Security Assessment Worksheet

Purpose:
The purpose of this worksheet is to be a guide when conducting security assessments in order to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

Refer to *IT0131-M - Security Assessment and Authorization Plan* for more information.

Date	
System Administrator	
System (DNS Name)	
IP Address	
OS and version	
Detailed system description and intended purpose	

Installed Applications (paste from terminal output):

Installed Services:

Name	Enabled / Disabled	Necessary (Y/N)

Mandatory and Discretionary Controls:

NIST Control		Inherited	Implemented	Planned	Exception
Access Controls					
AC-5	Separation of Duties			X	
AC-6	Least Privilege			X	
AC-7	Unsuccessful Login Attempts				
AC-8	System Use Notification				
AC-11	Session Lock			X	
Awareness and Security Training					
AT-1	Security Awareness and Training Policy and Procedures	X			
AT-2	Security Awareness Training	X			
AT-2.1	Practical Exercises	X			
AT-3	Role-Based Security Training	X			
AT-4	Security Training Records	X			
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	X			
AU-2	Audit Events				
AU-3	Content of Audit Records	X			
AU-4	Audit Storage Capacity	X			
AU-6	Audit Review, Analysis, and Reporting	X			
AU-8	Time Stamps	X			
AU-11	Audit Record Retention	X			
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	X			
CA-2	Security Assessments	X			
CA-3	System Interconnections	X			
CA-5	Plan of Action and Milestones	X			
CA-6	Security Authorization	X			
CA-7	Continuous Monitoring	X			
Configuration Management					
CM-1	Configuration Management Policy and Procedures	X			
CM-2	Baseline Configuration				
CM-2.1	Reviews and Updates				
CM-2.3	Retention of Previous Configurations				
CM-3	Configuration Change Control				
CM-4	Security Impact Analysis	X			
CM-6	Configuration Settings				
CM-7	Least Functionality				
CM-7.1	Periodic Review				
CM-9	Configuration Management Plan	X			
Contingency Planning					
CP-1	Contingency Planning Policy and Procedures	X			
CP-2	Contingency Plan	X			
CP-3	Contingency Training	X			
CP-4	Contingency Plan Testing	X			
CP-6	Alternate Storage Site	X			
CP-9	Information System Backup				
CP-10	Contingency Plan	X			
Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	X			
IA-4	Identifier Management				
IA-5	Authenticator Management				
IA-6	Authenticator Feedback				

NIST Control		Inherited	Implemented	Planned	Exception
Incident Response					
IR-1	Incident Response Policy and Procedures	X			
IR-3	Incident Response Testing	X			
IR-4	Incident Handling	X			
IR-5	Incident Monitoring	X			
IR-6	Incident Reporting	X			
IR-7	Incident Response Assistance	X			
IR-8	Incident Response Plan	X			
Media Protection					
MP-1	Media Protection Policy and Procedures	X			
MP-2	Media Access	X			
MP-4	Media Storage	X			
MP-5	Media Transport	X			
MP-6	Media Sanitization	X			
MP-7	Media Use	X			
Physical and Environmental Protection					
PE-1	Physical and Environmental Protection Policy and Procedures	X			
PE-2	Physical Access Authorizations	X			
PE-3	Physical Access Control	X			
PE-6	Monitor Physical Access	X			
PE-8	Visitor Access Records	X			
PE-10	Emergency Shutoff	X			
PE-11	Emergency Power	X			
PE-12	Emergency Lighting	X			
PE-13	Fire Protection	X			
PE-14	Temperature and Humidity Controls	X			
Personnel Security					
PS-1	Personnel Security Policy and Procedures	X			
PS-3	Personnel Screening	X			
PS-4	Personnel Termination	X			
PS-7	Third-Party Personnel Security	X			
PS-8	Personnel Sanctions	X			
Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	X			
RA-2	Security Categorization				
RA-3	Risk Assessment				
RA-5	Vulnerability Scanning				
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	X			
SC-5	Denial of Service Protection	X			
SC-7	Boundary Protection	X			
SC-12	Cryptographic Key Establishment and Management	X			
SC-15	Collaborative Computing Devices	X			
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	X			
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)				X
SC-22	Architecture and Provisioning for Name/Address Resolution Service				X
System and Information Integrity					
SI-1	System &Information Integrity Policy & Procedures	X			
SI-2	Flaw Remediation	X			
SI-3	Malicious Code Protection				
SI-4	Information System Monitoring				
SI-8	Spam Protection	X			
SI-12	Information Output Handling and Retention				

Summary and Recommendations:

Summary of Assessment

Recommendations

Notes

Appendix A - Useful Commands:

Linux:

List installed applications with versions and repository (Oracle Linux / RedHat)
```
yum list installed
```

Show services and runlevels
```
chkconfig
```

Account status information (L-locked / P-password set / NP-no password)
```
passwd -S -a
```
Returns: username | password status | password set date | min age | max age | warn | inactivity

Accounts with passwords set
```
passwed -S -a | grep P
```

Unlocked accounts (accounts that a person can log into)
```
egrep -v '.*:\*|:\!' /etc/shadow | awk -F: '{print $1}'
```

Accounts that have not been shadowed
```
grep -v ':x:' /etc/passwd
```

Listening network ports (TCP and UDP sockets)
```
lsof -i -n | egrep 'COMMAND|LISTEN|UDP'
```

NIC information
```
ip addr
```

Windows

List installed applications, vendor, and version

```
wmic <enter>
product get name, version, vendor <enter>
```

List services, status, and dependent services

```
Get-Service | select name, status, dependentservices
```

List users and enabled status

```
Get-LocalUser | select name,enabled
```

List full user information

```
Get-LocalUser username | fl
```

List users in local Administrators group

```
Get-LocalGroup administrators | fl
```

List startup programs

```
Get-CimInstance -ClassName Win32_StartupCommand | Select-Object -Property Command, Description,
User, Location
```

List NIC information

```
Get-NetAdapter | fl
```

List IP information

```
Get-WmiObject win32_networkadapterconfiguration -filter "ipenabled = 'True'"
```