Deployment	
The application/asset has been assigned to an application/asset owner.	
The design identifies, understands, and accommodates the company security policy.	
Services, protocols, and firewall rules required are identified.	
Only required services/features are enabled.	
Remote components exposed to the internet only if required, and utilize the DMZ where applicable.	
Authentication	
The design identifies service account requirements.	
Account management policies are taken into consideration by the design.	
The identity that is used to authenticate with the database is identified by the design.	
The design adopts a policy of using least-privileged accounts.	
Strong passwords are used.	
Shared accounts are not used.	
If hosted externally, access is restricted by IP address	
Authorization	
Role-based security is enabled.	
The role design offers sufficient separation of privileges (the design considers authorization granularity).	
All identities that are used by the application are identified and the resources accessed by each identity are known.	
AD authentication is used to avoid credential management.	
Administration interfaces are secured (strong authentication and authorization is used).	
Configuration secrets are not held in plain text in configuration files.	
Least-privileged process accounts and service accounts are used.	
Sensitive Data	
Database connections, passwords, keys, or other secrets are not stored in plain text.	
Sensitive data is not logged in clear text by the application.	
The design identifies protection mechanisms for sensitive data that is sent over the network. (IPSec/SSL)	

Sensitive data is not stored in persistent cookies.	
Sensitive data is encrypted at rest	
Session Management	
Session lifetime is limited.	
Session state is protected from unauthorized access.	
Session identifiers are not passed in query strings.	
Exception Management	
Application errors are logged to the error log.	
Private data (for example, passwords) is not logged.	
Auditing and Logging	
Failed login attempts are audited and logged.	
The design identifies the level of auditing and logging necessary for the application and identifies the key parameters to be logged and audited.	
The design identifies the storage, security, and analysis of the application log files.	
Logging is configured to send logs to Splunk.	
Patches and Updates	
Latest patches and updates are available and installed.	
Monitoring for and reviewing updated code (e.g., application, firmware) is assigned to:	