Executive Development Programme in Leadership Strategy for Commercial Crime Statutory Offences Commanders

Risk Assessment and Threat Analysis

A Adverse Event – an incident or outcome that negatively impacts an organization's security posture, often used in risk registers to track events such as data breaches or fraud. Related terms: Incident, loss event, impact. Example: An unauthorized access attempt that results in data exfiltration is recorded as an adverse event.

Actual Likelihood – the probability that a specific threat will materialize, based on historical data and current controls. It differs from perceived likelihood, which may be biased. Example: A company that has experienced three phishing attacks in the past year may assign a higher actual likelihood to future phishing attempts.

Asset – any resource, tangible or intangible, that has value to the organization and therefore requires protection. Assets include physical property, information, reputation, and personnel. Related terms: Asset value, critical asset, asset inventory.

Asset Valuation – the process of assigning monetary or strategic worth to an asset. Methods include cost replacement, market value, and risk-based valuation. Example: Valuing customer data at the cost of potential regulatory fines plus reputational damage.

Attack Vector – the path or method used by a threat actor to deliver a malicious payload or exploit a vulnerability. Common vectors include phishing emails, compromised websites, and insider access. Related terms: Delivery mechanism, exploit chain.

Baseline Risk – the level of risk that exists before any mitigation measures are applied. Establishing a baseline helps measure the effectiveness of controls. Example: The baseline risk of cash theft in a retail outlet may be high before installing CCTV.

Behavioral Analytics – the use of statistical models to detect abnormal user behavior that may indicate a security threat. Often applied to identify insider threats or compromised accounts. Related terms: Anomaly detection, user-entity behavior analytics (UEBA).

Black-Box Testing – a risk-assessment technique where the tester has no prior knowledge of the system's internal structure, simulating an external attacker's perspective. Contrast with white-box testing.

Blended Threat – a combination of multiple threat types (e.G., Malware plus social engineering) used to increase the chance of success. Example: A ransomware campaign that begins with a phishing email and follows with a drive-by download.

Business Impact Analysis (BIA) – a systematic process to determine the effects of disruption on business functions, identifying critical processes and recovery priorities. Related terms: Continuity planning, impact assessment.

Capability Maturity Model Integration (CMMI) – a framework for assessing and improving organizational processes, including risk-management practices. Higher maturity levels indicate more robust, repeatable risk processes.

Catastrophic Risk – a risk that could cause severe, organization-wide damage, potentially threatening survival. Examples include large-scale fraud schemes or coordinated cyber-attacks on critical infrastructure.

Cause-Effect Diagram – also known as an Ishikawa or fishbone diagram; a visual tool to explore root causes of a risk or incident. Useful for identifying underlying factors in commercial crime.

Chain of Custody – the documented process that tracks evidence from collection through analysis, ensuring its integrity for legal or disciplinary action. Critical in investigations of statutory offences.

Clearance Level – an authorization tier that defines the extent of information an individual may access. Aligns with the principle of least privilege to reduce insider threat exposure.

Compliance Gap – a discrepancy between current practices and regulatory or statutory requirements. Identifying gaps is a core step in risk assessments for commercial crime statutes.

Confidentiality – one of the CIA triad principles; ensures that information is accessible only to those authorized to view it. Breaches of confidentiality often constitute statutory offences.

Consequence – the outcome or impact resulting from a risk event, measured in financial loss, reputational damage, legal penalties, or operational disruption. Distinct from likelihood.

Control Effectiveness – the degree to which a security control mitigates a specific risk, often measured through testing or audit results. Example: Multifactor authentication reducing credential-theft likelihood by 70 %.

Control Objective – a high-level statement of what a control aims to achieve, such as “prevent unauthorized access to financial systems.” Serves as a basis for selecting specific controls.

Counterfeit Documentation – forged or altered documents used to facilitate fraud, such as falsified invoices or identity papers. Detection relies on verification controls and forensic analysis.

