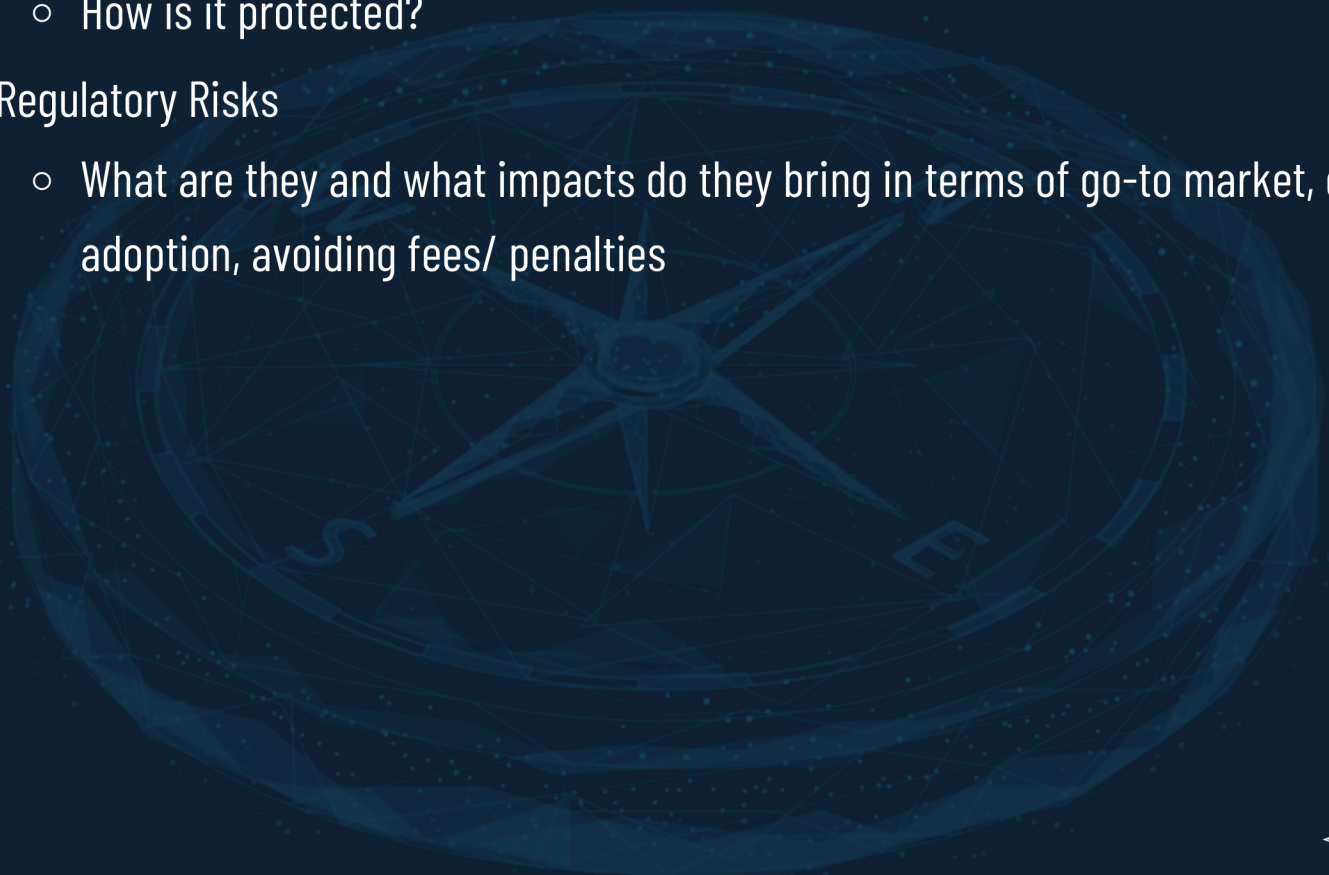
Stage 1: Know Your Business & What Supports Your Organization

- How does your company make money?
  - What are the online components that support revenue?
  - What are the physical components that support revenue?
- What does downtime mean over a unit of time? Over how many units of time do things get bad?
  - How is continuity ensured for the components of your business?
- How important is information/data to the business model?
  - Is it confidential?
  - Is it regulated?
  - How is it protected?
- Regulatory Risks
  - What are they and what impacts do they bring in terms of go-to market, customer adoption, avoiding fees/ penalties



VERSPRITE

Stage 2: People – Process – Product. What, Where, and Who are they in the support of the Organization?

