NIS2 CYBER CRISIS MANAGEMENT

MAPPING EU NIS2 TO THE CYBER CRISIS MANAGEMENT CERTIFICATION SERIES

CYBER CRISIS MANAGEMENT
PLANNING PROFESSIONAL (C^2MP^2)
CYBER SECURITY TRAINING & CONSULTING LLC

CYBER CRISIS MANAGEMENT
EXERCISE PROFESSIONAL (C^2MEP)
CYBER SECURITY TRAINING & CONSULTING LLC

CYBER CRISIS MANAGEMENT
LEADERSHIP PROFESSIONAL (C^2MLP)
CYBER SECURITY TRAINING & CONSULTING LLC

5 TRAINING DAYS | 3 CERTIFICATIONS

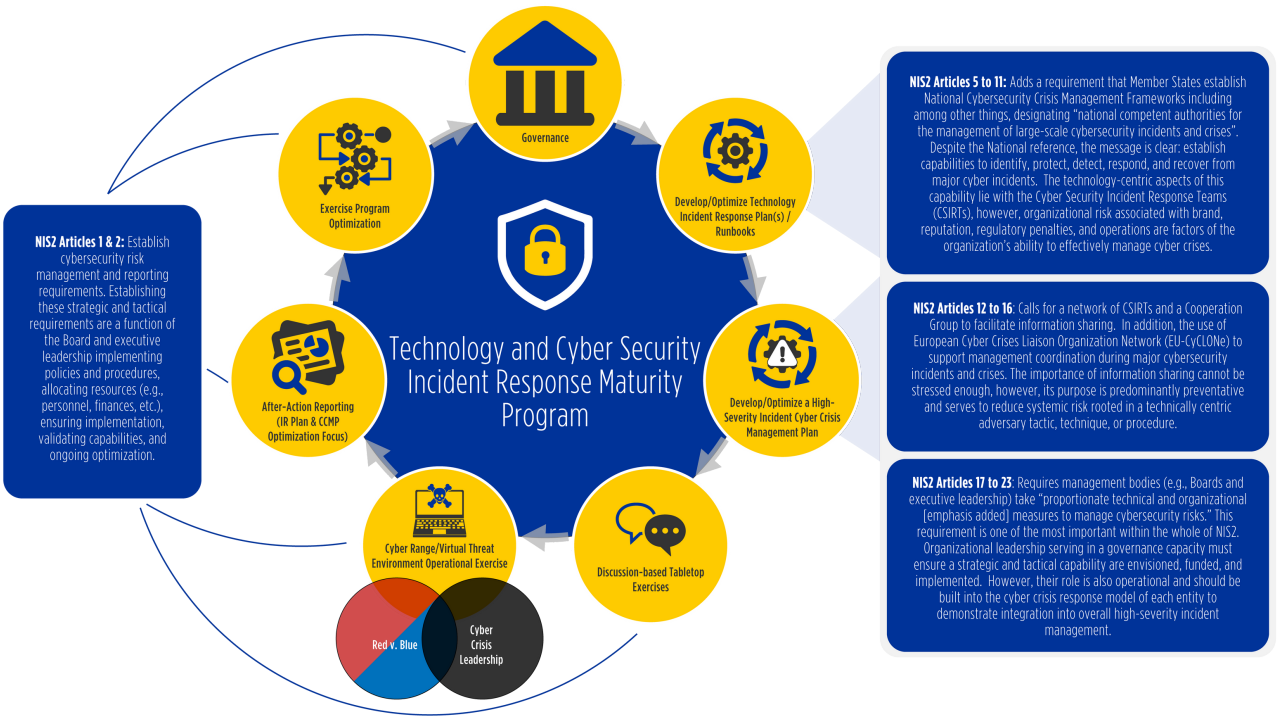
REDUCE RISK, INCREASE RESILIENCE

Cyber crisis management encompasses the broad spectrum of prevention, mitigation and incident response, and institutional learning and involves both public and private sectors.

From the perspective of cyber crisis management, the tone is set at the outset under NIS2 *(Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148)* with Articles 1 and 2 calling for each Member State to establish a national cybersecurity strategy, designate national authorities, single points of contact and Computer Information Security Incident Response Teams (CSIRTs); establish cybersecurity risk management and reporting requirements; and establish cybersecurity information sharing.

When viewed from a holistic perspective it becomes clearer that these facets do not stand in isolation; they are parts of a greater whole which we refer to as our Technology and Cyber Security Incident Response Maturity Program.

