- <101> **Audit**: A systematic, independent and documented process for obtaining evidence and evaluating it objectively to determine whether activities, processes, or results comply with established criteria. Audits are a form of assessment and often used to verify compliance. Reference: ISO 9000:2015(en) Quality management systems - Fundamentals and vocabulary
- <102> **BoD (Board of Directors)**: Governing Body; Top Management; person or group of people who directs and controls an organization at the highest level. Reference: ISO 37000:2021(en) Governance of organizations - Guidance
- <103> **Business Continuity**: Capability of an organization to continue the delivery of products or services at acceptable predefined levels following a disruptive incident. Reference: ISO 22300:2021(en) Security and resilience - Vocabulary
- <104> **Business Model**: A business model is a company's core strategy for profitably doing business. Models generally include information like products or services the business plans to sell, target markets, and any anticipated expenses. Reference: https://www.investopedia.com/terms/b/businessmodel.asp https://www.investopedia.com/terms/b/businessmodel.asp
- <105> **Certification**: Procedure by which a third party gives written assurance that a product, process, or system conforms to specified requirements, such as a management system standard. Certification bodies must themselves be competent and may be accredited to ensure impartiality and consistency. Reference: ISO/IEC 17021-1:2015(en) Conformity assessment - Requirements for bodies providing audit and certification of management systems
- <106> **Compliance**: Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled. Compliance may be assessed through internal controls, inspections, or formal audits. Reference: ISO 37301:2021(en) Compliance management systems - Requirements with guidance for use
- <107> **Corporate Governance**: System by which an organization is directed and controlled at the highest level to achieve its objectives and meet the necessary standards of accountability, integrity and openness. Reference: ISO 37000:2021(en) Governance of organizations - Guidance
- <108> **CxO**: Generic label for high-level executives with organisation-wide responsibility over strategic or operational domains. Examples include CEO (Chief Executive Officer), CIO (Chief Information Officer), CRO (Chief Risk Officer), CTO (Chief Technology Officer), and CISO (Chief Information Security Officer). References: ISO 37000:2021(en) Governance of organizations - Guidance; https://www.investopedia.com/terms/c/chief-risk-officer.asp / https://www.investopedia.com/terms/c/chief-information-officer-cio.asp / https://www.investopedia.com/terms/c/chief-risk-officer.asp
- <109> **Documented Information**: information (3.8.2) required to be controlled and maintained by an organization (3.2.1) and the medium on which it is contained / Note 1 to entry: Documented information can be in any format and media and from any source. Note 2 to entry: Documented information can refer to**: - the management system (3.5.3), including related processes (3.4.1); - information created in order for the organization to operate (documentation); - evidence of results achieved (records (3.8.10)). Note 3 to entry: This constitutes one of the common terms and core definitions for ISO management system standards given in Annex SL of the Consolidated ISO

Supplement to the ISO/IEC Directives, Part 1. Reference: ISO 9000:2015(en) Quality management systems - Fundamentals and vocabulary"

