**Overview**

Supply Chain Risk Management is common challenge for organizations and as many fight to keep their supply chain under control we often look for more effective ways to assess risk being introduced into the environment.  To address this challenge the Supply Chain Risk Assessment (SCRA) tool was created to assist organizations in identifying, evaluating and reporting risk within the supply chain process.

SCRA was developed with the following goals in mind:

* The foundation of the tool must be based on a common framework.
* There must be a cross walk for the questions defined to other standards/regulations.
* Remove the ambiguity in vendor responses.
* Eliminate the subjectivity in the scoring process.
* Provide an efficient way to identify gaps in the vendor response.
* Map assessments results to the tolerance levels defined by leadership.
* Offer an Executive Summary of the assessment.
* The tool must be macro/script free.

**Assessment Process**

Before we jump into the tool lets quick walk through the assessment process (your process may be different):

1. The initial request for new or change of technology is submitted by the customers Application Team/Business Unit, once complete the Technology Assessment Questionnaire is routed to the vendor.
2. The vendor will complete the multiple-choice questionnaire and return the results back to the customer.
3. The customers Security Team will assess the vendors response and summarize the results within the tab labeled “Assessment Summary”, this report will highlight the data value being handled by the solution, the risk exposure (impact/likelihood of a threat event) and whether the security controls implemented by the vendor meet the risk appetite defined by customers leadership.
4. The customers Security Team will present their findings to the customers Application Team/Business Unit, any gaps identified and/or guidance as to how the solution should be deployed within with the environment will be addressed at this time.
5. Results of the assessment are formally documented with the central Governance, Risk & Compliance (GRC) tool. Any gap identified in the prior step will be added to the risk register, prioritized by the Security Team and assigned to the Application Team/Business Unit for remediation.  If the assessment results fall within the tolerable levels of the organization the solution may at this point advance to Step 8 in the process (Approved for Use).  NOTE: it is suggested that the customers Application Team still work on developing a plan to address any gap in the long-term strategy of the solution.  If the assessment results however fall outside the tolerable levels of the organization the solution must move to Step 6 in the process (Remediation Phase) as it is not approved for use until gaps are addressed and risk is driven to an acceptable level.
6. The customers Application Team/Business Unit will establish a remediation plan to address the gaps identified (working with the vendor if needed). If the gaps are remediated and risk is reduced to a tolerable level the risk register is updated within the GRC tool and the request is moved to Step 8 of the process (Approved for Use).  If the gaps cannot be remediated to an accepted level (due to financial constraints, technology challenges, etc.) and the solution is still critical to the environment the Application Team/Business Unit will need to prepare a business case to be reviewed and the inherit risk accepted by the customers Leadership team before it can be advanced to Step 8.
7. The customers Leadership team will review the business case documented and decide whether to accept the residual risk which would advance the assessment process to Step 8 (Approved for Use) or reject the request which would halt any further movement of the project.
8. The solution is approved for use, the customers Security team is to remain involved during the planning, development, testing and implementation phases to ensure no additional risk is introduced.
9. Once the solution has been implemented it is to be re-assessed/evaluated on a regular basis, the customers Security team will create a reminder to trigger an event at the time defined within organizations policy.

**Assess Questionnaire**

This workbook contains the following worksheets (tabs):

* **Vendor Questionnaire** – This is one of the primary tabs within the workbook and will be used to collect information from your internal teams as well vendor direct. Ideally, this should be the only tab visible by default, no one but the security practitioner needs access to the other tabs noted below.
  + This worksheet is broken up into three sections.
    - The first is to be completed by your internal team and includes several sub-sections:
      * **Technology Request** – The section covers your basic information, Solution Name, Internal Project #, Department/Cost Center.
      * **Point of Contacts** – This section will be used to keep record of the key players for the project.
      * **Solution Profile** – This section helps us understand the type of technology being presented (is it new or existing tech being upgraded), we’re also looking to capture the target audience and this is a required field that will be used later to determine our overall Impact level.
      * **Data Classification** – As with any solution it’s important to capture the type of data that will be stored/processed by the technology, in this section we ask the requestor to identify the Information Types and desired Protection & Availability Levels. I’ve provided a legend (directly below this section) to aid in making your selections.  NOTE: It is required that at least one Type of data be defined and included expected Protection & Availability levels, this information will assist in determining our Impact level.
    - The second section is dedicated to the vendor and contains two primary sections:
      * **Vendor Profile** – This section is available for any general questions about the vendor or the service/product being assessed. NOTE: the responses to these questions do not currently have an impact on the overall scoring of the assessment.
      * **Technical Assessment** – This section contains a total of 104 multiple choice questions that are based on the Center of Internet Security (CIS) Top 20. All questions require a response and the vendor has the option to add comments (if desired).  The questions, along with other content that I’ll reference later, is directly pulled from the “Technology Master” tab so if any changes are needed those changes should be made within the Master sheet NOT the Vendor Questionnaire.
    - The third and final section is to be hidden by default but can be used as a reference for practitioners as it provides the Impact and Likelihood for each of the 5 Attack Scenarios identified.

