LAKE RIDGE

INCIDENT RESPONSE
TABLETOP EXERCISE WORKBOOK

Why this is important

By testing your incident response capability, you identify any weaknesses in your incident response plan. This helps you improve your incident response plan in preparation for a real incident. One method for testing your incident response plan is to use “tabletop exercises.”

What is a Tabletop Exercise?

According to the NIST glossary, a tabletop is “a discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.”

EXERCISE INFORMATION

Date of Exercise:

Exercise Lead & Title:

Exercise Participants & Job Roles:

SCENARIO 1: LOST USB DRIVE

Scenario:

John is a VP at ACME. The company prohibited the use of removable storage devices on all computers with the exception of a few employees who have a valid business need. One of the users with the exception was John. John is supposed to use an encrypted USB drive; however, John was recently using an unencrypted device to store company data. After a business trip, John noticed that he had lost his USB drive. John immediately reported the lost USB drive to ACME's incident response team.

Discussion Questions:

As the incident response team, what is the first action you would take?

What is our organization's policy on removable storage devices?

What security controls do we have in place to restrict the use of removable storage devices?

What could have been done to prevent the incident involving John?

SCENARIO 2: COMPROMISED USER ACCOUNT

Scenario:

Adam received a phishing email asking him to reset his Microsoft 365 password. The email appeared to come from Microsoft. Adam clicked the link and entered his old and “new” password on the form. Adam later noticed that his “new” password was not working so he contacted IT and informed them that he had just reset his password. IT checked the password reset logs and discovered that the password was not recently reset. Adam explained that he received an email where he clicked a link and “reset” his password. IT informed Adam that it was a phishing attack.

Discussion Questions:

As the incident response team, what actions would you take to contain and recover from this incident?

What actions can we take to prevent this incident from occurring again?

SCENARIO 3: UNAUTHORIZED ACCESS - PIGGYBACKING

Scenario:

Sarah was entering the office using her keycard, behind her was a man carrying several boxes of donuts. He was not wearing a company provided badge. Sarah politely held the door open for him to enter the office. About 10 minutes later, the facility security officer noticed the man in the IT wiring closet. When asked who he was and why he was there, the man was unable to provide an adequate response and was escorted out of the building. Upon reviewing security camera footage, it was discovered that he entered the building using the piggybacking social engineering attack against Sarah.

Discussion Questions:

As the incident response team, what actions would you take to respond to this incident?

How can we better prepare users for this type of attack?

Do we have sufficient physical security controls in place to prevent these types of incidents?

SCENARIO 4: UNAUTHORIZED CONFIGURATION CHANGE

Scenario:

Bill is the system administrator at ACME. This morning the helpdesk received a few requests to share OneDrive files externally. Currently, OneDrive files can only be shared with whitelisted domains. To “resolve” the tickets, Bill adjusted the SharePoint/OneDrive file sharing settings to allow file sharing with anyone. Upon reviewing various logs and reports, Doug, ACME’s cybersecurity analyst noticed that files were being shared with unauthorized external users.

Discussion Questions:

What policy did Bill violate?

How should the incident be handled?

What should we do with Bill?

Do we have sufficient security controls in place to prevent these types of incidents?

SCENARIO 5: USE OF UNAUTHORIZED CLOUD STORAGE

Scenario:

James is working with a customer and needs to share a large company document with them. He tried to share it with them using his company OneDrive, but the customer's domain is not whitelisted in SharePoint/OneDrive. James decides to upload the company document to his personal Google Drive and shares it with the customer.

Discussion Questions:

What did James do wrong?

Do we have a policy preventing personnel from using unauthorized cloud storage?

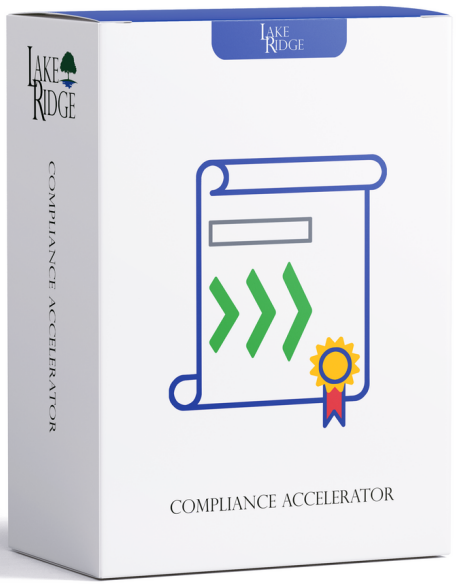
How do we respond to this incident?

What can we do to prevent the incident from reoccurring?

