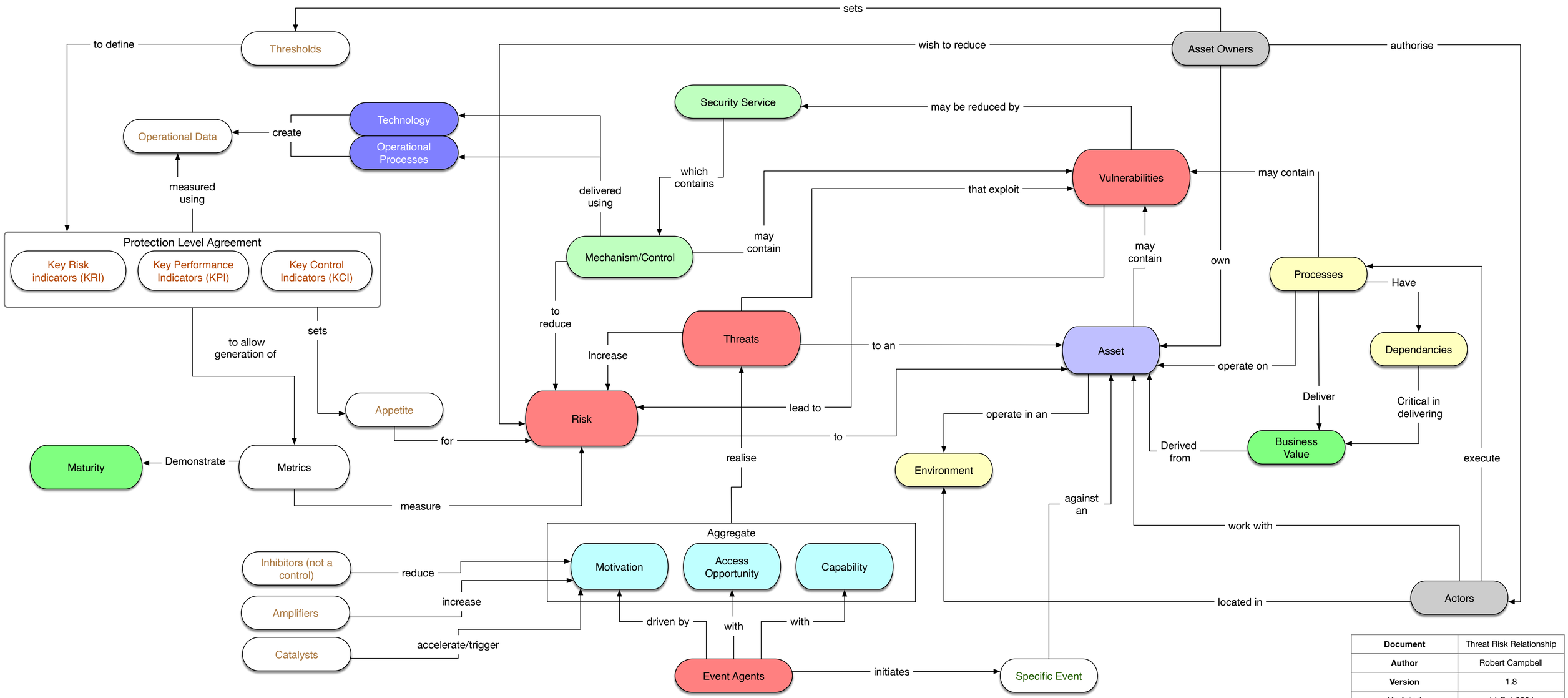

Document	Threat Risk Relationship
Author	Robert Campbell
Version	1.8
Updated	14 Oct 2024

KEY

Access Opportunity - The means or situations that provide a threat agent with the ability to approach or interact with an asset or system. This includes physical access, network connectivity, system vulnerabilities, or social engineering avenues. Minimising access opportunities is critical in preventing unauthorised actions and reducing risk exposure.