As an overview, the following graphic depicts the program and its connection points to NIS2. Following the graphic are NIS2 article-specific references and then the document ends by providing details on our certification courses that align to the maturity program and NIS2.



SENIOR LEADERSHIP RISK MANAGEMENT

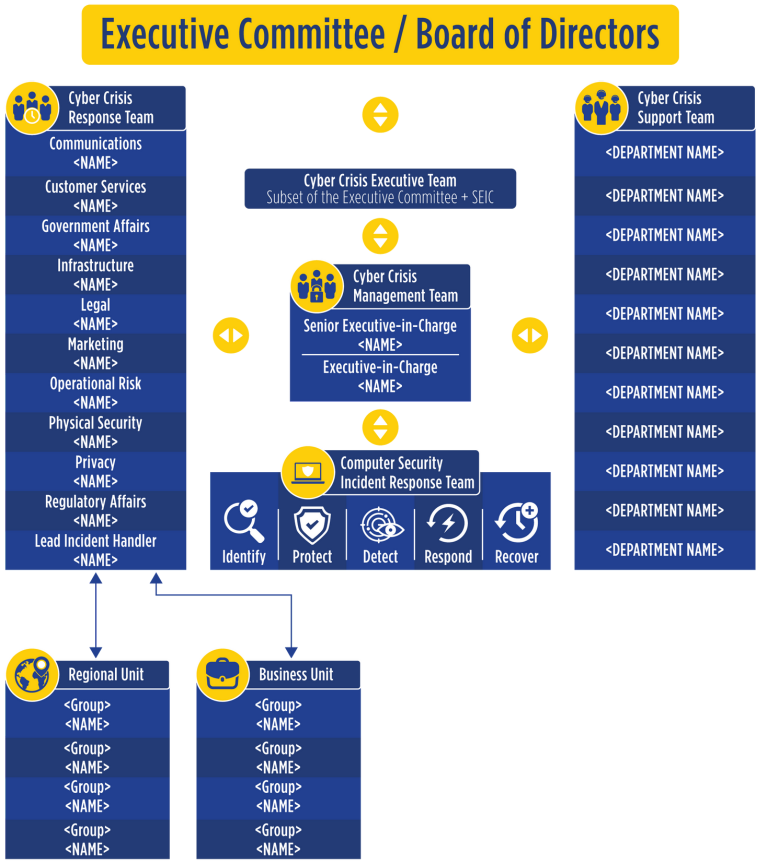
However, it's Articles 17 to 23 that establish the requirements for management bodies (e.g., Boards and executive leadership) to take "proportionate technical and organizational [emphasis added] measures to manage cybersecurity risks."

This requirement is one of the most important within the whole of NIS2. Organizational leadership serving in a governance capacity must ensure a strategic and tactical capability are envisioned, funded, and implemented.

Their role is also operational and should be built into the cyber crisis response model of each entity to demonstrate integration into overall high-severity incident management.

The pivotal role organizational leadership plays in cyber crisis management is not new to us. In fact, it was built into our framework well before NIS or NIS2 were conceived. As such, it's foundational in our response structure model and has been since day 1.

And, we knew that no framework is one size fits all, which is why we work with customers to ideate, craft, and re-craft innovative and workable solutions to meet the unique demands while still maintaining a standardized result that allows users across organizations, and Member States, to integrate and function without confusion.



THE CYBER CRISIS MANAGEMENT PLAN: STANDARDIZED & FLEXIBLE

As the author of the incident response maturity framework, we have a deep appreciation for the value and reliability a standardized approach provides. This framework affords the ability to streamline cyber crisis management plan (CCMP) development and implementation. At the same time, a framework must be flexible to allow for the unique requirements each customer brings to its structure.

The CCMP has a core, the information that needs to be comprehended in short order. This core is how we make a large plan consumable by the audience.

We also bring a set of templates and checklists, which can be reused as they are but customers are encouraged to customize them. These valuable assets are exclusive to our service and we customize them to your organization.

Graduates of our Cyber Crisis Management Planning Professional (C2MP2) course are positioned to successfully lead the development of a CCMP and supporting materials for their own organization as an integrated solution to meet the demands of NIS2 and the mission of Union cyber resilience.

