**Guidelines for mapping NIST controls:**

Some of the NIST controls are technical in nature (i.e., implemented as part of the system) while others are implemented beyond the scope of the system (e.g., controls related to Policy, Configuration of the system, Management of the system or the organization).

**Step-1**: Identify the overall category of the control:

* Policy [e.g., access control policy, system maintenance policy]
* Management [e.g., configuration management plan, risk assessment]
* Configuration [e.g., configuration settings]
* Technical [e.g., audit generation, vulnerability scanning]

**Step-2**: For the ‘Technical’ controls, additionally identify the ‘security property’ and ‘security action’.

**Security Properties**

We have identified the following six core categories of security properties. Each security property counters a specific threat in the Microsoft STRIDE[[1]](#footnote-1) threat model.

* Confidentiality (C)
  + counters threat of Information Disclosure
* Integrity (I)
  + counters threat of Tampering
  + counters threat of Elevation of Privileges
* Availability (A)
  + counters threat of Denial of Service
* Identification & Authentication (ID)
  + counters threat of Spoofing
  + counters threat of Elevation of Privileges
* Accountability (AY)
  + counters threat of Repudiation
* Privacy (PR)
  + counters threat of Information Disclosure

Different security properties are important to consider based on the actions that are performed on assets. To map the NIST controls to security properties, consider the following:

* Confidentiality is important when performing ‘read’, ‘store’ and ‘transfer’ actions.
* Integrity is important when performing ‘create, update, delete’ and ‘transfer’ actions.
* Availability is important when performing any of the six action types (create, read, update, delete, store, transfer).
* Identification & Authentication is important when a system is accessed, prior to performing any of the six action types. If some actions are allowed without authentication, they should be explicitly specified.
* Accountability is important when performing any of the six action types.
* Privacy is important if the owner of information can exercise control over who can access the information during the actions ‘read’, ‘store’, and ‘transfer’.

**Security Action:**

For each NIST control, also identify which of the following three security actions the control supports:

* *Prevent* (*p*): proactively prevent a security breach.
* *Detect* (*d*): in case of a security breach, detect the breach.
* *Respond* (*r*): in case of a security breach, respond to the detected breach.

1. https://msdn.microsoft.com/en-us/magazine/cc163519.aspx [↑](#footnote-ref-1)