Defense Industrial Base (DIB) Sector Coordinating Council (SCC) Supply Chain Cyber Training

Cyber/Cybersecurity Maturity Model Certification (CMMC) v2.0

CyberAssist

Agenda

- Module 1: Cybersecurity: Why it is Important?
- Module 2: Cybersecurity Maturity Model Certification
- Module 3: Assessment Process - Interim
- Module 4: Incident Reporting
- Module 5: Cybersecurity Best Practices
- Module 6: Risk Management and Assessing Risk
- Resource Guide: Glossary, Acronym Guide and Resources for Additional Information
- CMMC Domains
- Survey

Risk Management and Assessing Risk

Module 6

Disclaimer and Overview

Note: CMMC is still going through the rule-making process and certain aspects and requirements may change. Refer to the *Resources Guide* provided in this training for the most updated information.

- The intent of this training is to build awareness for Defense Industrial Base (DIB) suppliers of the likely requirements of the Cybersecurity Maturity Model Certification (CMMC) and their obligation to meet FAR 52.204-21 (basic cyber hygiene) and DFARS 252.204-7012 (specialized data handling and protection requirements).
- This training is self-paced and intended for a range of roles and responsibilities including, but not limited to, executives, project managers and technical staff from organizations seeking certification (OSC) and need to comply with CMMC. Currently, CMMC does not apply to any contractor.
- Note: Completion of this training DOES NOT certify your organization. This training is intended for the purposes of providing awareness of the subjects outlined above.
- The DIB Sector Coordinating Council (SCC) Supply Chain Task Force does not take responsibility for suppliers' certification by the CMMC 3rd Party Assessment Organization (C3PAO).
- This training focuses on U.S. regulations and industry best practices:
  - U.S. Department of Defense (DoD) Chief Information Officer (CIO) Cybersecurity Maturity Model Certification (CMMC) Information
  - National Institute of Standards & Technologies (NIST) publications
  - National Archives & Records Administration (NARA) definitions
  - DIB SCC Supply Chain Task Force – CyberAssist website

Module Topics and Objectives

Helpful Hint:
Refer to the Resource Guide for a Glossary and Acronym Guide

Topics covered in this module:

- Risk Management 101
- Risk Identification
- Risk Evaluation and Measurement
- Risk Control Management and Implementation
- Risk Management Key Points

The objectives of this module are:

- Provide understanding of risk management;
- Provide understanding of risk identification; and
- Provide understanding of risk control management and implementation.

A legend has been provided to assist with determining the content that you will need to know for each of the CMMC levels and what is additional content that will assist your organization with your cybersecurity posture. The corresponding symbol will be located at the top left corner of the slide.

Content Legend

= CMMC L1 Content
= CMMC L2 Content
= CMMC L3 Content
= Non-CMMC Content/Extra

CyberAssist

Risk Management 101

- Risk management applies to many aspects of a business.
  - Internal risks (weaknesses) - controllable
  - External risks (threats) – typically uncontrollable
  - Negative (weaknesses and threats)
  - Positive (opportunities)
- The ultimate goal is to minimize the effects of risks on your business.
  - Business continuity
  - Greater stability
  - Better cash flow
  - Longevity
- Stages of Risk Management
  - Risk Identification
    - Internal vs. External Risks
  - Risk Evaluation
  - Risk Measurement
  - Risk Control Management and Implementation

Risk Identification

- Internal Risks
  - Employee Risks
    - Illness and death
    - Theft and fraud
    - Low employee morale
    - Personal conflicts
    - Complacency
    - Insider threat
  - Equipment and Information Technology Risks
    - Old equipment
    - Patching
    - Cybersecurity
  - Other
    - Other technologies such as phones
    - Injuries and damage to business
    - Cash flow
    - Visibility
- External Risks
  - Competition and Market Risks
    - Market changes
    - Loss of employees
    - Rent increase
  - Business Environment Risks
    - Laws and ordinances (federal, state, local)
    - Weather and natural disasters
    - Community changes
    - Visibility
  - Non-Employee Risks
    - Unprovoked violence
    - Theft of goods and services
    - Malicious Cyber Threat Actor

Risk Evaluation and Measurement

- Evaluate SWOT (Strengths, Weaknesses, Opportunities, Threats)
- Identify Warning Signs
  - Excessive debt to equity ratio
  - Reliance on small number of customers, products, vendors
  - Cash flow issues
  - Irregularities in records (timekeeping, accounting, bank)
  - Irregularities in reports (computers, users)
  - High turnover rate
- Risk Measurement
  - Likelihood vs impact

Risk Control Management and Implementation

- Equipment
- Vendors
- Business Continuity
- IT Systems
- Competition
- Accounting and Cash Flow
- Employee Management
- Business Work Strategy
- Exit Strategy

Risk Management Key Points

1. Risks associated with a small business, or any business, can be characterized as internal or external.
2. Begin assessing risks by listing events or resources that could impact continued operations and cash flow.
3. The costs to insure or minimize risks should be weighed against the potential impact of the risk.
4. A business continuity plan should be part of your overall business plan.
5. Strategies to avoid risks can include: communication, setting expectations, support systems, staff training, insurance, risk assessment, and contingency planning.
6. Be honest in reviewing your business for risk and know the warning signs.
7. Seek assistance from others.
8. Include an exit strategy in your initial business plan and revisit that strategy from time to time.

Note: For more information on risk management, there is a free NIST training course (approximately three hours): Risk Management Framework for Systems and Organizations Introductory Course

Module Summary

- **Ultimate goal on Risk Management:** To control the effects of risks on your business
- There are four stages for Risk Management:
  - Risk Identification
  - Risk Evaluation
  - Risk Measurement
  - Risk Control Management and Implementation
- Risks associated with business can be characterized as internal or external