INTEGRATING CSIRTS: BOUNDARIES & LIMITATIONS OF SCOPE

Articles 5 to 11 adds a requirement that Member States establish National Cybersecurity Crisis Management Frameworks including among other things, designating "national competent authorities for the management of large-scale cybersecurity incidents and crises." This builds off of the network of CSIRTs, however, entities should clearly understand that organizational risk associated with brand, reputation, regulatory penalties, and operations are factors of the organization's ability to effectively manage cyber crises; CSIRTs support technical aspects of an incident, not organizational.

IMPACT CATEGORIES, SCALES & SCORES

Impact Category	Severity Scale	Criteria	Score*
Financial Impact	High	>$2.5 MM Impact witin 1 week	50
	Medium	>$1.25 MM to >$2.5 MM Impact witin 1 week	30
	Low	>$0 to >$1.25 MM Impact witin 1 week	10
Operational Impact	High	• Order and/or fulfillment exceeds 24/7 resource capacity • Country and/or international customers consider moving to competitor	40
	Medium	• Orders and/or fulfillment requires staff overtime • Regional and market-specific customers consider moving to a competitor	24
	Low	• Limited to no impact on orders or fulfillment • Limited customers consider a competitor	8
Brand & Reputation Impact	High	• National or International media coverage • Extended image problem • Reputation and/or image severely impacted	30
	Medium	• Local media coverage • Long-term customer loss	18
	Low	• No media coverage • Short-term customer loss, recoverable	6
Regularity & Legal Impact	High	• Potential to cause penalty or fine • Criminal or civil charges possible	15
	Medium	• Increased intentation from regulators and/or auditors	9
	Low	• Little to no regulatory and/or auditors inquiries	3

Incident Severity Scale

Low	Medium	High
0-35	36-105	106+

*For each Impact Category, select the score corresponding to the appropriate criteria and add together to calculate a Total Score. Cross-reference the total score with the Incident Severity Scale to determine an objective Incident Severity.

IMPROVE THE ART OF CYBER WAR GAMING

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

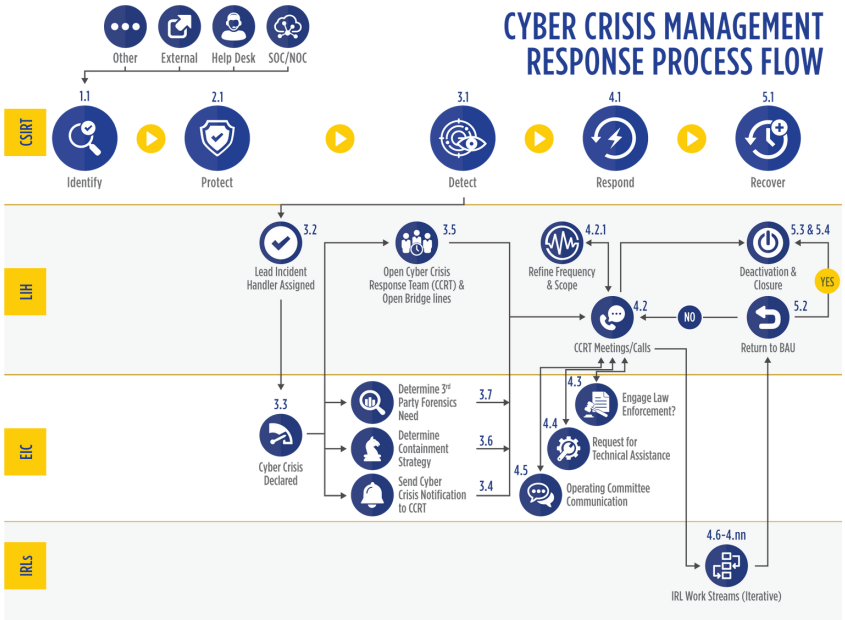
"CYBER EXERCISES ARE AN IMPORTANT TOOL TO ASSESS THE PREPAREDNESS OF A COMMUNITY AGAINST CYBER CRISES, TECHNOLOGY FAILURES AND CRITICAL INFORMATION INFRASTRUCTURE INCIDENTS."

STRATEGIES FOR INCIDENT RESPONSE AND CYBER CRISIS COOPERATION
EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

Cyber war games, whether discussion-based or operations-based, are of paramount importance to ensure both the cyber crisis management plan and cyber crisis leaders are prepared for real-world crises situations. Building realistic exercises is as much art as it is science. Our Cyber Crisis Management Exercise Professional (C2MEP) course teaches students how to build and deliver on this front.

Our cyber war game exercise training merges multiple international standards resulting in an integrated best practice.

