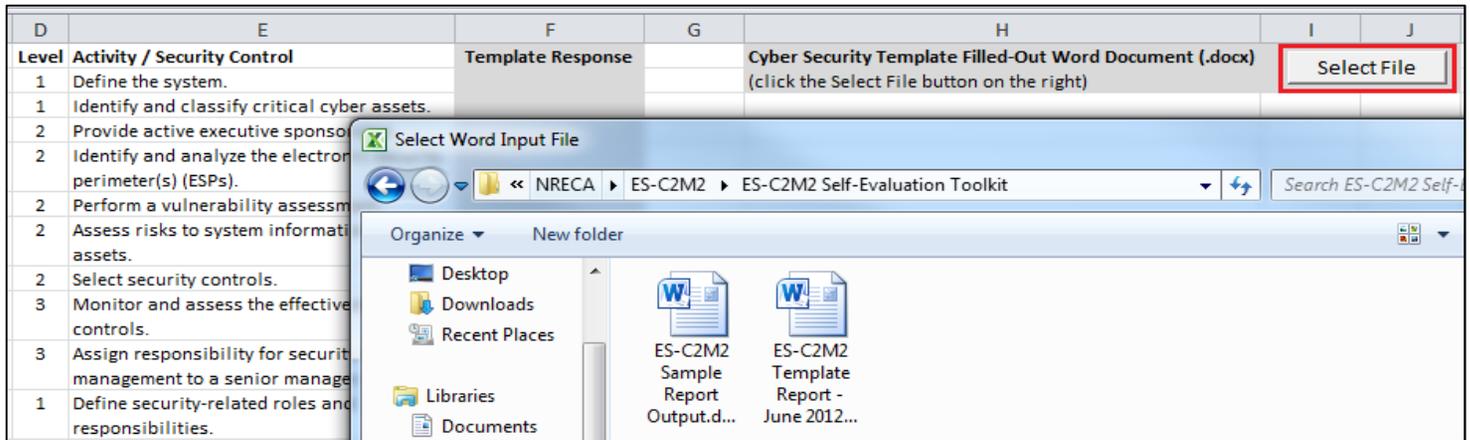
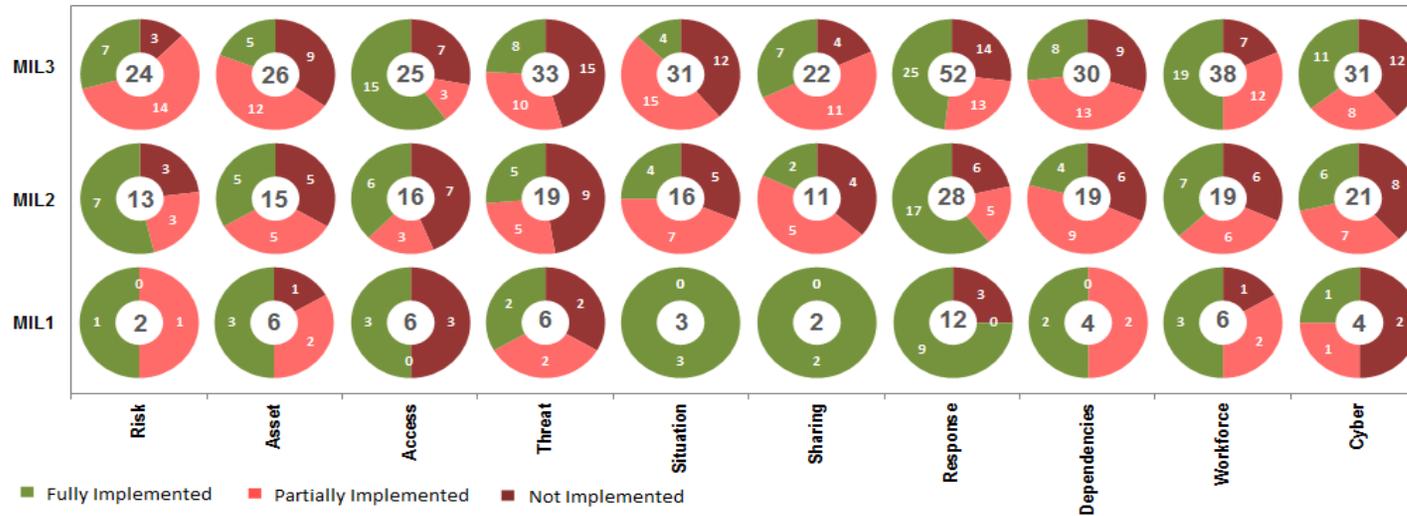