*Screenshot of the Vendor Questionnaire tab*

* **Assessment Results** – Based on the responses received by the Vendor & Customers Application Team, this tab will summarize the following for the solution:
  + Data Value (Low, Medium, High)
  + Risk Exposure (Low, Medium, High)
  + Appetite Level (Unacceptable, Tolerable, Acceptable)
  + Summary of the Security Controls Assessed
  + Breakdown of Responses by Control Area
  + Gaps Identified in the Vendors Response
  + Potential Gaps where Customer is Responsible for Control Implementation

*Screenshot of the Assessment Results tab*

* **Guide** – Provides on overview on this tool as well as the expected process follow (which your welcome to modify).
* **Revisions**– Will display the change history of the tool as it matures.

*Screenshot of the Revisions Tab*

* **Technology Master** – This tab is critical to the overall workbook as it contains the total population of questions within the tool and it outlines how those questions are mapped back to various attributes, any changes to the questions (or attributes linked to these questions) should be made within this sheet as it will self-correct the Vendor Questionnaire tab.
  + Details on the columns defined and their purpose:
    - **Category**– CIS Controls V7 separates the controls into three distinct categories: basic, foundational, and organizational.
      * **Basic**– key controls which should be implemented in every organization for essential cyber defense readiness.
      * **Foundational**– these technical best practices provide clear security benefits and are a smart move for any organization to implement.
      * **Organizational**– are more focused on people and processes involved in cybersecurity.
    - **Control #**- This column is linked to the actual question number that will appear in the Vendor Questionnaire tab.
    - **CIS Actual #**- This aligns to the actual CIS sub-control number (wording modified slightly) for each question.
    - **Control Focus**– CIS Controls V7 is made up of 20 control areas and each question is mapped to a control, they are:
      * Inventory of Authorized and Unauthorized Devices
      * Inventory of Authorized and Unauthorized Software
      * Continuous Vulnerability Assessment and Remediation
      * Controlled Use of Administrative Privileges
      * Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
      * Maintenance, Monitoring, and Analysis of Audit Logs
      * Email and Web Browser Protections
      * Malware Defenses
      * Limitation and Control of Network Ports, Protocols, and Services
      * Data Recovery Capabilities
      * Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
      * Boundary Defense
      * Data Protection
      * Controlled Access Based on the Need to Know
      * Wireless Access Control
      * Account Monitoring and Control
      * Implement a Security Awareness and Training Program
      * Application Software Security
      * Incident Response and Management
      * Penetration Tests and Red Team Exercises
* **Security Function**– The CIS framework is based on five primary pillars Identify, Detect, Protect, Respond and Recover. Each question is mapped back to one of these areas.
* **Control Question**– This column contains the actual question that would appear on the Vendor Questionnaire tab.
* **Data Value (High, Medium, Low)**– The questions documented may be viewed differently by an organization based on the type of data being handled or by impacted audience, with that said this tool was built to allow a practitioner to tag which questions they feel are REQUIRED & RECOMMEND.
  + REQUIRED EXPLAINED: if this option is selected it is expected that the vendor have the necessary control in place (answer YES) should they answer NO then points will be deducted from their overall score and enough negative points may push the solution outside the tolerance allowed by the organization.  NOTE: by answering Customer Responsibility will neither hurt or help the vendor but it does provide awareness to the customer that they’re on the hook for addressing said control.
  + RECOMMEND EXPLAINED: if this option is selected it means a response of YES by the vendor will be viewed as a compensating control and depending on the Security Function of that question additional points will be added to the overall assessment.  The response of anything else will neither hurt nor harm the vendor.
* **Response Options**– The goal when building this questionnaire out was to establish an effective yet efficient way to assess responses, to do this all questions were configured with a multiple-choice response. The three options are YES, NO and CUSTOMER RESPONSIBILITY, details below:
  + "YES" - the VENDOR acknowledges responsibility for the control/process AND it is included within the service offering.
  + "NO" - the VENDOR acknowledges responsibility for the control/process AND it is NOT included within the service offering OR does not meet the criteria defined.
  + "CUSTOMER RESPONSIBILITY" - You the vendor are providing a commercially available solution and its owner's responsibility to implement said control/process.
* **NIST Policy Reference**– Each of the applicable control questions were mapped back to a NIST 800-53 control/s. Details on how this was accomplished can be found under the NIST MAP tab.
* **HIPAA Reference**– Each of the applicable control questions were mapped back to a HIPAA Regulation. Details on how this was accomplished can be found under the HIPAA MAP tab.
* **PCI Reference**– Each of the applicable control questions were mapped back to a PCI Control area. Details on how this was accomplished can be found under the PCI MAP tab.
* **Risk Statement**– A pre-canned risk statement has been documented for each control question. This statement can be modified by the practitioner and will display within the Assessment Results tab for any non-conforming control identified.
* **Comments**– This column has no bearing on the overall outcome of the solution, it can be used to record notes regarding any of the questions documented. This may be helpful if you have multiple practitioners collaborating within the tool.
* **Control Guidance**– This column is a place marker for a future add-on, as gaps are identified the goal here is to provide guidance on a potential solution that could be implemented to address the issue.
* **Attack Summary Mapping**– There are five attack scenarios that are defined and within scope for every assessment (see below). Each of the 104 questions defined within the Technical Assessment have been mapped back to one Attack scenario, while it’s possible that a question may be attributed to multiple scenarios for the intent of this tool the practitioner must choose only one (this can be done by modifying Column Q of this worksheet).
  + The five scenarios are:
    - Cyber Attack
    - Unauthorized Access to Systems or Data
    - Human Error (User, Maintenance, Operation)
    - System Failure (Hardware, Software, Communication, Power, etc.)
    - Environmental Disaster (Fire, Water, Natural Disaster, Terrorism)
  + NOTE: The Attack scenarios results can be found (and overridden) under the Vendor Questionnaire tab, you’ll need to scroll down and unhide Rows 186-206 within the sheet.  Presently the Impact level for each scenario will be the same as this is determined by *Data Value \* Audience*, the assumption was made that those two attributes will not change as it is challenged by each scenario.  This again can be manually overridden by the practitioner (if needed).