Critical Infrastructure – systems and assets essential to national security, public health, or economic stability. Threat analysis for these assets often involves higher-level government guidance.

Cyber Threat Intelligence (CTI) – data about existing or emerging threats that is collected, analyzed, and

disseminated to inform defensive actions. Sources include open-source feeds, industry sharing groups, and internal logs.

Data Breach – unauthorized acquisition, access, use, or disclosure of data. In commercial crime contexts, breaches may trigger statutory reporting obligations and fines.

Data Classification – the process of categorizing data based on sensitivity and impact of loss. Common categories: Public, internal, confidential, restricted. Supports appropriate control selection.

Deception Technology – tools such as honeypots or honeytokens that lure attackers, providing early warning and intelligence. Helps in assessing threat tactics.

Defense-in-Depth – a layered security strategy that employs multiple controls across people, processes, and technology to reduce reliance on any single measure.

Denial-of-Service (DoS) Attack – an attempt to make a service unavailable by overwhelming it with traffic. While primarily a cyber threat, DoS can be used as a smokescreen for fraud.

Detection Capability – the ability of an organization to identify a threat or breach in a timely manner. Measured by mean time to detect (MTTD).

Deterrence – measures designed to discourage potential offenders, such as visible surveillance, strict penalties, or publicized enforcement actions.

Disaster Recovery (DR) – a set of policies and procedures to restore IT systems after a catastrophic event. Complements business continuity planning.

Disruption Probability – the likelihood that an event will interrupt normal operations. Often expressed as a percentage or a rating scale.

Domain-Specific Threat Model – a threat model tailored to a particular industry or business function, such as retail fraud or financial services money-laundering.

Due Diligence – the process of investigating a partner, vendor, or transaction to identify potential risks before committing resources. Essential for third-party risk management.

Economic Loss – direct monetary loss resulting from a risk event, such as stolen cash, fraud penalties, or remediation costs.

Emergency Response Plan (ERP) – a documented set of actions to take immediately after an incident to protect life, property, and evidence.

Enterprise Risk Management (ERM) – an organization-wide approach to identifying, assessing, and

managing risks across all functions, aligning with strategic objectives.

Escalation Procedure – defined steps for raising an incident to higher authority levels when severity thresholds are crossed.

Event Correlation – the process of linking multiple security events to identify patterns indicative of a larger attack or fraud scheme.

Ex Ante Assessment – risk analysis performed before a decision or activity, used to inform preventive measures.

Ex Post Evaluation – review of risk outcomes after an event, providing lessons learned and informing future controls.

Exploit – a piece of code or technique that takes advantage of a vulnerability. In commercial crime, exploits may include social-engineering scripts or technical vulnerabilities in payment systems.

External Threat Actor – individuals or groups outside the organization that pose a risk, such as organized crime syndicates, hacktivists, or competitor spies.

False Positive – an alert or detection that incorrectly indicates a threat, leading to unnecessary investigation.

Financial Crime – illegal activities involving monetary gain, including fraud, money laundering, bribery, and embezzlement. Statutory offences often define specific thresholds and reporting duties.

Forensic Analysis – systematic examination of digital or physical evidence to reconstruct events and identify perpetrators. May involve disk imaging, log review, or document verification.

Frequency Rating – a numeric value assigned to how often a particular risk is expected to occur, used in risk matrices.

Geopolitical Threat – risk arising from political instability, sanctions, or international conflicts that can affect commercial operations.

Governance, Risk, and Compliance (GRC) – integrated framework that aligns risk management with regulatory compliance and corporate governance.

Hazard – any source of potential damage, harm, or adverse health effect. In a commercial crime context, hazards include counterfeit currency, insider collusion, and cyber intrusion.

Heat Map – visual representation of risk levels across assets or processes, typically using color gradients to indicate severity.

Impact Assessment – evaluation of the consequences of a risk event, often expressed in financial terms,

operational disruption, or reputational loss.