- <110> **Due diligence**: Refers to the structured and proactive assessment of risks, obligations, and potential impacts before or during decision-making.
- <111> **Ethical Values**: Ethics is the discipline concerned with what is morally good and bad and morally right and wrong. The term is also applied to any system or theory of moral values or principles. (...) Its subject consists of the fundamental issues of practical decision making, and its major concerns include the nature of ultimate value and the standards by which human actions can be judged right or wrong. Reference: https://www.britannica.com/topic/ethics-philosophy
- <112> **Governance**: System by which the whole organization is directed, controlled and held accountable to achieve its core purpose over the long term. Reference: ISO 37000:2021(en) Governance of organizations - Guidance
- <113> **GRC (Governance, Risk and Compliance)**: Integrated collection of capabilities that enable an organization to reliably achieve objectives (governance), address uncertainty (risk management), and act with integrity (compliance). GRC aims to align activities across functions, reduce duplication, and ensure accountability. Reference: OCEG GRC Capability Model; ISO 37301:2021(en); ISO 31000:2018(en)
- <114> **IMS**: An Integrated Management System (IMS) integrates all of an organization's systems and processes into one complete framework, enabling an organization to work as a single unit with unified objectives. # Integrated Management Systems are systems which integrates all components of a business into one complete system so as to enable the achievement of its purpose and mission. Reference: https://integrated-standards.com/articles/what-is-integrated-management-system/
- <115> **Internal Control**: Process designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance. Reference: COSO Internal Control - Integrated Framework, 2013
- <116> **KPI (Key Performance Indicator)**: A quantifiable measure used to evaluate the success of an organisation, employee, or process in meeting objectives. Reference: https://www.investopedia.com/terms/k/kpi.asp
- <117> **Leadership**: Ability to lead a group of people or an organization, typically involving the establishment of a clear vision, sharing that vision with others, providing information, knowledge and methods to realize that vision, and coordinating and balancing the conflicting interests of all members and stakeholders. Reference: ISO 9000:2015(en) Quality management systems - Fundamentals and vocabulary
- <118> **Management**: Coordinated activities to direct and control an organization. Reference: ISO 9000:2015(en) Quality management systems - Fundamentals and vocabulary
- <119> **Management Frameworks**: Structured collections of concepts, guidelines and best practices used to support consistent and effective management across domains. Frameworks may include formal standards (e.g., ISO/IEC 27001) and de facto best practices (e.g., COBIT, ITIL), providing reference models, processes, and controls to guide governance, risk, and compliance efforts. References: ISO/IEC 27000 family; COBIT 2019 Framework; ITIL 4 Foundation Reference:

- <120> **Management System**: Set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives. Reference: ISO 9000:2015(en) Quality management systems - Fundamentals and vocabulary
- <121> **Maturity**: Degree of formality and optimisation of processes, from ad hoc practices to formally defined steps, improved and measured processes, and continuous improvement. Reference: CMMI Institute - Capability Maturity Model Integration
- <122> **Mission**: Organisation's purpose for existing as expressed by top management. Reference: ISO 9000:2015(en) Quality management systems - Fundamentals and vocabulary
- <123> **MSS (Management System Standard)**: Documented specification for a management system that provides requirements, guidance, or characteristics to be consistently used to ensure that materials, products, processes, and services are fit for their purpose. ISO/IEC MSSs include standards such as ISO 9001, ISO/IEC 27001, and ISO 14001. Reference: ISO/IEC Directives, Part 1 - Consolidated ISO Supplement - Procedures specific to ISO
- <124> **Organisational Culture**: values, beliefs and practices that influence the conduct and behaviour of people and organizations # Corporate culture refers to the beliefs and behaviors that determine how a company's employees and management interact. Reference: ISO/DIS 10010(en) Quality management - Guidance to understand, evaluate and improve organizational quality culture to drive sustained success / https://www.investopedia.com/terms/c/corporate-culture.asp
- <125> **Organizational Culture**: Set of shared values, beliefs, norms and practices that influence the way people within an organization interact with each other and with external stakeholders. Reference: ISO 30400:2016(en) Human resource management - Vocabulary
- <126> **Organizational Structure**: Arrangement of responsibilities, authorities and relationships between people. Reference: ISO 9000:2015(en) Quality management systems - Fundamentals and vocabulary
- <127> **Policy**: A policy is a formal statement of principles or rules adopted by an organisation to guide decisions and behaviours in a consistent and accountable manne
- <128> **Procedure**: A procedure is a documented set of specific steps or actions that must be followed to carry out a particular task or process in accordance with established policies.
- <129> **Process**: Set of interrelated or interacting activities which transforms inputs into outputs. Reference: ISO 9000:2015(en) Quality management systems - Fundamentals and vocabulary
- <130> **Quality**: degree to which a set of inherent characteristics (3.10.1) of an object (3.6.1) fulfils requirements (3.6.4) Note 1 to entry: The term "quality" can be used with adjectives such as poor, good or excellent. Note 2 to entry: "Inherent", as opposed to "assigned", means existing in the object (3.6.1). # Uniformity around a target value Reference: ISO 9000:2015(en) Quality management systems - Fundamentals and vocabulary. Definition attributed to Genichi Taguchi - https://en.wikipedia.org/wiki/Genichi_Taguchi"
- <131> **RACI**: RACI is one of many examples of a role responsibility framework, which stands for "Responsible, Accountable, Consulted, Informed". Role and responsibility frameworks define who is related to what within an organization or project, clarifying roles, tasks, duties, deliverables, etc.,

promoting accountability and efficiency. Reference: https://www.cio.com/article/287088/project-management-how-to-design-a-successful-raci-project-plan.html

