
NIST Alignment
Crisis Simulation Service
CORE TO CLOUD™

# Crisis Simulation Service – Alignment to NIST

## Introduction

The National Institute of Standards and Technology (NIST) established the Risk Management Framework (RMF) as a set of operational and procedural standards or guidelines that a US government agency must follow to ensure the compliance of its data systems. NIST has been adopted and adapted by many nations, including the UK and acts as a common reference for customers, vendors, and services organisations. According to NIST, these standards, guidelines, and best practices are essential to managing cyber-security-related risk.

Core to Cloud has created a portfolio of support and managed services that combine leading vendor technologies, robust processes, and highly experienced resources that align with NIST, MITRE and ATT&CK frameworks. It's critical that these frameworks are applied to the services we deliver to customers to improve the protection and resilience of critical infrastructure and systems.

The aim of this document is to illustrate how each of our services aligns to the key elements of NIST. It will outline how the combination of technology, people, and process in the context of NIST will greatly improve the outcomes of our customers.

## Crisis Simulation Service Overview

Core to Cloud's crisis simulation service is based on Immersive Lab's platform. The service combines the expertise of Core to Cloud's security consultants and the functionality of the Immersive Labs application. The outcome will be a set of insightful reports that includes suggestions and recommendations that together will significantly improve how your organisation can improve its ability and readiness to respond to a cyber-attack.

## Service Description

The process to conduct the crisis simulation will be led by Core to Cloud's senior consulting team and will consist of three stages:

- **Consultation**: This collaborative session will decide on the specific scenario to be executed. Consideration will be given to the client's potential areas of concern or areas of perceived high risk. Examples of the scenarios are Website attacks, data theft, denial of service, ransomware attacks, insider data breaches etc. The consultation period should take between 1 and 2 hours but can vary depending on the number of stakeholder conversations we need to have.
- **Execution**: During this stage, the participants will be guided through a series of situations and be presented with several questions that relate to the scenario. Depending on the option chosen as a response the impact and consequences will be reflected in a visual representation in the tool. The aim here is to see the impact of decision-making on key indicators such as share price, reputation, corporate risk and so on. Each instance of the crisis simulation is expected to take approximately half a day and will be delivered remotely unless requested otherwise.
- **Reporting and Recommendations**: Once the session has been completed, the results will be presented to the client. The Crisis Simulation generates a report which will be the basis of a discussion that Core to Cloud will lead. The desired outcome of this session will be to highlight the client's overall response and recovery processes and behaviours in the event of a serious cyber-attack. The discussion will allow the team to prioritise the areas where lessons can be learned, and improvements can be identified.

# Immersive Labs Platform Description

Immersive Labs' Cyber Crisis Simulator is an online solution that drops defenders into real-time cyber crises. The system challenges teams to make critical decisions when dealing with emerging incidents such as ransomware outbreaks, insider threats, data breaches, and spear-phishing attacks.

These responsive scenarios create rich, realistic storylines that twist and turn based on the choices your people make. They are designed to drive your organization's cyber resilience and human readiness, preparing your people to face the real-world consequences of a cyber incident. The simulator tracks individual and team responses in real-time, providing executives with an instant view of performance, and packaging post-exercise insights into areas for improvement.

For cyber exercise to be effective, it needs to feel as close to the real thing as possible. The Crisis Simulator adjusts the narrative of scenarios based on the decisions participants make, allowing them to experience an evolving incident. The quantitative impact of these choices is also measured, tracking changes to share price, brand reputation, and even an organization's liquidity. Individuals rank how confident they feel in their own choices and justify why they selected options, offering insight into areas of uncertainty and vulnerability.

## NIST Framework

- Common and Accessible language.
- Adaptable to many technologies, lifecycle phases, sectors and uses.
- Risk-based.
- Based on international standards.
- Living document.
- Guided by many perspectives – private sector, academia, public sector.

| NIST STAGE | FUNCTION | SERVICE/PLATFORM ALIGNMENT |
|---|---|---|
| **IDENTIFY** | The Identify Function assists in developing an organisational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organisation to focus and prioritise its efforts, consistent with its risk management strategy and business needs. | The consultation process will define the scenarios which will be used in the simulation exercises. These scenarios are designed to identify the key risks to systems, people, assets, data, and capabilities.<br>The responses recorded from the scenario exercises will expose any weaknesses and potential areas of improvements to strengthen the organisation's ability to identify risk and implement changes in the systems and business structure. |
| **PROTECT** | The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. | The scenarios specific to critical infrastructure will highlight compromised systems and networks. The detailed reports will provide evidence of high-risk areas that could be vulnerable to attacks and make suggestions of changes to limit the impact of a cybersecurity event. |
| **DETECT** | The Detect function defines the appropriate activities to identify the occurrence of a cybersecurity event.<br>The Detect function enables the timely discovery of cybersecurity events. | The output from the scenario exercises could expose weaknesses in the organisation's ability to detect cybersecurity events, either through lack of correct systems, low skills levels in the team, or lack of good process.<br>The Core to Cloud would make suggestions on the priority elements that needed to improve detection capabilities |
| **RESPOND** | The Respond Function includes appropriate activities to act regarding a detected cybersecurity incident. The Respond function supports the ability to contain the impact of a potential cybersecurity incident. | The outcome of the scenario exercises will highlight an organisation's ability to respond to a cyber-attack or any detected serious event. Incident response planning is at the heart of the crisis simulation service, with organisations being presented with a comprehensive report of their ability to respond and suggested steps that can improve their ability to contain the impact of an incident. |
| **RECOVER** | The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. | Incident recovery is a key area covered in the service. The report created from the exercises will be discussed with the customer, resulting in decisions on how further resilience could be gained and how response planning can be further enhanced.<br>The scope includes not just how systems an data can be recovered with minimal business impact but how the business's functions and its 3rd parties can effectively recover. |

Core to Cloud Ltd, The Castle, Cecily Hill, Cirencester, GL7 2EF, United Kingdom
+44 (0) 1285 708 313 | info@coretocloud.co.uk | www.coretocloud.co.uk