Incident Response Plan (IRP) – documented procedures for detecting, containing, eradicating, and recovering from security incidents.

Indicator of Compromise (IOC) – artifact observed on a network or system that suggests a breach, such as malicious IP addresses, file hashes, or unusual login patterns.

Information Asset – any piece of data or knowledge that has value, including customer records, intellectual property, and trade secrets.

Information Security Management System (ISMS) – a set of policies and procedures for systematically managing an organization's sensitive data, often aligned with ISO 27001.

Insider Threat – risk posed by employees, contractors, or partners who have authorized access and may misuse it intentionally or unintentionally.

Integrity – a core security principle ensuring that data is accurate, complete, and unaltered without authorization.

Intervention Cost – resources expended to stop or mitigate a risk event while it is occurring, such as hiring investigators or deploying emergency controls.

Key Risk Indicator (KRI) – metric that signals increasing risk exposure, enabling proactive management. Example: A rising number of failed login attempts.

Likelihood – the probability that a threat will exploit a vulnerability. Often expressed qualitatively (low, medium, high) or quantitatively (percentage).

Loss Event – an occurrence that results in a measurable loss, such as theft, fraud, or system downtime.

Loss Expectancy – the anticipated monetary loss from a risk over a defined period, calculated as Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) × Annual Rate of Occurrence (ARO).

Malware – malicious software designed to infiltrate, damage, or disrupt systems. Variants include ransomware, spyware, and Trojan horses.

Managed Risk – risk that has been identified, assessed, and mitigated to an acceptable level as defined by the organization's risk appetite.

Mitigation Strategy – a plan of action to reduce either the likelihood or impact of a risk. Strategies include avoidance, transfer, acceptance, or reduction.

Monitoring Control – a control that continuously observes activities to detect deviations, such as log

aggregation or transaction monitoring.

National Crime Agency (NCA) – a UK law-enforcement body that tackles serious and organized crime, including commercial fraud. Its guidance informs statutory risk assessments.

Net Risk – residual risk after controls have been applied, often expressed as the difference between inherent risk and mitigated risk.

Operational Risk – risk arising from internal processes, people, systems, or external events that affect day-to-day operations.

Opportunity Cost – the benefit foregone by allocating resources to risk mitigation instead of alternative investments.

Organizational Culture – shared values and behaviors that influence how risk is perceived and managed within a company.

Outsourced Service Provider – a third-party entity that delivers a business function; requires due-diligence and contractual controls to manage associated risks.

Penetration Testing – simulated attack performed to evaluate the effectiveness of security controls. Provides insight into exploitable weaknesses.

Perpetrator – the individual or group that carries out a criminal act. In threat analysis, profiling perpetrators helps anticipate tactics.

Physical Security – measures that protect people, assets, and facilities from physical threats, such as locks, guards, and surveillance.

Policy Violation – an action that contravenes an organization's established rules, potentially creating a security gap.

Post-Incident Review – analysis conducted after an event to determine root causes, assess response effectiveness, and update controls.

Predictive Analytics – statistical techniques that forecast future risk trends based on historical data, supporting proactive risk reduction.

Prescribed Safeguard – a control mandated by law or regulation, such as anti-money-laundering (AML) procedures for financial institutions.

Probability Distribution – a mathematical function that describes the likelihood of different outcomes, useful for modeling risk scenarios.

Process Mapping – visual representation of business processes to identify points of vulnerability and control gaps.

Protected Disclosure – a legally protected channel for employees to report wrongdoing without fear of retaliation, encouraging early detection of fraud.

Public-Private Partnership (PPP) – collaboration between government agencies and private sector entities to address shared security challenges, often in critical infrastructure protection.

Quantitative Risk Assessment – a numeric approach that assigns monetary values to likelihood and impact, enabling cost-benefit analysis of controls.

Ransomware – malware that encrypts data and demands payment for decryption. Frequently used in extortion schemes targeting commercial enterprises.