- <132> **Records Management**: Records Management deals with the management of current and archival records, regardless of format. It includes the planning, control, directing, organising, training, promoting and other managerial activities related to records creation, maintenance and disposition. Reference: ISO 15489-1:2016 - Information and documentation - Records management - Part 1**: Concepts and principles
- <133> **Regulatory body**: An authorised institution responsible for enforcing a regulatory framework and overseeing compliance.
- <134> **Regulatory framework**: A structured set of laws, rules, or guidelines that govern specific activities or sectors.
- <135> **Risk**: Effect of uncertainty on objectives. Reference: ISO Guide 73:2009(en) Risk management - Vocabulary
- <136> **Top Management**: Person or group of people who directs and controls an organization at the highest level. Reference: ISO 9000:2015(en) Quality management systems - Fundamentals and vocabulary
- <201> **BIA**: Business Impact Analysis / Business Impact Assessment / process of analysing the impact over time of a disruption on the organization. The outcome is a statement and justification of business continuity requirements. Reference: ISO 22300:2021(en) Security and resilience - Vocabulary
- <202> **CIA triad**: The CIA triad is an InfoSec concept that refers to confidentiality, integrity and availability. Confidentiality means restricting access to information; Integrity is ensuring accuracy and completeness; Availability ensures information is accessible when needed. Reference: ISO/IEC 27000:2018(en) and https://csrc.nist.gov/glossary/term/availability
- <203> **Consent mechanism**: The technical and organisational process by which an organisation requests, records, and manages data subject consent for personal data processing. Consent mechanisms must align with the legal basis of processing, and support traceability, revocability, and enforcement. They are fundamental to privacy compliance and user trust.
- <204> **Consultant**: A consultant provides expert advice to organisations to improve performance, solve problems, and support change. This includes auditing procedures, advising management, and proposing implementation plans. Reference: https://www.brightnetwork.co.uk/career-path-guides/consulting/what-management-consulting/
- <205> **C-SCRM**: Cybersecurity Supply Chain Risk Management is a systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures. Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1305.ipd.pdf
- <206> **Cybersecurity**: Preservation of confidentiality, integrity and availability of information in cyberspace. It includes technologies, practices and policies to prevent or respond to cyber threats. Reference: ISO/IEC 27032:2012(en) and https://www.ibm.com/think/topics/cybersecurity