LAKE RIDGE

COMPLIANCE ACCELERATOR

Your NIST SP 800-171 &
CMMC 2.0 Solution



Compliance Accelerator Makes It Easy

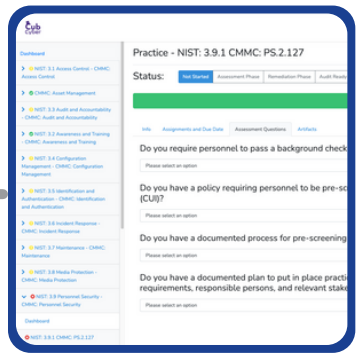
MEET YOUR DFARS REQUIREMENTS & STAY COMPLIANT

"This app put into perspective and laid out exactly what we needed to do to become NIST compliant."
Christopher Davis, IT Manager at InnovaPrep

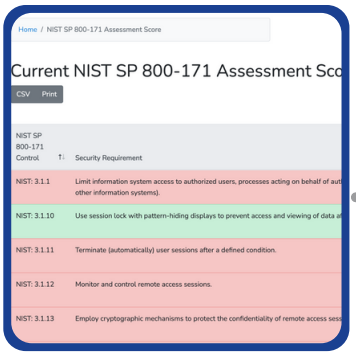
- 252.204-2008 Compliance with Safeguarding Covered Defense Information
- 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
- 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements
- 252.204-7020 NIST SP 800-171 DoD Assessment Requirements

NON-COMPLIANT

PERFORM THE SELF-ASSESSMENT



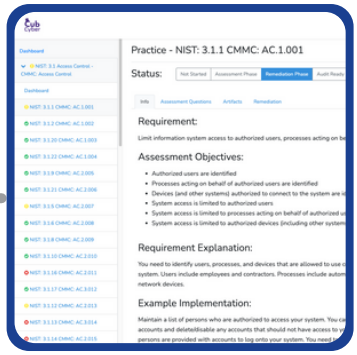
GENERATE THE SUMMARY LEVEL (SPRS) SCORE



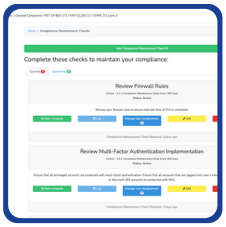
GENERATE THE POA&M

GENERATE THE SYSTEM SECURITY PLAN

IMPLEMENT PLAN



MAINTAIN COMPLIANCE



COMPLIANT

LAKE RIDGE

Everything You Need

- ✓ SPRS Score
- ✓ System Security Plan
- ✓ Plan of Action & Milestones
- ✓ Assessment Report
- ✓ Gap Remediation
- ✓ Policy & Procedures Documents
- ✓ Compliance Maintenance

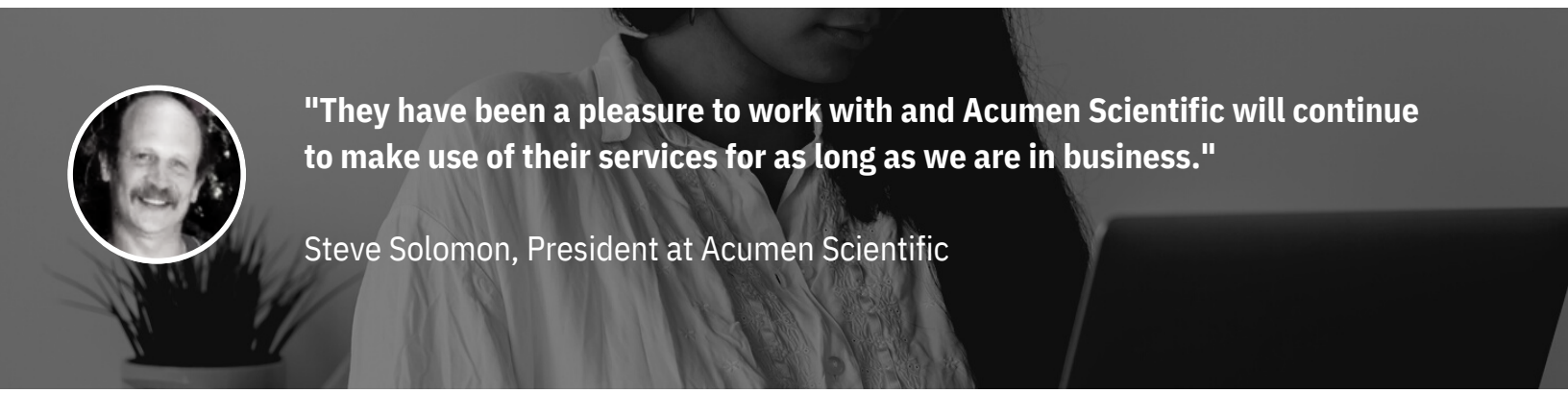
"I like how the app simplifies the ask of each question. This is helpful for non-IT employees to understand."
Teresa Vanderford, Facility Security Officer at EchoFive Group

"The app helped us tremendously! We were able to go into the audit with heightened confidence because we had internally assessed our efforts using the tool...This confidence in turn was then seen by DCMA auditors who appreciated our preparedness and attention to detail given NIST 800-171 compliance."
Mahvash Shah, VP at Sunrays International

Real Customer Support

- Initial on boarding call
- Quarterly check up calls by a cybersecurity professional
- We are always happy to answer questions about compliance requirements

Certified Support Staff



"They have been a pleasure to work with and Acumen Scientific will continue to make use of their services for as long as we are in business."

Steve Solomon, President at Acumen Scientific

TRUSTED BY THE INDUSTRY

UNIVERSITY OF
South Carolina

"I would highly-recommend this product for any business trying to achieve compliance."
Tonyia Bellina - *Sr. Director Projects & Strategic Planning, Mereo 4*

AS SEEN ON

Daily Herald

FOX 40

DIGITAL JOURNAL

"App is very easy to use and very straight forward. I have seen many apps in searching for a company to work with, the Lake Ridge app was by far easier to use."

Chris Clark, VP at EOS-AV

LAKE RIDGE

Sign Up

Book a Call

lakeridge_us

www.lakeridge.us

info@lakeridge.us