# Cyber Security Template Scoring Worksheet - Instructions

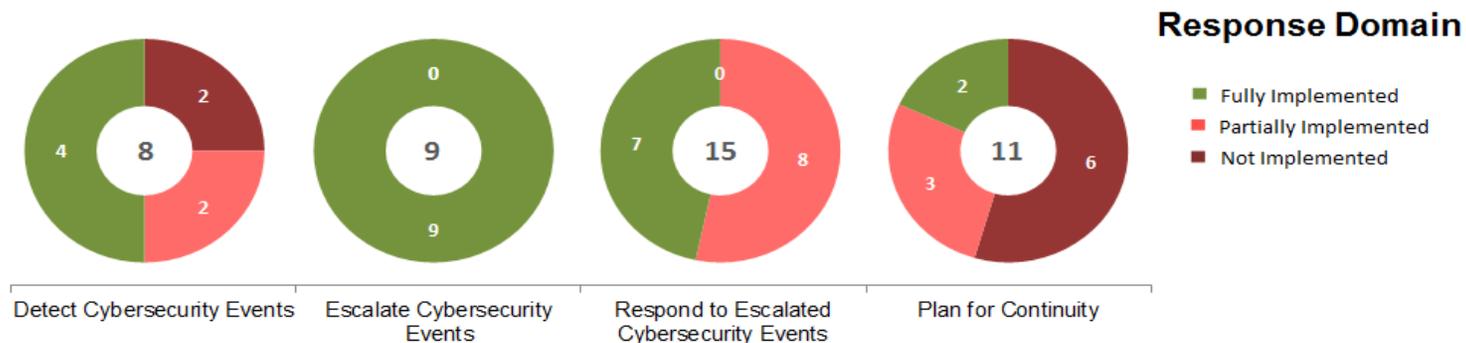
1. Completely fill out the template document by selecting Yes, No, or Partial for each Activity listed in the tables below, then save the document.
2. Open this Cyber Security Template Scoring Worksheet, making sure to enable Excel macros if prompted (check for a yellow bar across the top).
3. In the CS Template tab, click the Select File button at top right, then select the Word document that contains the filled-out template, as shown below.



4. If the data imported successfully, you will see all of the template responses filled into column F in the CS Template tab. If you receive an error message, refer to the details in the message and make sure that neither the reporting spreadsheet nor the template have been structurally altered.
5. Review the scoring results in the ES-C2M2 Objectives and ES-C2M2 Domains tabs, which can be directly compared to the Objective and Domain tabs in the ES-C2M2 Report Builder spreadsheet or to a full ES-C2M2 report.



6. The “donut charts” above essentially show how close the organization is to achieving each of the maturity levels (MIL1-3) in each of the 10 ES-C2M2 domains. For example, the circle on the very top left indicates that at MIL3 in the Risk domain, there are 24 total activities, and out of these, 3 are not implemented, 14 are partially implemented, and 7 are fully implemented. For detailed instructions on interpreting these results and charts, please refer to the ES-C2M2 materials (available at <http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model>), including the section titled “Using the Model” (see p. 48). The worksheet also produces charts organized by objective, showing a donut chart for each objective within a domain. The example below shows the Response domain objectives.



7. Note: There are two important differences to consider when comparing scoring output:

a. This template uses a three-item scale (Yes, No, Partial) to determine the organization's level of implementation, while ES-C2M2 uses a fourth item ("Largely Implemented") in its scale, which can sometimes be open to interpretation. Since the template does not use this concept, all items are mapped to the three corresponding levels in ES-C2M2:

i. Yes – Fully Implemented

ii. Partial – Partially Implemented

iii. No – Not Implemented

b. Since this template does not explicitly score the "Manage DOMAIN Activities" objectives in each ES-C2M2 domain, these are not reflected in the Objectives tab.

*For additional instructions, please refer to the "Using the Template" section in the Cyber Security Plan Template document, pages 5-8.*