- <207> **Data Localization**: A concern with Data Protection. A mandatory legal requirement for data to be stored within a specific country. Reference: https://doi.org/10.1787/7fbaed62-en, https://www.atlanticcouncil.org
- <208> **Data Privacy**: The right of individuals to control how their personal information is collected and used. Reference: https://iapp.org/about/what-is-privacy/
- <209> **Data Residency**: A concern with Data Protection. Where a business, industry body or government specifies that their data is stored in a geographical location of their choice, usually for regulatory or policy reasons. A decision by businesses to store data in a specific geographical location. Once an organization chooses a location for its data, it is subject to data sovereignty. Reference: https://www.insightsforprofessionals.com/it/storage/data-sovereignty-data-residency-data-localization
- <210> **Data Retention**: Keeping records in accordance with legal, regulatory or operational requirements. Reference: ISO 30300:2020(en) Information and documentation - Records management - Core concepts and vocabulary
- <211> **GDPR**: General Data Protection Regulation is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). Reference: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
- <212> **Governance of IT**: Information Technology - system by which the current and future use of IT is directed and controlled. Reference: ISO/IEC 38500:2015(en) Information technology - Governance of IT for the organization.
- <213> **HR**: Human Resources refers to the people who provide labour and services to achieve organisational goals. Reference: ISO 30400:2016(en) Human resource management - Vocabulary
- <214> **IAM**: Identity and Access Management**: security and business discipline that includes multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons, while keeping unauthorized access and fraud at bay. Reference: https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam
- <215> **InfoSec**: Information Security involves safeguarding the confidentiality, integrity and availability of information (the CIA triad), and may also involve authenticity, accountability, and non-repudiation. Reference: ISO/IEC 27000:2018(en)
- <216> **ISMS**: Information Security Management System is a set of processes to manage information security risks, including incident detection, response, and learning. Reference: ISO/IEC 27000:2018(en)
- <217> **ITSM**: IT Service Management involves practices and standards for managing IT services throughout their lifecycle, aiming at value delivery to stakeholders. Reference: https://www.axelos.com/certifications/itil-service-management/what-is-it-service-management
- <218> **MDR**: Managed Detection and Response (MDR) denotes outsourced cybersecurity services designed to protect your data and assets even if a threat eludes common organizational security controls. https://www.gartner.com/reviews/market/managed-detection-and-response-services

- <219> **MSP**: A Managed Service Provider delivers IT services such as infrastructure, network, or security management on an ongoing basis. Reference: https://www.gartner.com/en/information-technology/glossary/msp-management-service-provider and https://www.techtarget.com/searchitchannel/definition/managed-service-provider
- <220> **MSSP**: A Managed Security Service Provider offers outsourced monitoring and management of security services like firewalls, VPNs, and threat detection. Reference: https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider
- <221> **Opt-in**: A consent mechanism in which the data subject must take an explicit, affirmative action to authorise the processing of their personal data. Under GDPR, opt-in is required for most non-essential or sensitive data uses, such as marketing, profiling, and data sharing. Valid opt-in consent must be freely given, specific, informed, and unambiguous.
- <222> **Opt-out**: A consent mechanism in which the data subject is included by default in a data processing operation but has the option to decline or withdraw consent. Under GDPR, opt-out is only acceptable under specific lawful bases and must ensure ease of refusal, transparency, and accountability. Improper use of opt-out undermines data subject autonomy and may breach regulatory requirements.
- <223> **PII**: Personally Identifiable Information refers to any information that identifies or could identify a natural person. Reference: ISO/IEC 29100:2011(en) Information technology - Security techniques - Privacy framework
- <224> **PII Controller**: The entity that determines the purposes and means of processing PII, excluding individuals using it for personal purposes. Reference: ISO/IEC 29100:2011(en)
- <225> **PII Principal**: The natural person to whom the PII relates; also called data subject in some legal contexts. Reference: ISO/IEC 29100:2011(en)
- <226> **PII Processor**: Entity that processes PII on behalf of and under instruction from a PII controller. Reference: ISO/IEC 29100:2011(en)
- <227> **PIMS**: A Privacy Information Management System is an ISMS that also addresses the protection of privacy in PII processing. Reference: ISO/IEC 27701:2019(en)
- <228> **Privacy-by-design**: A principle requiring that privacy and data protection are integrated from the earliest stages of system design. It includes applying minimisation, secure defaults (e.g. opt-in rather than opt-out), and user control features as part of both technical architecture and governance practices. Mandated under GDPR Article 25.
- <229> **Public Procurement**: The process by which public bodies acquire goods, services, or works from private providers. Reference: https://ec.europa.eu/growth/single-market/public-procurement_en
- <230> **SBOM**: A Software Bill of Materials is a complete list of components used in a software product, including open-source libraries and their metadata. Reference: https://www.paloaltonetworks.com/cyberpedia/what-is-software-bill-materials-sbom