- People
  - Which roles are essential?
  - Who has access to the keys to the kingdom?
  - What external human resources play a critical role?
- Process
  - What operations are core to revenue generation and growth?
    - What information is leveraged by these operations?
    - How is this information safeguarded?
    - Is this information regulated?
  - What third party operations support the business?
    - Consider Shared Services, Offshore Development, Business Process Outsourcing, and Foreign Manufacturing as some examples.
- Product
  - What proprietary products support current revenue cycles or growth?
  - What infrastructure (e.g., CoLo, Managed Services, orCloud) supports these products?
  - What third party vendors contribute to the product success?
  - What information is managed by these products?
    - What actions are taken by the organization to manage such information?
    - What third parties or sub-processors are in play to support the information managed by the product/services of the Organization?

Stage 3: Process Mapping to Business Objectives.

- Enumerate mission critical processes, products and serves and map these to People, Process and Product that play a role.
- Consider the following as process to objectives are put together:
  - Information flow
  - Information ownership
  - Regulatory laws (private/public) that are in scope
  - Business use cases supported by all People, Process and Product components
  - Inherent security controls that are in place
  - Technology footprint that is being leveraged (e.g., MS, Linux, Oracle, Apache, Zigbee, iOS, React.js, AS/400, HID, etc.) by critical or high impact business processes

VERSPRITE

Stage 4: Threat Analysis

- Build a threat library for your organization. An immutable mnemonic like STRIDE will not do since threats are dynamic and vary greatly by industry and organization. Threat libraries are living lists so they should be updated on a regular basis. An example threat library for a consumer electronic manufacturing company may look like:
  - Information Compromise
  - Account Compromise
  - Introduce malicious SDK or alter existing SDK
  - Compromise device via Supply Chain

*Note that the above are not attack patterns but threats.

- Stage 6 will begin to create attack libraries from frameworks like ATT&CK or CAPEC to map what types of attack patterns could realize threats depicted in this stage.

- Use the information and context from Stages 1-3 to shape how threat intel is meaningful. Context is everything and can more accurately help funnel threat intel in the right way for an organization. This is a many-to-limited mapping. Threat intel and data are plentiful, but custom develops threat libraries and the attack surface defined by Stages 1-3 can help funnel to more meaningful results.

Stage 5: Vulnerability Analysis.

- What active weaknesses or vulnerabilities (vulns) do we have?
- How do they help support the threat library that was created in Stage 4?
- Build your threat patterns based on abuse cases that can alter your product/service use cases.
- Focus on the vulns that could facilitate threat objectives. Build a vulnerability list and use vulns frameworks like CVEs to better map to exploits in the next stage.
- Vulns don't only come from vuln scanners. Consider human and physical weaknesses as well.

Stage 6: Attack Modeling

- Build a custom attack library. A sample of one that correlates to the one above is as follows (these don't have CAPEC IDs, but they definitely can and are suggested):
    - Device NFC Man-in-the-Middle (for Information Compromise)
    - Credential Stuffing Attack for Management Account Page
    - DNS Spoofing Attack to Fake SDK Site for Users
    - Hijacked embedded library in mirror sites for package inclusion in device
- It'll be important to test attack viabilities as this will factor in threat likelihood for the overall risk analysis.
- c.Attack libraries are also fluid lists but should always be supporting the threats and threat objectives that were previously defined. This is a major difference as many security professionals use threats and attacks as interchangeable words, even though their meanings are different.

Stage 7: Residual Risk Analysis – What's the net-net of where we should be concerned as an organization?

- With a net of identified vulnerabilities and simulated attack patterns all supported by a customized threat library, an organization is able to successfully see the residual effects in a controlled environment. This allows a security operations team to discover the detective and reactive technologies that are most critical to triage in the event an incident occurred?
- This stage allows for a more threat supportive and risk-focused alignment that allows threat data and threat intel sources to operate in a more concerted and strategic effort, as compared to simply leveraging tool-based alerts that are devoid of so much context.