CRISIS RESPONSE HARMONIZATION



When building complex process integration, it helps to begin with a framework that is standardized, yet flexible.

Whether harmonizing across a Member State or across the Union, a cyber crisis management response process flow serves to simplify the complex into a form that is not only understandable but, equally important, actionable in the fog of cyber war.

CRISIS LEADERSHIP READINESS

Cyber crisis readiness helps reduce chaos by establishing a plan, building awareness of the plan, refining crisis leadership confidence and capability, and optimizing for excellence and cyber crisis management maturity.

We have developed the world's first and only cyber crisis leadership simulation series that immerses leaders into a series of realistic scenarios designed to transform senior managers and executives from problem solvers to sense-making experts of non routine situations.

Leveraging the groundbreaking leadership research our program integrates non routine cyber crises scenarios to teach leaders how to assume and demonstrate responsibility in a crisis, how to make decisions and collaborate with others during periods of uncertainty, and skills to cope with substantial stress.

And since our business world is inherently culturally diverse we delve into cultural and societal dimensions from the Hofstede Insights worth considering when leading during a crisis.

Our industry-exclusive Cyber Crisis Management Leadership Professional (C2MLP) certification course is designed to ensure these leaders are poised for success.

CYBER CRISIS MANAGEMENT
PLANNING PROFESSIONAL (C^2MP^2)
CYBER SECURITY TRAINING & CONSULTING LLC

CYBER CRISIS MANAGEMENT
EXERCISE PROFESSIONAL (C^2MEP)
CYBER SECURITY TRAINING & CONSULTING LLC

CYBER CRISIS MANAGEMENT
LEADERSHIP PROFESSIONAL (C^2MLP)
CYBER SECURITY TRAINING & CONSULTING LLC

SELECT MEMBER STATE REFERENCES

In the *Austrian Strategy for Cybersecurity 2021* (*Österreichischen Strategie für Cybersicherheit 2021*), the public sector is called upon to improve and continually develop "mechanisms for effective management of cyber incidents and crises."

Section 14 of *Entire legal regulation for network and information system security law, version of 16.03.2022* (*Gesamte Rechtsvorschrift für Netz- und Informationssystemsicherheitsgesetz, Fassung vom 16.03.2022)* calls for establishment of computer emergency teams, which shall be supported by the national computer emergency team and sector-specific computer emergency teams. It also states the public administration computer emergency team (GovCERT) shall support public administration institutions in managing risks and incidents. The scope of services can be generalized as technical, awareness-building, and reporting. Organizational resilience and risk management are not within their scope.

Section 15 provides details for the operational and resourcing requirements of computer emergency response teams. Notably, this section also highlights that business continuity at the entity level is a result of organizational readiness (i.e., personnel, technical, and infrastructure).

Section 24 specifies the decision on whether or not there is a cyber crisis is to be made by the Federal Minister of the Interior.

Section 25 outlines responsibilities of the Coordination Committee to assist the Federal Minister of the Interior in the determination of a cyber crisis and the operational measures measures to address a cyber crisis, the option to expand the committee to included federal and state agencies, essential services, computer emergency response teams, and others, as deemed necessary, and that the Inner Circle of Operational Coordination (IKDOK) provide technical assistance.

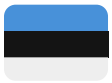
In *Cybersecurity Strategy Belgium 2.0: 2021-2025* published by the Center for Cyber Security Belgium, it states "In cooperation with the National Crisis Centre (NCCN), the Centre for Cybersecurity Belgium (CCB) ensures crisis management in cyber incidents. For administrations and public institutions, the CCB disseminates standards, guidelines and safety norms."

The CCB, acting as the national computer security incident response team (CSIRT) it is responsible for detecting, observing and analyzing online security issues such as cyber threats, vulnerabilities in ICT systems or cyber incidents.

Belgium outlines that Organizations of Vital Interest (OVI) need to be optimally protected against cyberattacks, as incidents affecting these organizations can have a large-scale, national impact. In this context, Organizations of Vital Interest Refer to the public and private entities that provide an essential service to the Belgian population and that use network and information systems to do so. These OVI are therefore considered a part of the nation's critical infrastructure.

In the *Danish Cyber and Information Security Strategy 2018-2021*, it states that the Centre for Cyber Security will use and integrate with the Belgium national crisis management system.

