

WELCOME TO THE RADICL CMMC TOOLKIT

CMMC compliance is critical for businesses in the Defense Industrial Base, but navigating the complexities can be challenging, especially for small and medium-sized companies.

That's why we created these templates – to simplify the process and help you improve your cybersecurity posture and achieve CMMC compliance with ease. This toolkit provides you with over 25 templates designed specifically for SMBs in the DIB. These resources will guide you through the necessary steps to meet Level 1 CMMC requirements efficiently and effectively.

VICTOR CICH, REGISTERED PRACTITIONER & COMPLIANCE CONSULTANT, RADICL

HOW TO USE THIS TOOLKIT

- **IDENTIFY YOUR NEEDS:**
Browse through the categories and determine which areas of compliance your organization needs to address.
- **DOWNLOAD TEMPLATES:**
Click on the templates you need to download them. Each template is available in an editable Word format.
- **CUSTOMIZE:**
Tailor each template to fit your specific organizational needs and requirements.
- **IMPLEMENT:**
Use the templates as part of your CMMC compliance strategy, ensuring all necessary policies and procedures are in place.

TABLE OF CONTENTS



- 1 PHYSICAL ACCESS AUTHORIZED PERSONNEL TEMPLATE**
PE.L1-3.10.1 Objective [a], [c]
- 2 PHYSICAL SECURITY POLICY**
PE.L1-3.10.1 Objective [a], [b], [c], [d]
PE.L1-3.10.3 Objective [a]
PE.L1-3.10.4 Objective [a]
PE.L1-3.10.5 Objective [c]
- 3 VISITOR LOG TEMPLATE**
PE.L1-3.10.4 Objective [a]
- 4 PHYSICAL ACCESS DEVICE INVENTORY**
PE.L1-3.10.5 Objective [a]
- 5 AUTHORIZED PUBLIC POSTING TEMPLATE**
AC.L1-3.1.22 Objective [a]
- 6 PUBLICLY POSTING INFORMATION POLICY**
AC.L1-3.1.22 Objective [b], [d], [e]
- 7 PUBLICLY POSTED CONTENT LOG TEMPLATE**
AC.L1-3.1.22 Objective [d]
- 8 DATA RETENTION AND DISPOSAL POLICY**
MP.L1-3.8.3 [a], [b]
- 9 AUTHORIZED DEVICES TEMPLATE**
SI.L1-3.14.2 Objective [a]
IA.L1-3.5.1 Objective [c]
AC.L1-3.1.1 Objective [c]
- 10 CONNECTIONS TO EXTERNAL SYSTEMS TEMPLATE**
AC.L1-3.1.20 Objective [a]
- 11 CONNECTIONS FROM EXTERNAL SYSTEMS TEMPLATE**
AC.L1-3.1.20 Objective [b]
- 12 ACCESS CONTROL AND TERMINATION POLICY**
AC.L1-3.1.2 Objective [a],[b]
IA.L1-3.5.1 Objective [a]
IA.L1-3.5.2 Objective [a], [b]
AC.L1-3.1.1 Objective [d]
- 13 SYSTEM USER ACCOUNTS TEMPLATE**
IA.L1-3.5.1 Objective [a]
- 14 AUTHORIZED PROCESSES TEMPLATE**
IA.L1-3.5.1 Objective [b]
IA.L1-3.5.2 Objective [b], [c]
AC.L1-3.1.1 Objective [b]
- 15 RESOURCES NOT REQUIRING AUTHENTICATION TEMPLATE**
IA.L1-3.5.2 Objective [a]
- 16 AUTHORIZED USERS INVENTORY TEMPLATE**
AC.L1-3.1.1 Objective [a]
- 17 ACCESS CONTROL LOG TEMPLATE**
AC.L1-3.1.1 Objective [d]
- 18 AUTHORIZED ADMINISTRATIVE ACCESS TEMPLATE**
AC.L1-3.1.1 Objective [d]
- 19 RADICL CMMC LEVEL 1 SSP**
Practice: Showing the value of our Level 2 template
- 20 PERSONAL SOCIAL MEDIA SECURITY POLICY TEMPLATE**
Not a physical template, but links to publicly posting information policy

TACKLE CMMC COMPLIANCE WITH EASE USING RADICL'S INNOVATIVE SOLUTIONS

Why struggle with the complexities of CMMC compliance when RADICL can streamline the process for you? Our Xtended Threat Protection platform not only simplifies compliance but also addresses the most challenging and cost-intensive requirements of the CMMC framework. With RADICL, you gain access to:

- **XTENDED THREAT PROTECTION:**
Leverage this powerful platform designed to meet high-cost CMMC requirements efficiently, ensuring your cybersecurity defenses are robust and compliant.
- **COMPLY MODULE:**
Our automated module simplifies the NIST 800-171 / CMMC assessment and remediation process, guiding you step-by-step and cutting through the complexity of compliance.

Forget the hassle of managing compliance on your own. RADICL is here to equip you with cutting-edge tools and expert guidance. Reach out to discover how our solutions can make CMMC compliance straightforward and stress-free.

CONTACT US NOW



<https://radicl.com/lp-lets-talk-now>