- <231> **Supply Chain**: A set of coordinated functions and processes to manage the flow of goods, services, and information, including IT-specific supply chain security considerations. Reference: https://www.gartner.com/en/information-technology/glossary/supply-chain
- <232> **Vendor Assessment**: The process of evaluating potential vendors based on quality, risk, and compliance to determine suitability for collaboration. Reference: https://nira.com/vendor-assessment/
- <233> **Vulnerability Management**: A continuous process of identifying, classifying, prioritising, and remediating security vulnerabilities in systems. Reference: https://www.cisa.gov/news-events/news/what-vulnerability-management
- <234> **Zero Trust**: A security model based on the principle of not trusting any user or device by default, even if inside the network perimeter. Reference: https://www.nist.gov/publications/zero-trust-architecture.
- <301> **BPM (Business Process Management)**: A discipline involving the combination of modelling, automation, execution, control, measurement, and optimisation of business activity flows to support enterprise goals. Reference: https://www.omg.org/bpmn
- <302> **Contingent Workforce**: People who are engaged as casual labour, flexible workers, or contract-based professionals. Reference: ISO 30400:2016
- <303> **Cyber Resilience**: The ability of an organisation to continuously deliver the intended outcome despite adverse cyber events. Reference: ENISA
- <305> **Data Protection**: Legal and technical measures aimed at ensuring the confidentiality, integrity, and lawful processing of personal or sensitive information, in compliance with applicable regulations. Reference: https://www.snia.org/education/what-is-data-protection
- <306> **Enterprise IT Infrastructure**: The entire set of hardware, software, networks, facilities, and related equipment used to develop, test, operate, monitor, manage, and support IT services. Reference: https://searchdatacenter.techtarget.com/definition/IT-infrastructure
- <307> **ERM**: Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. Reference: https://www.coso.org/documents/coso-erm-executive-summary.pdf
- <308> **Failover**: The capability to switch to a redundant or standby computer server, system, hardware component, or network upon the failure or abnormal termination of the previously active application, server, or system. Reference: https://www.ibm.com/cloud/learn/failover
- <309> **ICT Asset Management**: A systematic process of deploying, operating, maintaining, upgrading, and disposing of IT assets cost-effectively. Reference: ISO/IEC 19770-1:2017
- <310> **Incident Response**: An organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident. Reference: https://www.cisa.gov/incident-response

- <311> **IT Operations Management (ITOM)**: Activities that manage the provisioning, capacity, performance, and availability of computing, networking, and application resources. Reference: https://www.bmc.com/it-solutions/it-operations-management.html
- <312> **IT Service Continuity Management (ITSCM)**: The process responsible for managing risks that could seriously impact IT services. Reference: ITIL v3
- <313> **ITSM (IT Service Management)**: A set of policies, processes, and procedures for delivering IT services to end users. Reference: ISO/IEC 20000-1:2018
- <314> **Logging**: The process of recording events, messages, and other data points during software execution or system operation. Reference: NIST SP 800-92
- <315> **Maintenance Window**: A scheduled period of time during which planned outages and changes to production systems may occur. Reference: https://www.ibm.com/docs/en/i/7.4?topic=definitions-maintenance-window
- <316> **Monitoring**: A process to detect, assess, and understand the current operational status of IT systems and services. Reference: https://www.datadoghq.com/knowledge-center/what-is-it-monitoring
- <317> **Operational Risk**: The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Reference: Basel II
- <318> **Operational Technology (OT)**: Hardware and software that detects or causes changes through direct monitoring and control of physical devices, processes, and events in an organisation. OT is commonly used in industrial control systems (ICS) such as manufacturing, energy, water treatment, and transportation. Reference: https://www.cisa.gov/resources-tools/resources/what-operational-technology
- <319> **Patch Management**: The process of distributing and applying updates to software. Reference: https://www.nist.gov/programs-projects/patch-management
- <320> **Penetration Testing**: An authorised simulated cyberattack on a system to evaluate its security. Reference: https://owasp.org/www-community/penetration_testing
- <321> **Ransomware**: A type of malicious software designed to block access to a computer system until a sum of money is paid. Reference: ENISA
- <322> **Redundancy**: The duplication of critical components or functions of a system with the intention of increasing reliability. Reference: https://www.techopedia.com/definition/25504/redundancy
- <323> **Service Level Agreement (SLA)**: A documented agreement between a service provider and a customer that identifies services and performance expectations. Reference: ISO/IEC 20000-1:2018
- <324> **Shadow IT**: Information technology systems and solutions built and used inside organisations without explicit organisational approval. Reference: https://www.gartner.com/en/information-technology/glossary/shadow-it

