The Gridiron Risk Model

Aptible Gridiron uses a graph database to model information security **risks**, events or situations that have the potential to cause adverse impacts.

1. Unanalyzed risks are called **threat events**. Each threat event has an associated impact level. Threat events become relevant to an organization through the presence of **predisposing conditions** that contribute to the likelihood that threats will result in adverse impacts. The mapping between a specific predisposing condition and a threat event is a **threat condition**.

2. Each threat event is associated with one or more **vulnerabilities**, each of which in turn is associated with zero or more **security controls**. The mapping between a specific security control and a vulnerability is a **mitigation**.

3. Each threat event is also associated with one or more **threat sources**, which are adversaries that may intentionally exploit a vulnerability or situations that may accidentally exploit a vulnerability.

4. The **likelihood that a threat event will be initiated or will occur** is determined by the interaction between the event and its associated threat sources. For adversarial threats, the attacker capability required to execute the attack is also considered.

5. The **likelihood that adverse impacts will result**, assuming the threat event is initiated or occurs, is determined by the interaction between the event and its associated vulnerabilities and security controls.

6. Together, these two likelihoods determine the **overall likelihood** that a threat event will occur and result in adverse impacts.

7. The severity of a risk is determined by the **overall likelihood** that it will occur and the **impact** that would result if it did occur.

Component (Environmental)

Component (Organizational)

Relationship

Risk Factor