As outlined in the *National Emergency Response Plan, 6th edition 2009,* procedures and responsibilities that apply during normal day-to-day operations shall also, insofar as possible, apply in the crisis management system. It also states that the emergency response tasks must, insofar as possible, be managed locally and as close to the afected citizens as possible, and accordingly at the lowest suitable and relevant organisational level.



The Republic of Estonia's Ministry of Economic Affairs and Communications published the *2019-2022 Republic of Estonia Cybersecurity Strategy* and established priorities for strengthening a capability for early detection and prevention of cyber threats and integrating cybersecurity with planning of national defense and preparedness for coping with crises.

Through the implementation of NIS (Cybersecurity Act) provisions, the nation ensures practical readiness to cope with crises. It states regular joint cooperative exercises will be held with the state's political leadership, vital service providers and structures that ensure military defense. Capability-based resolution of cyber crises will be implemented in the public sector to make optimum use of the competence of various institutions.

France's *National Digital Security Strategy* leads its list of strategic objectives with establishing fundamental interests, defense and security of State information systems and critical infrastructures, and major cybersecurity crisis. France states it will continue to contribute to the emergence of an environment of voluntary cooperation for cybernetic crisis management at the European level, by supporting the work of the European agency ENISA (European Union Agency for Network and Information Security) in particular.

France will continue to support cybersecurity crisis management exercises led by CERT-EU (Computer Emergency Response Team of the European Union (EU), however, it must transfer acquired knowledge to the private sector to contribute to the handling of its cybersecurity.

The *Cyber Security Strategy for Germany 2021* outlines the need to "continually adapt its capabilities for the technical and operational detection of and reaction to cyber security incidents."

The *Second Act to Increase the Security of Information Technology Systems (Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme)*, refered to as IT Security Act 2.0, requires that during a significant disruption, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) may, in agreement with the respective competent federal supervisory authority, demand that the affected operators of critical infrastructures or the companies in the special public interest hand over the information, including personal data, necessary to manage the disruption.

Greece's *National Cyber Security Strategy* called for the development of a National Cyber Emergency Plan to define the structure and measures for dealing with the important incidents that take place in critical communication and IT systems. It is here that the criteria are defined to characterize an incident as critical, the definition of the important procedures and actions to deal with it, as well as the definition of the roles and responsibilities of the various actors involved to manage the specific incident.

The strategy called for the National Computer Emergency Response Team (CERT) to cooperate with other CERTs to monitor at a national and international level for threats and vulnerabilities as well as communicating with relevant bodies to help ensure resilience against cyber incidents.

The Luxembourg National Cyber Emergency Response Team (GOVCERT) manages the *National Contingency Plan*. This plan is transformed into a national information awareness platform called InfoCrise (https://infocrise.public.lu/en.html) whereby citizens can view the current national threat profile and incidents across critical service areas such as cyber, nuclear, weather, chemical and biological, flooding, water, energy and more.

The cyber section provides linkages to the *Cyber Emergency Response Plan Measures* and to the *Cyber Emergency Response Plan* (as decreed by the Council of Government on 19 March 2014). Among other goals, it aims to define the bodies that will manage the cyber crisis and define the emergency measures, associated actions, and the respective stakeholders in charge during a cyber crisis.

On 5 January 2018 Luxembourg's Government Council approved an update of the Emergency Response Plan to deal with attacks against information systems or the technical failure of information systems (Cyber ERP). The changes included clarification of the role and reinforcement of the crisis management missions of the Cybernetic Risk Evaluation Cell (Cellule d'Evaluation du Risque Cybernétique - CERC) as soon as a large-scale incident occurs, development of relations with the operators in the public and private sectors, and integration of the Crisis Communication Service (Service de la Communication de Crise - SCC) which, in the event of an emergency situation or national crisis, is responsible for the horizontal coordination of the organization of communication.

In Portugal's *National Strategy for Cyberspace Security 2019-2023*, it calls for a need to "strengthen the coordination and strategic and operational coordination of national entities involved in the security of cyberspace in order to safeguard the efficient and effective national crisis management" while adapting, for crisis management purposes, the capabilities of the Armed Forces, Security Forces and Services and other public and private entities, with the objective of boosting an integrated approach to the threats and risks of cyberspace security.

In the *National Cybersecurity Framework* published by the Portuguese National Cybersecurity Centre, ID.AO-5 instills resilience requirements to support the delivery of critical services for all operating states, including the ability to identify crisis scenarios, identify a recovery strategy, and defining a critical services recovery plan.

