



INFORMATION SECURITY'S CERTIFICATION AND ACCREDITATION CHECKLIST

http://www.state.nj.us/it/ps/14-13-NJOIT_205_Certification_and_Accreditation.pdf

Agency / Asset Information	
Date:	
Agency:	
ASAI:	
Project Name:	
Application Name:	

<p>The purpose of the checklist is to guide an agency and for the Statewide Office of Information Security to follow in validating security requirements for systems, applications, system software, and other technologies before they are deployed into a production environment. It is designed to ensure compliance with specifications, regulations, standards and objectives identified during each phase of the System Development Life Cycle (SDLC). Reference the 205 – Certification and Accreditation Policy.</p> <p style="text-align: right; margin: 0;">Check Boxes for those that are Completed</p>	Initiation	Certification	Accreditation
<p>Business Case Review</p> <p>Begin the System Architecture Review (SAR) process. http://www.nj.gov/it/reviews/forms/0133_Business_Case_Review_Template.dot</p>			
<p>On-Premise and/or Cloud Provider</p> <p>Identify: <input type="checkbox"/> On Premise <input type="checkbox"/> Cloud Service Provider <input type="checkbox"/> Hybrid. (Infrastructure as a Service – single tenant). (Software as a Service – multi-tenant with no Personal Identifiable Information or Intellectual Property).</p>	<input type="checkbox"/>		
<p>Cloud Provider: RFP appendix requirements (including Security Plan)</p> <p>http://www.nj.gov/treasury/purchase/noa/contracts/m0003_11-r-21493.shtml In addition to the Standard Terms and Conditions, please reference Amendment #3 – Change to Method of Operation. This needs to be completed by the software publisher and approved by DPP. Once the terms and conditions have been addressed, we are then able to move into the system architecture review (SAR) and security realm. We will treat the software publisher as an Business Entity. Standard Security Controls Language for RFPs – reference RFP Security Controls with Extranet & File Transfer.</p>	<input type="checkbox"/>		
<p>Asset Classification</p> <p>Completed the Asset Classification worksheet.</p>	<input type="checkbox"/>		
<p>Security Requirements</p> <p>Identified anticipated security needs based on regulatory compliance.</p>	<input type="checkbox"/>	<input type="checkbox"/>	

The purpose of the checklist is to guide an agency and for the Statewide Office of Information Security to follow in validating security requirements for systems, applications, system software, and other technologies before they are deployed into a production environment. It is designed to ensure compliance with specifications, regulations, standards and objectives identified during each phase of the System Development Life Cycle (SDLC). Reference the 205 – Certification and Accreditation Policy. Check Boxes for those that are Completed		Initiation	Certification	Accreditation
Logical SAR	http://www.nj.gov/it/reviews/forms/0132_Logical_SAR_Template.dot			
Authentication and Access Controls	Implemented an authentication service such as State’s Credential and Identity Access System. Implemented account provisioning procedures and defined access roles.		<input type="checkbox"/>	
Firewall Controls	Verified and implemented firewall rule set. http://www.nj.gov/it/reviews/forms/GSN%20Extranet%20Firewall%20Form.dot		<input type="checkbox"/>	
Business Entity or Extranet: Appendix A, B, C, and D	Completed the Business Entity and Extranet Appendices. http://www.state.nj.us/it/ps/09-11-NJOIT_Extranet_Policy.pdf		<input type="checkbox"/>	
A. Application Form. http://www.state.nj.us/it/ps/09-11-P1-NJOIT_0110%20GSN%20Extranet%20Application%20Form_Appendix_A.pdf			<input type="checkbox"/>	
B. Memorandum of Understanding. http://www.state.nj.us/it/ps/09-11-NJOIT_0184_Business_Entity_IT_Services_Extranet_%20MOU_Appendix_B.dot			<input type="checkbox"/>	
C. Operational Form. http://www.state.nj.us/it/ps/09-11-NJOIT_0145_Business_Entity_IT_Services_Extranet_Connection_Detail_Appendix_C.dot			<input type="checkbox"/>	
D. Security Controls Assessment Checklist. Documentation is available through SOIS (njinfosecure@oit.nj.us) request or NJ-ISAC			<input type="checkbox"/>	
Encryption	The data is encrypted in transit.		<input type="checkbox"/>	
	The data is encrypted at rest.		<input type="checkbox"/>	
PCI-related application	PCI certification (Attestation of Compliance). The Attestation is a PCI-DSS assessment and certification of the Business Entity’s PCI security requirements performed by a security representative (Qualified Security Assessor). A copy of the Attestation of Compliance has been provided.		<input type="checkbox"/>	
Data Transfer	An interface report has been completed and workflow established.		<input type="checkbox"/>	