- <325> **Technical debt**: Technical debt, or tech debt, is the implied cost incurred when businesses do not fix problems that will affect them in the future. Reference: https://www.techtarget.com/whatis/definition/technical-debt
- <326> **XaaS (Everything as a Service)**: A general category of services related to cloud computing and remote access that includes PaaS (Platform as a Service), IaaS (Infrastructure as a Service), and SaaS (Software as a Service). Reference: NIST SP 800-145
- <327> **xOps**: An umbrella term for various "as code" operational practices such as DevOps, SecOps, AIOps, and MLOps, aimed at improving automation, collaboration, and agility across IT and business operations. Reference: https://www.gartner.com/en/articles/what-you-need-to-know-about-xops
- <401> **AI (Artificial Intelligence)**: Technology that enables machines to perform tasks that typically require human intelligence, such as reasoning, learning, and decision-making. Reference: https://www.ibm.com/topics/artificial-intelligence
- <402> **AI governance**: The set of policies, structures, and responsibilities that guide the development, deployment, and oversight of AI and algorithmic systems within an organisation. It ensures that AI use aligns with institutional goals, legal obligations, and societal values, integrating considerations of transparency, fairness, and risk control.
- <403> **Algorithmic system**: A software-based mechanism that makes or influences decisions using predefined rules, statistical models, or learning algorithms. Algorithmic systems are increasingly embedded in organisational processes and strategic decision-making. They raise governance challenges related to opacity, bias, and accountability, and require clear oversight frameworks.
- <404> **CAF (Cloud Adoption Framework)**: A Cloud Adoption Framework provides a baseline methodology for organisations to plan and implement cloud technologies effectively. Reference: https://cloud.netapp.com/blog/cvo-blg-top-3-cloud-adoption-frameworks
- <405> **Cloud Foundation**: A structured set of policies, technical components, and governance practices that enable secure and scalable cloud usage across business units.
- <406> **Capability-Based Planning**: A strategic planning approach that focuses on the identification, development, and coordination of the capabilities an organisation needs to achieve its objectives. Reference: https://www.gartner.com/en/information-technology/glossary/capability-based-planning
- <407> **CapEx (Capital Expenditure)**: Funds used by an organisation to acquire, upgrade, and maintain physical assets such as property, industrial buildings, or equipment. Reference: https://www.investopedia.com/terms/c/capitalexpenditure.asp
- <408> **Change Readiness**: The degree to which an organisation is mentally, culturally, and operationally prepared to implement and sustain strategic change. Reference: https://www.prosci.com/resources/articles/organizational-change-readiness
- <409> **CIAM (Customer Identity and Access Management)**: A subset of identity management focused on managing the identity, authentication, and authorisation of external users such as customers or partners. Reference: https://securityintelligence.com/articles/what-is-ciam-and-why-it-matters