On January 30, 2018, the National Council of the Slovak Republic adopted the *Cybersecurity Act*. Article 27, Cybersecurity Incident Handling, it outlines that the National Security Authority may alert when there are serious cyber security incidents, handle the incident, direct reactive measures, and draft measure to prevent further spread and recurrence.

Alerting and warnings are issued via the Cybersecurity Single Information System, and if warranted, to mass media and the Central Portal of Public Administration.

The technical handling is fulfilled by the Computer Security Incident Response Team (CSIRT) Unit for operators of essential services and digital services providers. CSIRT activities are outlined in Article 15 and address cybersecurity incident detection, analysis, response, coordination, containment, and recurrence elimination.

Sweden's *Comprehensive Information and Cyber Security Action Plan (Samlad informations- och cybersäkerhetshandlingsplan 2019–2022)* acknowledges the recommendation from the Swedish Armed Forces and Defense Committee to build upon current capabilities within crisis preparedness.

Strategic Prioritization 3 outlines objectives to strengthen the ability to prevent, detect and manage cyber attacks and others IT incidents. Strategic Prioritizations 5 and 6 add requirements to establish both cross-sectorial and technical exercises and expand international cooperation.

NON-EU NATIONAL REFERENCES

The United Kingdom's *National Cyber Strategy* seeks to strengthen resilience at national and organizational levels to prepare for, respond to and recover from cyber attacks. Part 119 outlines the goal to make the UK's strategic management and coordination of the response to nationally significant cyber incidents is even more effective.

As such, the Nation will "build upon the government's experience of responding to significant cyber incidents, ensuring that lessons identified are used to improve our policies and processes" while sharing crisis management experience with international partners and industry and, in turn, work to identify best practices from elsewhere to enhance preparedness and processes.

Part 122 expands on this to ensure "incident management teams have the requisite expertise, capacity and capabilities to respond to the full range of evolving incident types."

In Switzerland, the Center for Security Studies (CSS), ETH Zürich highlights the need for the "creation of sound, resilient structures for crisis management, including efficient crisis communications, and the development of a strong ability to respond to serious incidents which takes this communications aspect into account."

The *National strategy for the protection of Switzerland against cyber risks (NCS) 2018-2022* lists spheres of action and measures including crisis management. This sphere includes the integration of the responsible cyber security offices into the federal crisis teams and conducting joint crisis management exercises.

The responsible cyber security offices must be directly involved in crisis management at the federal level and private sector must also continue to be rehearsed on a regular basis.

CYBER CRISIS MANAGEMENT CERTIFICATION SERIES

CYBER CRISIS MANAGEMENT PLANNING PROFESSIONAL (C2MP2)

OBJECTIVE

A deep, hands-on immersion into the development of a Cyber Crisis Management Plan (CCMP), which like a major cyber event, requires the collaboration of both line of business leaders and their partners in information technology / information security.

VALUE

During the fog of war (cyber crisis) is not the time to figure out how to respond. An effective response requires careful planning across an organization. This in-depth, hands-on immersion boot camp gives attendees the knowledge and tools to complete their own CCMP.

COURSE OUTLINE

FOUNDATIONS OF A CYBER CRISIS MANAGEMENT PLAN

THE PLAN CORE

- Acronyms
- How to Use the Cyber Crisis Management Plan
- Define Plan Purpose
- Response Organization
- Response Structure

FUNCTIONAL INCIDENT RESPONSE PLANS

- Functional Incident Response Plan (Detailed)
- Functional Incident Response Plan (Summary)
- Linking Incident Response Plans

RESPONSE PROCESS FLOW

- Response Process Flow Foundation
- Master and CSIRT Incident Response Plans
- Response Process Flow Completion

CYBER CRISIS MANAGEMENT PLANNING PROFESSIONAL (C2MP2)

COURSE OUTLINE (CONTINUED)

CYBER WAR ROOMS & BRIDGE LINES
- War Rooms
- Bridge Lines
- Cyber Crisis Logistics

TEAMS, ROLES & RESPONSIBILITIES
- Cyber Crisis Executive Team (CCET)
- Cyber Crisis Management Team (CCMT)
- Cyber Crisis Response Team (CCRT)
- Computer Security Incident Response Team (CSIRT)
- Cyber Crisis Support Team

WORKING GROUPS
- Communications Working Group
- Technology Working Group
- Additional Working Groups

