# INFORMATION SECURITY ASSESSMENT TOOL
## *User Guide*

## Introduction
The following assessment document is designed to be downloaded and completed to measure the current information security capability maturity of your organization. Below are the step-by-step instructions for how to use this tool effectively.

## Step 1: Determine Your Level
This assessment document is designed for organizations of different sizes and with varying resources. Please use the following qualifying questions to establish the level of assessment that you should complete.

1. How many FTE's are dedicated to information security-focused job responsibilities?

   ☐ 0 or outsourced to third party (Level 1)
   ☐ 5 or less (Level 2)
   ☐ More than 5 (Level 3)

2. How many of these protections do you have?

   - Antivirus
   - Email security
   - Web traffic filtering
   - Password management
   - Installed and maintained firewalls

   ☐ 0 to 2 (Level 1)
   ☐ 3 (Level 2)
   ☐ 4 to 5 (Level 3)

3. Does your organization have comprehensive information security policies including technology acceptable use; access control (password and authentication); monitoring/detection and response; secure development; configuration and change management; awareness training and exercises; risk assessment; physical security; third party procurement; and systems hardening and protection?

   ☐ Minimal or none of the above (Level 1)
   ☐ Some of the above, but in need of updating (Level 2)
   ☐ Most of the above and updated at least yearly (Level 3)

This is your level based on your answers to the above questions:
- ☐ At least 2 out of 3 are a Level 1. Answer Level 1 questions in the *Information Security Assessment Tool*.
- ☐ At least 2 out of 3 are Level 2 or a combination of Level 1 and 2. Answer Level 1 and 2 questions in the *Information Security Assessment Tool*.
- ☐ At least 2 out of 3 are Level 3. Answer all questions in the *Information Security Assessment Tool*.

# Step 2: Rate Your Maturity

Once you have determined your level, you will then rate your maturity on all of the applicable questions in the *Information Security Assessment Tool*. All scoring is done using the capability maturity model guidelines outlined below.

## Maturity Rating Guide

**1 = Initial**
The starting point for use of a new or undocumented repeat process. Your organization has little or no procedures to manage this issue (chaotic, ad hoc, and individual heroics).

**2 = Repeatable**
The process or capability has at least been discussed and is at least documented sufficiently such that repeating the same steps may be attempted.

**3 = Defined**
The process is defined/confirmed as a standard business process and has begun to be accepted and used organization-wide.

**4 = Managed**
The process is quantitatively managed in accordance with agreed-upon metrics; accepted, encouraged and expected by management.

**5 = Optimizing**
Process management is inherent throughout the organization and includes deliberate, ongoing process optimization/improvement.

NOTE: Aspects of this tool are complex and detailed, requiring significant expertise in information security to make an accurate assessment. While your internal stakeholders may be able to do some or all of the assessment, bringing in an objective third party with specific expertise in information security risk assessments may provide you with a more valuable and actionable outcome.

As you or your assessor score this assessment, please ensure you have as much information as possible from the correct subject matter experts in order to assign an objective score.

# Step 3: Create an Information Security Plan

When you have completed the assessment, it should be used to develop strategic planning toward attainable goals that will increase your organization's information security capability maturities.

To do so, start with the Level 1 questions and note any that have low maturity scores. Prioritize these using risk management methodology (e.g. based on your organization's resources and the level of impact to your core business should these particular procedures continue in their current state).

If applicable, move on to the Level 2 and 3 questions, again prioritizing them using risk management methodology.

## Maturity Rating Guide

**1 = Initial**
The starting point for use of a new or undocumented repeat process. Your organization has little or no procedures to manage this issue (chaotic, ad hoc, and individual heroics).

**2 = Repeatable**
The process or capability has at least been discussed and is at least documented sufficiently such that repeating the same steps may be attempted.

**3 = Defined**
The process is defined/confirmed as a standard business process and has begun to be accepted and used organization-wide.

**4 = Managed**
The process is quantitatively managed in accordance with agreed-upon metrics; accepted, encouraged and expected by management.

**5 = Optimizing**
Process management is inherent throughout the organization and includes deliberate, ongoing process optimization/improvement.