- <411> **Digital Capability**: The ability of an organisation to leverage digital technologies to improve business performance and outcomes. Reference: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-about-deloitte-digital-capability-framework.pdf
- <412> **Digital Maturity**: A measure of an organisation's ability to respond to digital trends, transformation, and innovation effectively. Reference: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-about-deloitte-digital-maturity-model.pdf
- <413> **Digital Sovereignty**: The capacity of a state or organisation to have control over its digital infrastructure, data, and technologies (Data Sovereignity; Cloud Sovereignity) Reference: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273
- <414> **Digital Strategy**: A plan that outlines how an organisation will use digital technologies to achieve its business goals. Reference: https://www.bcg.com/publications/2020/digital-strategy-roadmap-for-digital-transformation
- <415> **Digital Wallet**: A digital wallet is a storage place of secure information necessary to authenticate a user and initiate an authorization process to make a transaction to purchase goods and services. A secure application used to store and manage digital identity credentials issued under the eIDAS 2.0 regulation. Reference: https://www.gartner.com/en/information-technology/glossary/digital-wallet
- <416> **Disruptive Innovation**: Innovation that creates a new market and value network, eventually disrupting existing markets and displacing established market-leading firms, products, and alliances. Reference: https://claytonchristensen.com/key-concepts/
- <417> **DPIA (Data Protection Impact Assessment)**: A process to help organisations identify and minimise the data protection risks of a project, particularly when introducing new technologies or data processing practices. Reference: https://edps.europa.eu/data-protection-impact-assessment-dpia_en
- <418> **eIDAS**: stands for electronic Identification, Authentication and Trust Services. The eIDAS Regulation established the framework to ensure that electronic interactions between businesses are safer, faster and more efficient, no matter the European country they take place in. It is a European Regulation that created one single framework for electronic identification (eID) and trust services, making it more straightforward to deliver services across the European Union. Reference: https://digital-strategy.ec.europa.eu/en/policies/discover-eidas
- <419> **Electronic Identification**: A digital solution for proof of identity of citizens or organizations. Reference: https://www.igi-global.com/dictionary/electronic-identification-eid/100546
- <420> **Enterprise Architecture (EA)**: A conceptual blueprint that defines the structure and operation of an organisation through its IT and business alignment. Reference: https://www.opengroup.org/ea/togaf
- <421> **Executive Sponsorship**: The active and accountable leadership role played by senior executives to champion and support projects or change initiatives, ensuring alignment with strategic

goals and removing obstacles to success. Reference: https://www.prosci.com/resources/articles/role-of-executive-sponsor

- <422> **Explainability**: The capacity to account for how and why an algorithmic system produces a given output or decision. Explainability is essential for legal compliance, operational effectiveness, and stakeholder trust, particularly in sectors where decisions affect individuals' rights or well-being. It involves both technical design choices and organisational communication practices.
- <423> **Human-in-the-loop**: A governance and design principle in which human actors retain the ability to understand, intervene in, or override the decisions of automated systems. Especially important in high-risk applications, this principle supports accountability, ethical alignment, and error mitigation.
- <424> **Hyperautomation**: A business-driven, disciplined approach that organizations use to rapidly identify, vet and automate as many business and IT processes as possible. Hyperautomation involves the orchestrated use of multiple technologies, tools or platforms... Reference: https://www.gartner.com/en/information-technology/glossary/hyperautomation
- <425> **IT Investment Portfolio**: A collection of IT assets, projects, and capabilities grouped for the purpose of strategic investment and resource allocation. Reference: https://www.gartner.com/en/information-technology/glossary/it-portfolio-management
- <426> **IT Strategy**: A comprehensive plan that outlines how technology should be used to meet IT and business goals. Reference: https://www.cio.com/article/274752/strategy-how-to-develop-an-it-strategy.html
- <427> **OpEx (Operational Expenditure)**: The ongoing cost for running a product, business, or system. Reference: https://www.investopedia.com/terms/o/operating_expense.asp
- <428> **Organisational Agility**: The ability of an organisation to renew itself, adapt quickly to change, and succeed in a rapidly changing, ambiguous environment. Reference: https://www.mckinsey.com/business-functions/organization/our-insights/the-keys-to-organizational-agility
- <429> **Portfolio**: portfolio**: collection of portfolio components (3.16) grouped together to facilitate their management to meet strategic objectives - [SOURCE:ISO/TR 21506:2018, 3.42] portfolio component**: project (3.20), programme (3.18), portfolio (3.15) or other related work [SOURCE:ISO/TR 21506:2018, 3.43] Reference: ISO 21502:2020(en) Project, programme and portfolio management - Guidance on project management
- <430> **Programme**: programme**: group of programme components (3.19) managed in a coordinated way to realize benefits (3.2) [SOURCE:ISO/TR 21506:2018, 3.50] programme component**: project (3.20), programme (3.18) or other related work [SOURCE:ISO/TR 21506:2018, 3.52] Reference: ISO 21502:2020(en) Project, programme and portfolio management - Guidance on project management
- <431> **Project**: temporary endeavour to achieve one or more defined objectives [SOURCE:ISO/TR 21506:2018, 3.59, modified - The words "created to produce agreed deliverables" have been replaced by "to achieve one or more defined objectives".] Reference: ISO 21502:2020(en) Project, programme and portfolio management - Guidance on project management