Amplifiers - Conditions or elements that encourage or increase the likelihood of an event agent executing a threat. Amplifiers may involve weak security practices, high-value targets, vulnerabilities, or factors that enhance the agent's motivation, such as the potential for significant financial gain or ideological impact. Identifying amplifiers is crucial for mitigating their effects and lowering risk levels.

Appetite - The amount and type of risk an asset owner or organisation is willing to accept to pursue its objectives. Risk appetite influences the development of risk management strategies, controls, and the allocation of resources to protect assets appropriately.

Capability - The skills, knowledge, resources, and tools that an event agent possesses, enabling them to successfully execute a threat. Capabilities can range from basic technical abilities to advanced expertise with significant resources at their disposal. Assessing the capability of potential threat agents helps in evaluating the seriousness and potential impact of threats.

Catalysts - Triggers or changes in circumstances that prompt an event agent to act. Catalysts can be internal or external events such as new vulnerabilities discovered, organizational changes, geopolitical events, or specific incidents that motivate the agent to execute a threat. Recognising catalysts allows organisations to anticipate potential threats and prepare accordingly.

Dependencies - The interconnections between assets, processes, or services that are critical for delivering business value. A disruption in a dependency may increase risk or amplify the impact of an event. Understanding these relationships is essential for effective risk assessment and management.

Event Agent - The actor or entity responsible for carrying out a specific event or attack. Event agents may be individuals, groups, or automated systems that exploit vulnerabilities to realise threats. They include malicious insiders, external attackers, automated malware, or even unintentional actors who cause harm through negligence.

Inhibitors - Factors or circumstances that deter an event agent from executing a threat. Inhibitors can include robust security controls, legal consequences, strong deterrence measures, or lack of access opportunities. Strengthening inhibitors is essential for reducing the likelihood of threat realisation.

Key Control Indicator (KCI) - Metrics that measure the effectiveness and performance of specific controls implemented to mitigate risks. KCIs provide insights into whether controls are operating as intended and help identify any deficiencies or areas that require improvement to enhance overall security posture.

Key Performance Indicators (KPIs) - Quantitative measurements that reflect how effectively an organisation is achieving its objectives, including the management of risks. In risk management, KPIs help assess the performance of risk mitigation strategies, processes, and controls, indicating how well risks are being managed over time.

Key Risk Indicator (KRI) - Metrics or indicators that provide early warning signals about increasing risk exposures or potential risk events within the organisation. KRIs help monitor changes in risk levels and enable proactive management by highlighting areas where risk may be approaching or exceeding acceptable thresholds.

Motivation - The underlying reasons or incentives that drive an event agent to execute a threat. Motivations may include financial gain, revenge, political or ideological beliefs, curiosity, or the desire for notoriety. Understanding the motivations of potential threat agents assists in risk assessment and in developing targeted defence strategies.

Operational Data - Information generated by systems, applications, and processes during regular operations. Operational data is essential for monitoring security performance, detecting anomalies, and informing risk management decisions. It may be used to support metrics like KPIs, KRIs, and KCIs.

Protection Level Agreement (PLA) - A formal agreement outlining the expected levels of security and protection for assets aligned with the organisation's risk appetite and objectives. PLAs define security requirements, responsibilities, and performance metrics between service providers and clients, ensuring that adequate protection measures are established and maintained.

Security Maturity - An evaluation of the organisation's security practices, processes, and capabilities regarding their effectiveness and sophistication. Security maturity models, such as the Capability Maturity Model Integration (CMMI) or the Cybersecurity Capability Maturity Model (C2M2), offer frameworks for assessing current security levels and guiding continuous improvement efforts.

Specific Event - A distinct occurrence or incident, such as a cyber attack, where a threat is actualised by exploiting vulnerabilities in an asset. Specific events represent actionable instances that can cause harm or disruption to an organisation's systems, data, or operations. Understanding these events aids in effective planning and response strategies.

Thresholds - The specific levels or limits of risk tolerance that, when reached, trigger a required response or action. Thresholds help in defining acceptable risk levels and guide decision-making in risk management processes, ensuring that risks are maintained within acceptable bounds.