CYBER CRISIS MANAGEMENT ROLES, CHECKLISTS & TEMPLATES

PLAN OWNERSHIP AND GOVERNANCE
- Plan Ownership
- Plan Governance

IMPACT CATEGORIES, SCALES & SCORES
- Impact Categories, Scales & Scores Table

CYBER ATTACK & CRISIS ANATOMIES
- Cyber Attack Anatomy
- Cyber Crisis Management Anatomy™

CYBER CRISIS INFORMATION FORM
- CCIF Development

CHECKLISTS
- Lead Incident Handler Checklist
- Pre-Confirmation
- Post-Confirmation
- Cyber Crisis Deactivation Checklist

CYBER CRISIS MANAGEMENT PLANNING PROFESSIONAL (C2MP2)

COURSE OUTLINE (CONTINUED)

TEMPLATES

- LIH-to-EIC Email Template
- EIC-to-CCRT Incident Notification Email Template
- LIH-to-CCRT Initial Meeting Email Template
- Initial CCRT Meeting Agenda Template
- Subsequent CCRT Meeting Agenda Template
- SEIC-to-CCET Email Template

QUICK REFERENCE CARDS

- CCET Quick Reference Card
- SEIC Quick Reference Card
- EIC Quick Reference Card
- LIH Quick Reference Card
- IRL Quick Reference Card

CYBER CRISIS MANAGEMENT PLAN USAGE AND VALIDATION (TABLETOP WAR GAME INTRODUCTION)

PROJECT PLANNING

- Project Resources
- Project Phases & Activities
- Phase I: Plan
- Phase II: Build
- Phase III: Test
- Phase IV: Implement

TRAINING THE ORGANIZATION

- CCMP Training Deck

TABLETOP CYBER WAR EXERCISES

- Tabletop Exercises vs. Immersive Simulations
- Exercise Roles & Responsibilities
- Exercise Logistics
- Exercise Materials
- Exercise Execution
- Exercise Conclusion
- After-Action Reporting

WRAP-UP

- Version Control
- Release Planning

CYBER CRISIS MANAGEMENT CERTIFICATION SERIES

CYBER CRISIS MANAGEMENT EXERCISE PROFESSIONAL (C2MEP)

OBJECTIVE

An immersion into planning, developing, conducting, and assessing tabletop cyber war games that are aligned to and compliant with the U.S. Homeland Security Exercise and Evaluation Program (HSEEP), National Institute of Standards and Technology (NIST) (800-34, 800-61, 800-84 & 800-184), and International Standards Organization (ISO) (27035 & 22398).

VALUE

The ability to plan, develop, deliver, and assess tabletop war games are essential skills required to validate an organization's incident response and cyber crisis management plans. Acquiring this certification demonstrates a unique and specialized set of knowledge, skills, and abilities.

COURSE OUTLINE

FOUNDATIONS OF TABLETOP CYBER WAR EXERCISES

- Tabletop Exercises vs. Immersive Simulations
- Exercise Scope
- Exercise Design & Development
- Setting the Foundations
- Planning Meetings
- Concept and SMART Objectives Meeting
- Initial Planning Meeting
- Midterm Planning Meeting
- Master Scenario Events List Meeting
- Final Planning Meeting
- Exercise Roles & Responsibilities
- Exercise Execution & Logistics
- Exercise Materials
- Situation Manual
- Player Handbooks
- Facilitator Guide
- Exercise Presentation
- Exercise Evaluation Guide
- Participant Feedback Form
- Exercise Conclusion
- After-Action Reporting
- Exercise Improvement Planning

TABLETOP CYBER WAR EXERCISE PRACTICALS

- Customize all contents required to build, deliver, and assess an exercise
- Serve as facilitator for a given exercise subset
- Act as observer for a given exercise subset

CYBER CRISIS MANAGEMENT CERTIFICATION SERIES

CYBER CRISIS MANAGEMENT LEADERSHIP PROFESSIONAL (C2MLP)

OBJECTIVE

The objective of this service is to immerse an organization's cyber crisis leadership team into a real-world like integrated education, analysis and performance optimization experience designed to prepare the team to effectively lead the response to a major cyber incident. Training material integrates British Standards Institution (BSI) 11200 guidance.

VALUE

Cyber crisis leaders graduate from the course with new-found knowledge, confidence, and capabilities uniquely designed to prove to the board, regulators, customers and shareholders that the organization is committed to doing all it can to reduce cyber risk and increase organizational resilience.

