www.iso17799software.com</a>   <a href="http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf">http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf</a> </td> </tr> </table>	International Standard, ISO/IEC 17799, Information Technology—Code of Practice for Information Security Management. NIST SP800-12 An Introduction to Computer Security: The NIST Handbook.	<i>Website</i>	<a href="http://www.iso17799software.com">http://www.iso17799software.com</a>  <a href="http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf">http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf</a>
International Standard, ISO/IEC 17799, Information Technology—Code of Practice for Information Security Management. NIST SP800-12 An Introduction to Computer Security: The NIST Handbook.	<i>Website</i>	<a href="http://www.iso17799software.com">http://www.iso17799software.com</a>  <a href="http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf">http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf</a>		
<i>Contact Information</i>				
<b>KEYWORDS</b>				
<i>List all Keywords</i>	Management, administration, policy, procedures, planning, staffing, critical tasks, sensitive, data.			
<b>COMPONENT CLASSIFICATION</b>				
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i> <input checked="" type="checkbox"/> <i>Current</i> <input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>			
<b>Rationale for Component Classification</b>				
<i>Document the Rationale for Component Classification</i>				
<b>Conditional Use Restrictions</b>				
<i>Document the Conditional Use Restrictions</i>				
<b>Migration Strategy</b>				
<i>Document the Migration Strategy</i>				
<b>Impact Position Statement</b>				
<i>Document the Position Statement on Impact</i>				

### CURRENT STATUS

*Provide the Current Status)*

*In Development*

*Under Review*

*Approved*

*Rejected*

### AUDIT TRAIL

<i>Creation Date</i>	05/25/06	<i>Date Accepted / Rejected</i>	06/13/06
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>		<i>Last Date Updated</i>	
<i>Reason for Update</i>			