Real-Time Monitoring – continuous observation of systems and transactions, enabling immediate detection of anomalies.

Recovery Time Objective (RTO) – the maximum acceptable length of time to restore a business function after a disruption.

Recovery Point Objective (RPO) – the maximum tolerable period in which data might be lost due to an incident.

Red Team Exercise – an adversarial simulation where a group mimics threat actors to test defenses, often revealing hidden vulnerabilities.

Regulatory Compliance – adherence to laws, statutes, and industry standards governing commercial crime, such as the Bribery Act or GDPR.

Residual Risk – risk that remains after all feasible controls have been implemented. Managed through acceptance or transfer.

Risk Appetite – the amount and type of risk an organization is willing to pursue or retain in pursuit of its objectives.

Risk Assessment – systematic process of identifying, analyzing, and evaluating risks to determine appropriate treatment. Core component of the Executive Development Programme.

Risk Register – centralized repository that records identified risks, their analysis, mitigation actions, owners, and status.

Risk Tolerance – the specific threshold of risk exposure that the organization deems acceptable for a

particular activity or asset.

Risk Treatment – the selection and implementation of measures to modify risk, encompassing avoidance, mitigation, transfer, or acceptance.

Scenario Analysis – technique that evaluates the effects of plausible future events, helping leaders anticipate complex threat combinations.

Security Architecture – design of security controls and processes that align with business objectives and risk profile.

Security Information and Event Management (SIEM) – platform that aggregates, correlates, and analyzes log data to detect security incidents.

Social Engineering – manipulation of individuals to obtain confidential information or perform actions that compromise security. Common tactics include pre-texting and baiting.

Stakeholder – any party with an interest in the organization's risk outcomes, including shareholders, customers, regulators, and employees.

Strategic Risk – risk that affects the organization's long-term goals, such as market entry decisions or regulatory changes.

Supply Chain Risk – exposure arising from dependencies on suppliers, logistics providers, or third-party services. Includes counterfeit components and data leakage.

Suspicious Activity Report (SAR) – a filing required by financial regulators when a transaction appears indicative of money laundering or fraud.

Threat Actor – individual, group, or organization that poses a potential danger to assets. Actors can be internal, external, state-sponsored, or criminal enterprises.

Threat Capability – the resources, skills, and tools that a threat actor possesses to execute an attack.

Threat Landscape – the overall environment of existing and emerging threats that affect an industry or organization.

Threat Modeling – structured approach to identify, prioritize, and address potential threats to a system or process. Common methodologies include STRIDE and PASTA.

Threat Vector – the route by which a threat actor delivers an attack, such as email, USB devices, or remote access services.

Threat-Based Assessment – risk analysis that begins with identification of likely threat actors and then

evaluates vulnerabilities they could exploit.

Time-Based Attack – an attack that relies on timing, such as a coordinated fraudulent transaction at month-end when oversight may be reduced.

Tokenization – process of substituting sensitive data with non-sensitive equivalents (tokens) to reduce exposure.

Trade-Based Money Laundering (TBML) – laundering technique that disguises illicit funds through over- or under-invoicing of goods and services.

Transfer Risk – shifting risk to a third party, typically through insurance or contractual indemnities.

Trend Analysis – examination of data over time to identify patterns that may indicate emerging threats or increasing risk levels.

Trojan Horse – malicious software disguised as legitimate, used to gain unauthorized access or exfiltrate data.

Vulnerability – weakness in a system, process, or control that can be exploited by a threat actor.

Vulnerability Assessment – systematic examination of assets to identify and prioritize vulnerabilities, often preceding or complementing penetration testing.

Weighted Scoring – method of assigning numerical values to risk criteria (likelihood, impact, detectability) to calculate an overall risk score.

Whistleblower – individual who reports wrongdoing within an organization, often protected by law; can be a source of early threat detection.

Zero-Day Exploit – a vulnerability that is unknown to the vendor and has no available patch, offering attackers a high-success opportunity.