COURSE OUTLINE

BECOMING A SENSEMAKER

- The Leadership Challenge
- Identifying the Root of Poor Crisis Management
- How Sense-Making Works
- The Value of Accuracy and Incremental Clarity

CLUE RECOGNITION

- Exploring the Wider System
- Creating Situational Maps
- Clue Overload
- What You See is All There Is
- Blind to the Obvious | Blind to our Blindness
- The Power of Recognition
- Three Common Heuristics
- Multinational Cross-Cultural Considerations | Cyber Attack Data Correlation
- Top Techniques Used by Advanced Persistent Threats (APTs): China, Iran & Russia
- Visual Influences on our Intuition

CYBER CRISIS MANAGEMENT
LEADERSHIP PROFESSIONAL (C2MLP)

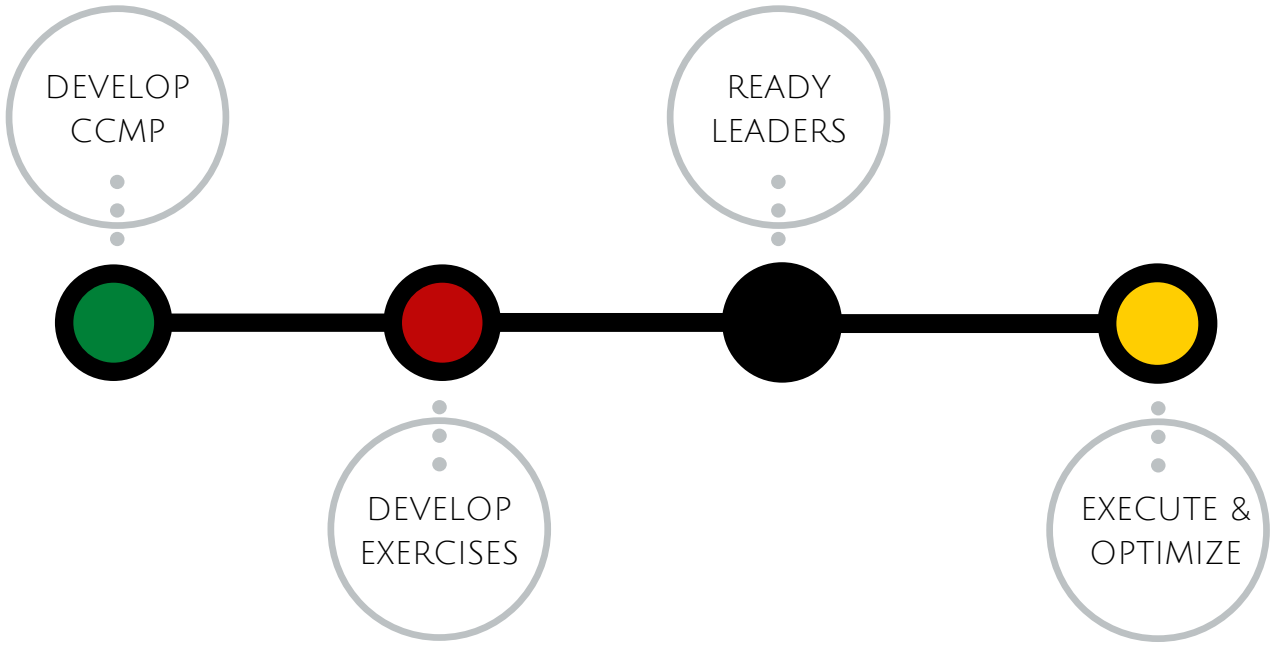
COURSE OUTLINE (CONTINUED)

THINKING IN FRAMES

- Magic Andrea
- What are Frames
- Recognition-primed Decision Making
- Influential Cyber Risk Frames
- The Professional Risk Frame
- (Re)Framing to Remove Blind Spots
- Tools in the Kit
  - Perspective-taking
  - Issue Selling
  - Effective Communications
  - Creativity
  - Organizational Agility
  - Risk Taking
- Leveraging the Gift of Fear
- Surviving a Trip to the Edge of Chaos
- Dressing for Success | Employing the Bowtie Model
  - Factoring Impact Categories, Scales & Scores

CAPABILTY INTEGRATION

- Magic Andrea: Sharing her Secrets
- Change the System from Within | Tools for Change
- Exercises for Mental Muscle Memory
- After-action Reviews
- Giving Honest Performance Feedback to Leaders



NIS2

FOR MORE INFORMATION

JEFFREY CRUMP | JCRUMP@CYBERCRISISRESPONSE.COM