The purpose of the checklist is to guide an agency and for the Statewide Office of Information Security to follow in validating security requirements for systems, applications, system software, and other technologies before they are deployed into a production environment. It is designed to ensure compliance with specifications, regulations, standards and objectives identified during each phase of the System Development Life Cycle (SDLC). Reference the 205 – Certification and Accreditation Policy. Check Boxes for those that are Completed		Initiation	Certification	Accreditation																														
DOTGOV name space	<p>Create the dotgov name space space (include other domain space .com, etc) within the State’s environment.</p> <p>In order for a DOTGOV to be acquired by a state level authority the Chief Information Officer must approve the domain via a signed authorization letter. Creative Services keeps a copy of all the authorization letters.</p> <p>OIT does not pay for any client domains. All domains are registered by the client at their respective registrar; nj.gov and state.nj.us are registered through OIT.</p>		<input type="checkbox"/>																															
Physical SAR	http://www.nj.gov/it/reviews/forms/0135_Physical_SAR_Template.dot																																	
Vulnerability Assessment	<p>http://www.state.nj.us/it/ps/12-04-NJOIT_201_Vulnerability_Management.pdf</p> <p>Requests to OIT for a vulnerability assessment of applications, hosts, devices or networks should be submitted to oit.riskassessments@oit.nj.gov no later than 4:00 pm Thursdays and prior to 20 business days before production. Execution of security scanning will be conducted the next week following the request. The risk assessment and remediation are not included in the scanning process and must be factored into the project timeline.</p> <p>1) OS and Software scans.</p> <table border="1"> <tr> <td>Scan Date</td> <td></td> <td rowspan="2"></td> <td rowspan="2"><input type="checkbox"/></td> <td rowspan="2"></td> </tr> <tr> <td>Requestor Name</td> <td></td> </tr> </table> <p>2) Application security scans.</p> <table border="1"> <tr> <td>Scan Date</td> <td></td> <td rowspan="2"></td> <td rowspan="2"><input type="checkbox"/></td> <td rowspan="2"></td> </tr> <tr> <td>Requestor Name</td> <td></td> </tr> </table> <p>3) Penetration testing.</p> <table border="1"> <tr> <td>Scan Date</td> <td></td> <td rowspan="2"></td> <td rowspan="2"><input type="checkbox"/></td> <td rowspan="2"></td> </tr> <tr> <td>Requestor Name</td> <td></td> </tr> <tr> <td>Vulnerabilities Detected.</td> <td><input type="checkbox"/></td> <td rowspan="3"></td> <td rowspan="3"><input type="checkbox"/></td> <td rowspan="3"></td> </tr> <tr> <td>Vulnerabilities Results Reviewed.</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Vulnerabilities Report Distributed.</td> <td><input type="checkbox"/></td> </tr> </table>	Scan Date			<input type="checkbox"/>		Requestor Name		Scan Date			<input type="checkbox"/>		Requestor Name		Scan Date			<input type="checkbox"/>		Requestor Name		Vulnerabilities Detected.	<input type="checkbox"/>		<input type="checkbox"/>		Vulnerabilities Results Reviewed.	<input type="checkbox"/>	Vulnerabilities Report Distributed.	<input type="checkbox"/>		<input type="checkbox"/>	
Scan Date			<input type="checkbox"/>																															
Requestor Name																																		
Scan Date			<input type="checkbox"/>																															
Requestor Name																																		
Scan Date			<input type="checkbox"/>																															
Requestor Name																																		
Vulnerabilities Detected.	<input type="checkbox"/>		<input type="checkbox"/>																															
Vulnerabilities Results Reviewed.	<input type="checkbox"/>																																	
Vulnerabilities Report Distributed.	<input type="checkbox"/>																																	
Risk Assessment	http://www.state.nj.us/it/ps/14-02-NJOIT_Risk_Management.pdf		<input type="checkbox"/>																															

The purpose of the checklist is to guide an agency and for the Statewide Office of Information Security to follow in validating security requirements for systems, applications, system software, and other technologies before they are deployed into a production environment. It is designed to ensure compliance with specifications, regulations, standards and objectives identified during each phase of the System Development Life Cycle (SDLC). Reference the 205 – Certification and Accreditation Policy.		Initiation	Certification	Accreditation
Check Boxes for those that are Completed				
Risk Management Remediation Report Template	http://www.state.nj.us/it/ps/0166_Risk_Management_Remediation_Report%20Template.xls		<input type="checkbox"/>	
	Date Risk Remediation Rpt. Distributed:		<input type="checkbox"/>	
	Risk Remediation Rpt. Distributed to:			
	Date Risk Remediation Rpt. Returned:		<input type="checkbox"/>	
Logging / Audit	Implemented logging and auditing requirements. Reference minimum audit log requirements found in 171-01-Minimum System Security and Protection Standards.		<input type="checkbox"/>	
Minimum System Security	Implemented security requirements. http://www.state.nj.us/it/ps/14-01-NJOIT_171_Minimum_System_Security_Requirements.pdf 1) Harden the OS and software. CIS Security Benchmark tools. https://benchmarks.cisecurity.org/en-us/?route=default 2) Patch Management. 3) Anti-malware and Intrusion Detection.		<input type="checkbox"/>	
Email Relay	The State system is using the State's email relay and content inspection system.		<input type="checkbox"/>	
Privacy and Disclaimer	Added the standard privacy and disclaimer notices to the State's system.		<input type="checkbox"/>	
DOTGOV Address Assignment	Redirect the purchased name space to the DOTGOV IP address.		<input type="checkbox"/>	
Exception:	Received an exception request(s). http://www.state.nj.us/it/ps/08-02-NJOIT_Policy_Exception_Request_Form.pdf		<input type="checkbox"/>	
Implementation Review	http://www.state.nj.us/it/reviews/forms/0134_Implementation_Review_Template.doc			<input type="checkbox"/>

Please submit the Certified Accreditation Checklist and your Implementation Review to sar@oit.nj.gov.