ISMS Abbreviation Guidance (Glossary)

ABAC – Anti-Bribery and Anti-Corruption
Definition: Policies and controls prohibiting bribery/corruption.
Simple: Rules to ensure honest, lawful business conduct.

AES-256 – Advanced Encryption Standard (256-bit)
Definition: NIST-approved symmetric encryption standard using 256-bit keys.
Simple: Strong encryption to keep data unreadable if stolen.

AMO – Approved Maintenance Organisation
Definition: Maintenance organisation approved under aviation regulation (e.g., EASA Part-145).
Simple: A certified maintenance company.

API – Application Programming Interface
Definition: Rules/tools enabling software systems to communicate.
Simple: A connector that lets apps talk to each other.

AV – Antivirus
Definition: Endpoint software that detects/removes malware.
Simple: App that spots and stops viruses/malware.

BCP – Business Continuity Plan
Definition: Plan to keep operations running during disruption.
Simple: How we keep working when things break.

BCRs – Binding Corporate Rules
Definition: GDPR mechanism allowing intra-group data transfers outside EEA.
Simple: Group-wide privacy rules for moving data abroad legally.

BIA – Business Impact Analysis
Definition: Assessment of process/system criticality and outage impact.
Simple: Study of what's critical and how downtime hurts.

BIOS – Basic Input/Output System
Definition: Firmware that initialises hardware at system start.
Simple: Low-level startup software on computers.

BEC – Business Email Compromise
Definition: Fraud using executive/supplier impersonation by email.
Simple: Scam emails pretending to be the boss/supplier.

CAB – Change Advisory Board
Definition: Group that assesses/approves significant changes.
Simple: The team that green-lights important IT changes.

CIS (Benchmarks) – Center for Internet Security
Definition: Industry-standard secure configuration baselines.
Simple: “Gold standard” security settings.

CI/CD – Continuous Integration / Continuous Deployment
Definition: Automated software build, test, release pipelines.
Simple: The assembly line for safe software updates.

CSPM – Cloud Security Posture Management
Definition: Tools that detect misconfigurations in cloud platforms.
Simple: Cloud config checker and fixer.

CVSS – Common Vulnerability Scoring System
Definition: Standard 0–10 severity rating for vulnerabilities.
Simple: A score that shows how bad a flaw is.

DAST – Dynamic Application Security Testing
Definition: Security testing of running web/apps from outside-in.
Simple: “Black-box” hacking tests of live apps.

DDoS – Distributed Denial of Service
Definition: Attack that floods services with traffic to cause outage.
Simple: Overloading a site so no one can use it.

DPA – Data Processing Agreement
Definition: GDPR contract defining controller/processor duties.
Simple: Legal terms for how a supplier handles personal data.

DPO – Data Protection Officer
Definition: Role overseeing GDPR compliance.
Simple: The organisation’s privacy lead.

DPIA – Data Protection Impact Assessment
Definition: GDPR risk assessment for high-risk processing (Art. 35).
Simple: Privacy risk check before a new project.

DRP – Disaster Recovery Plan
Definition: Plan to restore IT/services after major incident.
Simple: How IT comes back after disaster.

EASA – European Union Aviation Safety Agency
Definition: EU aviation regulator issuing Part-145/Part-CAMO rules.
Simple: Europe's aviation safety rule-maker.

EDR – Endpoint Detection & Response
Definition: Endpoint tool that detects/responds to threats on devices.
Simple: Laptop/server watchdog that can isolate infections.

EEA – European Economic Area
Definition: EU + Iceland, Liechtenstein, Norway.
Simple: The region where GDPR freely allows data flows.

E&O – Errors & Omissions (Insurance)
Definition: Professional liability insurance for service errors.
Simple: Insurance covering costly mistakes.

GDPR – General Data Protection Regulation
Definition: EU data protection law.
Simple: The EU's privacy rulebook.

HQ – Headquarters
Definition: Primary corporate office location.
Simple: Main office.

HSM – Hardware Security Module
Definition: Tamper-resistant device safeguarding crypto keys.
Simple: A locked safe for encryption keys.

HSTS – HTTP Strict Transport Security
Definition: Policy forcing HTTPS/TLS for web connections.
Simple: Browser rule: "always use secure connection."

IAM – Identity & Access Management
Definition: Processes/tech managing user identities and access.
Simple: Who can log in and what they can do.

IdP – Identity Provider
Definition: Central service that authenticates users for apps.
Simple: The login gatekeeper.

IDTA – International Data Transfer Agreement (UK)
Definition: UK mechanism (post-Brexit) for extra-EEA data transfers.
Simple: UK's legal form for sending data abroad.

IR – Incident Response (Plan/Process)
Definition: Steps to detect, contain, eradicate, and recover from incidents.
Simple: Our playbook for cyber incidents.

ISO/IEC 27001
Definition: International standard for ISMS requirements.
Simple: The certificate for good information security management.

ISMM – Information Security Management Manual
Definition: Controlled manual documenting the ISMS.
Simple: The handbook of our security system.

ISM – Information Security Manager
Definition: Role responsible for ISMS implementation/oversight.
Simple: The person in charge of security controls.

JML – Joiner / Mover / Leaver
Definition: Identity lifecycle for onboarding, role change, leavers.
Simple: Create, change, or remove user access on time.

KMS – Key Management System
Definition: System to generate/store/rotate/revoke crypto keys.
Simple: Software that manages encryption keys.

