Co-funded by the Erasmus+ Programme of the European Union

secureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

ERASMUS+ Strategic partnership “Digital education tools for security risk management”
Project number: 2021-1-LV01-KA220-HED-000023056

Biometric Verification	Any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. These biological identifiers include fingerprints, hand and earlobe geometries, retina patterns, voice prints and written signatures. (General Data Protection Regulation, European Union, 2016)
Business Continuity	The capability of the organization to continue delivery of products or services at acceptable predefined capacities following a disruption. (ISO 22313:2020)
Business Continuity Management	The process of implementing and maintaining business continuity in order to prevent loss and prepare for, mitigate and manage disruptions. (ISO 22313:2020)
Crime prevention	Ethically acceptable and evidence-based activities aimed at reducing the risk of crime occurring and its harmful consequences with the ultimate goal of working towards the improvement of the quality of life and safety of individuals, groups and communities. (European Crime Prevention Network)
Critical infrastructure	The body of systems, networks and assets that are so essential that their continued operation is required to ensure the security of an organization, region, society, country. (U.S. Department of Homeland Security, website)
Cyber security	The practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. (Kaspersky, website)
Information security	To protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability. (National Institute of Standards and Technology, U.S. Chamber of Commerce, 2020)
Information warfare	A class of techniques, including collection, transport, protection, denial, disturbance, and degradation of information, by which one maintains an advantage over one's adversaries. (Burns, M. 1999)
Loss prevention	Any actions taken to reduce the amount of theft, breakage, or wastage in a business. (Collins dictionary)
Personnel security	A system of policies and procedures which aim to manage and minimize the risk of people exploiting legitimate access to an organization’s assets or premises for unauthorized purposes. (UK Government publication, Personnel and People security, 2020)

Physical security	To take active as well as passive measures, designed to deter intruders, prevent unauthorized access, including theft and damage, to assets such as personnel, equipment, installations, materials, and information, and to safeguard these assets against threats such as espionage, sabotage, terrorism, damage, and criminal activity. (Center for Development of Security Excellence, 2017)
Preparedness	A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response (Keim, M. 2021)
Recovery	To restore and return business activities from the temporary measures adopted during and after a disruption. (ISO 22301:2019)
Resilience	The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems. (National Institute of Standards and Technology, U.S. Chamber of Commerce, 2020)
Response force	Security force (security guards, police force or law enforcement officers) that prevent adversarial success. Response consists of interruption and neutralization.
Risk	Effect of uncertainty on objectives. (ISO 31000)
Risk analysis	To comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. (ISO 31000)
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation. (ISO 31000)
Risk evaluation	To compare the results of the risk analysis with the established risk criteria to determine where additional action is required. (ISO 31000)
Risk identification	To find, recognize and describe risks that might help or prevent an organization achieving its objectives. (ISO 31000)
Risk management	Coordinated activities to direct and control an organization with regard to risk. (ISO 31000)
Risk treatment	To select and implement options for addressing risk. (ISO 31000)
Safety management	To apply a set of principles, framework, processes and measures to prevent accidents, injuries and other adverse consequences. (Skybrary, website)
Security management	To protect (business) operations from disruption and harm, including people, information, assets, and reputation through procedural, technical, and physical risk mitigation and control measures. (Smith and Brooks 2012; Fischer et al. 2008; Talbot and Jakeman 2009).
Security officer/guard/steward	**A person** employed/contracted to guard, patrol and protect premises, property or people.
Surveillance	To monitor a person or place (e.g. by cameras), because of a crime that has happened or is expected. (Cambridge dictionary, adjusted)