Lifecycle Insight - Cyber Maturity

The Cyberfense Lifecycle is model Carnegie Mellon Capability Model Integration (CMMI). The purpose is to streamline organizational process improvement. Cyberfense leverages a modified version of CMMI. We simply call it “Cyber Maturity” (CM).

Our Cyber Maturity process starts with CM-0 and ends with CM-4. There are distinct objectives for each CM level.

CM-1 = Generate a policy

- Conveys the Business Leader’s intent.
- Defines the standard which is the criteria of acceptable achievement.
- Reduces error and liability.

There are 43 risk domains. The Bot will help generate a policy for each.

CM-2 = Establish Safeguards

- Safeguards are controls the support the policy.
- Types of safeguards
  - Adminsitrative (Ex. Guidelines and procedures)
  - Technical (Ex. Software, Hardware)
  - Physical (Ex. Physical protection - barriers, security guards, lighting)

The first safeguard will be offered for free by Cyberfense. This will be a “Guideline”. A guideline supports the policy and is generally a series of statements and recommendations about appropriate practice and descriptions of methodology and rational.

Each risk domain/CM-2 will have a guideline.

The Company (User) must complete the guideline before establishing other safeguards for that specific risk domain.

Once the guideline is complete, the Company/User can begin establishing additional safeguards. The more safeguards,

A. The more protection is in place to prevent human error and internal/external attacks.

B. Additionally, the more safeguards, the more points a Company/User gains.

C. The more points, the more “Cyber-Competitive” the Company/User is in contrast to its peers.

CM-3 = Identify Success Metrics of Safeguards

- Measures the effectiveness of the safeguard.
- Generally a quantitative metric such as uptime 99.99%.
- Helps decision making
  - Should we keep the safeguard?
  - Should we reconfigure it?
  - Should we upgrade or downgrade?
- All recommended solutions will have identified success metrics so the system can automatically populate the CM-3
- Examples
  - Policy: *“Is the guideline relevant, accurate and up to date?”* This is not quantitative but suitable for a policy.
  - Guideline = *“Has the guideline reduced human error (mistakes) X% over the last 12 months?”*
  - Technical Safeguard such as a VPN: *“Uptime 99.99%”.* This measurable. The information can be accepted by the vendor or outside monitoring tool.
  - At least one Success Metric will be identified for each safeguard.
  - All metrics are collected by Solvr (within the risk domain project card).
  - All the metrics will be reviewed at least annually.

CM-4 = Evaluate & Improve

- Solvr automatically consolidates the metrics from CM-3 into an agenda.
- The Bot will help the User identify other company representatives who should participate in the review.
- The Bot will propose a future date to meet and send a calendar invite to those individuals.
- The review committee will meet
  - Review each safeguard metric performance.
  - Determine next steps.
  - Determine next review.