KPI – Key Performance Indicator
Definition: Metric measuring performance (e.g., MTTD/MTTR).
Simple: A score that shows how we're doing.

LMS – Learning Management System
Definition: Platform for training delivery and records.
Simple: Online training system.

MFA – Multi-Factor Authentication
Definition: Login using two or more factors (something you know/have/are).
Simple: Password + code/app/biometric.

MDM – Mobile Device Management
Definition: Tools/policies to secure laptops/phones/tablets.
Simple: Enforce encryption, screen lock, remote wipe.

MSP – Managed Service Provider
Definition: External company managing IT/security services.
Simple: Outsourced IT/security support.

MTTD – Mean Time to Detect
Definition: Average time to detect an incident.
Simple: How fast we spot problems.

MTTR – Mean Time to Respond/Recover
Definition: Average time to contain/recover from incident.
Simple: How fast we fix problems.

NAC – Network Access Control
Definition: Controls that only allow compliant devices onto networks.
Simple: Only approved devices can connect.

NDA – Non-Disclosure Agreement
Definition: Legal agreement to keep shared information confidential.
Simple: Promise not to share secrets.

NC – Non-Conformity
Definition: Failure to meet a stated requirement.
Simple: A control gap that must be fixed.

NIST – National Institute of Standards and Technology
Definition: US body publishing cybersecurity standards (e.g., password/MFA guidance).
Simple: Widely used security best-practice source.

OS – Operating System
Definition: Core software (Windows, Linux, macOS) running on hardware.
Simple: The system that runs your computer.

PAM – Privileged Access Management
Definition: Securing/administering high-privilege accounts.
Simple: Extra protection for admin users.

PEP – Politically Exposed Person
Definition: Person with prominent public function; higher AML risk.
Simple: Public figures requiring extra checks.

PKI – Public Key Infrastructure
Definition: Framework managing certificates and crypto keys.
Simple: The system behind HTTPS, VPN certs, and digital signatures.

PR – Public Relations
Definition: Managing external communications, especially in crises.
Simple: How we communicate with the outside world.

RBAC – Role-Based Access Control
Definition: Permissions assigned to roles rather than individuals.
Simple: Your job role decides your access.

RACI – Responsible, Accountable, Consulted, Informed
Definition: Responsibility assignment matrix.
Simple: Who does it, who owns it, who's asked, who's told.

RoPA – Record of Processing Activities
Definition: GDPR Article 30 register of personal data processing.
Simple: Log of what personal data we use and why.

RPO – Recovery Point Objective
Definition: Maximum acceptable data loss (time since last backup).
Simple: How much data we can afford to lose.

RTO – Recovery Time Objective
Definition: Maximum acceptable downtime before restore.
Simple: How quickly a system must be back.

SBOM – Software Bill of Materials
Definition: List of components/dependencies in software.
Simple: Ingredients list for software.

SCCs – Standard Contractual Clauses
Definition: EU contractual safeguards for extra-EEA data transfers.
Simple: EU-approved legal terms for sending data abroad.

SecOps – Security Operations
Definition: Operational security monitoring/response function.
Simple: The team that watches and responds to threats.

SIEM – Security Information & Event Management
Definition: Centralised log collection, correlation, alerting, reports.
Simple: The security alarm hub.

SLA – Service Level Agreement
Definition: Contracted performance targets (uptime, response).
Simple: The supplier's minimum service promises.

SLSA – Supply-chain Levels for Software Artifacts
Definition: Framework to assess/build software supply-chain integrity.
Simple: A maturity ladder for secure software supply chains.

SFTP – SSH File Transfer Protocol
Definition: Encrypted file transfer protocol over SSH.
Simple: Secure way to move files.

SOC 2 Type II – System & Organization Controls (Type II)
Definition: Independent attestation of control design **and** operating effectiveness over time.
Simple: External audit proving controls worked over months.

SOW – Statement of Work
Definition: Contract schedule describing scope/deliverables/timelines.
Simple: The detailed "what we'll do" part of the contract.

SSO – Single Sign-On
Definition: One login granting access to multiple systems.
Simple: Log in once, access many apps.

TIA – Transfer Impact Assessment
Definition: GDPR risk assessment for third-country data transfers (post-Schrems II).
Simple: Check that data stays protected when sent outside the EEA.

TLS – Transport Layer Security
Definition: Protocol securing data in transit (successor to SSL).
Simple: Encryption for data moving over networks.

UEBA – User & Entity Behavior Analytics
Definition: Analytics detecting abnormal user/device behaviour.
Simple: Tools that spot actions out of character.

UPS – Uninterruptible Power Supply
Definition: Battery backup to keep systems running during power loss.
Simple: Short-term power to prevent sudden shutdowns.

VDP – Vulnerability Disclosure Policy
Definition: Public process for reporting security issues responsibly.
Simple: How external researchers tell us about bugs.

VPN – Virtual Private Network
Definition: Encrypted tunnel for remote/private network access.
Simple: Secure connection into our network.

HTTPS – HyperText Transfer Protocol Secure
Definition: HTTP over TLS/SSL for encrypted web traffic.
Simple: The padlock in the browser.

CREST – Council of Registered Ethical Security Testers
Definition: Pen-test accreditation body.
Simple: Recognised badge for trusted pen-testers.

TIGER (Scheme)
Definition: UK certification scheme for penetration testers.
Simple: Another recognised pen-tester qualification.

IA – Internal Audit
Definition: Independent internal review of controls/processes.
Simple: Our own compliance checkers