- <432> **Project Management Office (PMO)**: an organisational unit established to standardise and support the governance, planning, execution, and monitoring of projects and programmes. Reference: ...
- <433> **RegTech**: The use of technology (particularly information technology) to ensure compliance with monitoring of and reporting on regulatory requirements. Reference: https://www.fca.org.uk/firms/innovation/regtech
- <434> **Risk-based classification of AI**: A regulatory approach, exemplified by the EU AI Act, that categorises AI systems based on the level of risk they pose to safety, rights, or public interests. Obligations for governance, oversight, and compliance increase with the assessed risk level, guiding how AI is designed, deployed, and monitored.
- <435> **Roadmap**: A strategic plan that defines a goal or desired outcome and includes the major steps or milestones needed to reach it. Reference: https://www.productplan.com/learn/what-is-a-product-roadmap/
- <436> **Start-up**: A temporary organisation formed to search for a repeatable and scalable business model, often operating under conditions of extreme uncertainty. Reference: Eric Ries, The Lean Startup
- <437> **Strategic Alignment**: The process of aligning an organisation's structure, resources, and culture with its strategy and external environment. Reference: https://www.shrm.org/resourcesandtools/hr-topics/organizational-and-employee-development/pages/strategic-alignment.aspx
- <438> **Strategic Planning**: An organisational management activity used to set priorities, focus energy and resources, and ensure that employees and other stakeholders are working toward common goals. Reference: https://balancedscorecard.org/strategic-planning-basics/
- <439> **Strategy**: plan to achieve a long-term or overall objective (3.7.1) organization's approach to achieving its objectives Reference: ISO 9000:2015(en) Quality management systems - Fundamentals and vocabulary / ISO 30400:2016(en) Human resource management - Vocabulary
- <440> **Sustainability Strategy**: A plan for how an organisation will create long-term stakeholder value by pursuing opportunities and managing risks related to environmental, social, and governance (ESG) factors. Reference: https://www2.deloitte.com/global/en/pages/about-deloitte/articles/sustainability-strategy.html
- <441> **Technology Due Diligence**: The structured evaluation of an organisation's technological landscape, including its systems, infrastructure, governance, capabilities, risks, and future-readiness.
- <442> **Target Operating Model (TOM)**: A blueprint of a firm's business vision that aligns operating capabilities and strategic objectives. Reference: https://businesscasestudies.co.uk/what-is-the-target-operating-model-tom/
- <443> **Technology Research**: The collection, analysis, and understanding of data related to tech products. Technology research companies (such as Gartner, IDC, Forrester, etc.) conduct research services for clients to gain a better understanding of a given tech market, identify growing tech sectors; understand the competition, decipher new market trends, evaluate competitor products,

gauge demand for a new or existing product; improve marketing messaging to best reach the consumer, etc. Reference: https://www.greenbook.org/market-research-firms/high-technology#p1%200

- <444> **TRL (Technology Readiness Level)**: Technology readiness levels (TRLs) are a method for estimating the maturity of technologies during the acquisition phase of a program, developed at NASA during the 1970s. The use of TRLs enables consistent, uniform discussions of technical maturity across different types of technology Reference: https://en.wikipedia.org/wiki/Technology_readiness_level
- <445> **Value Proposition**: A statement that clearly identifies what benefits a company's products or services deliver to customers, and how it differentiates from competitors. Reference: https://www.strategyzer.com/canvas/value-proposition-canvas
- <446> **VUCA**: An acronym that stands for Volatility, Uncertainty, Complexity, and Ambiguity, used to describe challenging and unpredictable business environments. Reference: https://hbr.org/2014/01/what-vuca-really-means-for-you