DYNAMO - Dynamic Resilience Assessment Method including combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors

Business Continuity Management

The development of the DYNAMO platform enables the resilience assessment of the critical sector by combining the disciplines of Business Continuity Management (BCM) and Cyber Threat Intelligence (CTI). The combination of CTI processing with the BCM approaches will further enhance situational awareness and recovery planning capabilities of Businesses/ Critical Infrastructures. What exactly is meant by Business Continuity Management and how this discipline is built into DYNAMO is explained in more detail in the first edition of the DYNAMO factsheets.

Business Continuity Management in a Nutshell

Business continuity management refers to the advanced planning, preparation and implementation of procedures within an organisation to maintain business functions within acceptable time frames at predefined capacity during a disruption. An essential objective of the BCM process is Business impact analysis, which aims to identify potential events that risk business interruption. The procedures are then defined for identified risk to either avoid or mitigate the impact of the event. These procedures should be regularly tested to ensure that they work and should be regularly reviewed to ensure that they are up to date. Furthermore, regular and appropriate training should be offered to employees. With progress in technology and digitization of businesses, cyber-attacks threaten the integrity of businesses, especially for critical sectors. Hence, it is important to identify these feared events and ensure BCM processes are in place against them. The market for BCM solutions is fragmented against these evolving

threats and has significant gaps in their offerings for practitioners. DYNAMO aims to make a significant contribution to closing this gap and is therefore developing a platform with the help of business continuity management (and AI solutions) to deliver an integrated solution for the health, marine and energy sectors.

The DYNAMO BCM approach and assessment

Within the BCM approach, DYNAMO plans to incorporate and build on existing tools and approaches to create an advanced situational awareness toolset, knowledge repository, training tools and a forensic intelligence toolset. It is essential that by integrating a BCM approach, DYNAMO targets all professionals in charge of keeping critical functions of organisations running during a cyber-attack, not only cyber practitioners. As DYNAMO includes BCM approaches and tools, which measure the actions and performance under a cyber-attack (real or tested) and provide lessons-learned for process and tool improvements, considering both hard and soft aspects of the organisation system. This ensures that the platform and tools are effective to the end-users and enhance the development of more resilient infrastructure.

The BCM assessment raises the understanding of critical business processes, the interaction of single elements within a sector, potential vulnerabilities and existing processes aimed at maintaining the business operations at a minimum acceptable level. The cause and effect of cyber incidents can be evaluated and is aimed to be demonstrated with several use-cases. The following key points characterise the DYNAMO BCM Assessment:

- Within a business, the BCM assessment has different levels of detail and, with varying levels of data, provides a quick and detailed assessment of the area under review and helps identify critical processes.
- Through a detailed academic search, ISO standards review and discussions with practitioners on BCM, CTI and resilience, the current gaps in marrying these three terms effectively will be highlighted. From there, DYNAMO definitions for these key terms will be proposed, emphasising essential crossovers in a resilience cycle and framework.
- Through a review of existing state-of-the art commercial tools, gaps in existing tools will be noted, with DYNAMO seeking to address these gaps.
- Agent based simulations are expected to measure the resilience of the business/processes for various threats and rate mitigation and recovery strategies that are foreseen to be generated with the help of state-of-the-art AI-based solutions.
- The results will summarize sector based best BCM practices in consultation with CTI.
- End-user data is integrated to measure set performance targets. AI-based approaches are used in the functional description of the assessment for a deeper understanding and possible self-learning of the networked process.
- The results will generate knowledge about the susceptibility and vulnerability of the sector, existing mitigation measures and possibly define new measures to safeguard the critical aspects of the business.
- The solutions will support the BCM with regards to the five resilience phases (will be described in more detail in Factsheet 3).

Fraunhofer EMI · TECHNIKON · Information Technologies Institute · factorSOCIAL · LAUREA AMMATTIKORKEAKOULU University of Applied Sciences · NAVAL GROUP · KEMEA · KPMG · Future Analytics · VISIONSPACE · telelink BUSINESS SERVICES · Gemelli Fondazione Policlinico Universitario Agostino Gemelli IRCCS Università Cattolica del Sacro Cuore · RHEA GROUP · UCC University College Cork, Ireland Coláiste na hOllscoile Corcaigh · CRBC CENTRE FOR RESILIENCE & BUSINESS CONTINUITY · CUBS CORK UNIVERSITY BUSINESS SCHOOL · System X · Laborelec RESEARCH & INNOVATION

Consortium
15 Partners
10 Countries

Budget
€ 5 Million
100% EU-funded

Duration
36 Months
10/2022 - 09/2025