C&S Application Security Score Card

Note: *This score card intends to help application (or product) stake holders to self determine whether a specific application requires security assessment or not. Additionally it also helps assign weightage for individual security activities necessary for the application which in return helps application stakeholders priorities those activities keeping the cost factor in mind.*

Application Name:

* If all the questions below are all answered "No" then the application can be considered either "Least important" or "Not Recommended" for security assessment.

a) Does the application access any remote database or datafiles?	◯ Yes	◯ No
b) Does the application access any local database or datafiles?	◯ Yes	◯ No
c) Does this application open any ports for local or remote connections?	◯ Yes	◯ No
d) Does this application directly/indirectly make any remote connections?	◯ Yes	◯ No
e) Does this application require authentication for user access?	◯ Yes	◯ No
f) Does this application uses any role based access control (RBAC)?	◯ Yes	◯ No
g) Does this application query for confidential or private data locally?	◯ Yes	◯ No
h) Does this application process any direct or indirect user inputs to execute system critical processes or make any calls to system critical APIs that execute at higher priviledge level?	◯ Yes	◯ No

Evaluate

Status:

* If any one of the above question is answered "Yes" then then proceed to next page otherwise this application can be considered least important for any kind of security assessment. However in such scenario where all are answered "Yes" it is recommended to get it validated by your internal/external application security consultant to get their final opinion before you draw any conclusion.

Answer below questions to self determine the security activities required for the application

Application Architecture:

Deployment Type: ☐ Internet ☐ Intranet ☐ VPN / Dial-Up

Data type handled: ☐ Public ☐ Private ☐ Confidential / Restricted ☐ Secret / Top Secret

Business Criticality: ◯ Low Critical (0 - 3) ◯ Medium Critical (4 - 6) ◯ High Critical (7 - 9)

SDLC Phases	Design	Developement	Testing	Release
Security Activities	Threat Modeling	Static Code Review	Penetration Testing	Post-Release Audit
Importance				
Activity Weightage				

Check options below that are applicable for the application

☐ Application require authentication for user access

☐ Uses Role-based Access Controls (RBAC))

☐ integration with the enterprise identity management system (such as Directory Services, LDAP, Kerberos, etc.)

☐ Uses Web Services

☐ Handles sensitive data that requires encryption

☐ Application have a critical business impact if unavailable or down

☐ Authentication mechanism provide Single Sign-On to other applications

☐ Application provide a source of data to external applications

☐ Application query for confidential or private data locally

☐ Application extensively uses Web2 (e.g. AJAX)

☐ Access remote database or datafiles

☐ Access local database or datafiles

☐ Application open ports locally to accept remote or local network connections

☐ Application make direct or indirect remote network connections

☐ Requires higher priviledge level to run client side and make system critical api calls (e.g. syscall, WinExec)

Email d3basis.m0hanty@gmail.com for any clarifications or queries.

www.coffeeandsecurity.com
www.hackingspirits.com