*Screenshot of the Technology Master tab*

*Screenshot of the Attack Summary table under the Vendor Questionnaire tab*

* **Risk Calc** – This tab is also critical to the overall workbook as the information that is defined within here will determine the grading scale for how the solution is assessed. The Risk Calc worksheet is broken up into three sections… Data Value Calculation, Risk Exposure Calculation and Risk Appetite Calculation, each are explained in further detail below.  NOTE: Throughout this worksheet practitioners are encouraged to work with their leadership to ensure the values defined in RED align with views and expectations of the organization.
* **Data Value**– (*Protection \* Availability).*If there are multiple data types identified for the solution with various protection and/or availability levels the tool will calculate and use the greatest value (see Final Conclusion in this section).
  + **Protection**is broken down into four categories:
    - P1 - Public
    - P2 - Internal Data
    - P3 - Sensitive
    - P4 - Highly Sensitive
  + **Availability** is broken into four categories:
    - A1 - Minimal
    - A2 - Low
    - A3 - Moderate
    - A4 - High
* **Risk Exposure –***(Impact \* Likelihood).* Obviously, each attack scenario will display a different level of risk, the table to the far right in this section (labeled Final Conclusion) will run a calculation of all scenarios and determine the greatest risk area and use that in our report section.
  + First to calculate **Impact** we multiply *(Target Audience \* Data Value)* which will return a result of Insignificant, Moderate or Significant.
    - **Data Value** is pulled from the prior section.
    - **Target Audience** is broken into five categories:
      * Small group of users
      * Single department
      * Campus
      * Entire organization
      * Patients/General Public
  + Next we need to calculate our Likelihood, to get this information we sum up the responses of all questions by attack scenario. The first part in this is to calculate the compliance percentage of all questions identified as REQUIRED, we then we credit the vendor additional points for any RECOMMEND control (aka Compensating Control) to come up with our final percentage.  Listed below this area is a table that defines our thresholds for what is viewed as **Almost Certain**, **Possible** and **Rare**.
  + Finally to calculate Risk Exposure we multiply *(Impact \* Likelihood*).
* **Risk Appetite –** *(Data Value \* Risk Exposure)*. In the final section of this worksheet the practitioner (working with leadership) will define the tolerance levels of the organization, once that has been established there will be a clear path in how we disposition the assessment.
  + There three levels are:
    - **UNACCEPTABLE**- Risk cannot be justified except in extraordinary circumstances.
    - **TOLERABLE**- Residual risk is tolerable only if further risk reduction is impracticable. Extraordinary cost and effort would be required and would only marginally reduce the risk.
    - **ACCEPTABLE**- Risks are negligible or so small that can be managed by routine procedures and no additional risk measures are needed.

*Screenshot of the Risk Calc tab*

* **Customer Gap Calc** – This tab is calculating the questions where the vendor has responded CUSTOMER RESPONSIBILTY to a question, all the CUSTOMER RESPONSIBILTY’s are filtered, sorted then presented into the Assessment Result tab under the “Controls Customer is Responsible in addressing”.

*Screenshot of the Customer Gap Calc tab*

* **Vendor Gap Calc** – This tab is calculating the questions where the vendor has responded NO to a question, all the NO’s are filtered, sorted then presented into the Assessment Result tab under the “Controls Gaps Identified in Vendor Response”.

*Screenshot of the Vendor Gap Calc tab*

Additional Resources/Tabs within this workbook:

* **Why CIS Top 20** – This tab provides some basic information on CIS Top 20 and its importance.
* **NIST Map** – An aggregate of resources was used to build out this tab.
* **HIPAA Map** – An aggregate of resources was used to build out this tab.
* **PCI Map** - An aggregate of resources was used to build out this tab.

Special thanks to the following entities (see below), content from their website was used as an aid to build this questionnaire:

Cisecurity.org, AuditScripts.com, HHS.gov, Cisa.gov, and the Security Team at UC Irvine.