Your Logo
Will Be
Placed Here

CYBERSECURITY BUSINESS PLAN

ACME Consulting Services, LLC

CBP
Cybersecurity Business Plan

IT IS PROHIBITED TO DISCLOSE THIS DOCUMENT TO THIRD-PARTIES WITHOUT AN EXECUTED NON-DISCLOSURE AGREEMENT (NDA)

Table of Contents

CYBERSECURITY DEPARTMENT OVERVIEW

ORGANIZATION DESCRIPTION

[Company Name]'s cybersecurity department is made up of [insert #] teams, each with a functional area that provides its own unique set of services to [Company Name]. Each team focuses on a specific area to support the cybersecurity department's overall mission:

[edit the names and description of the teams your company has – the following teams are just common examples]

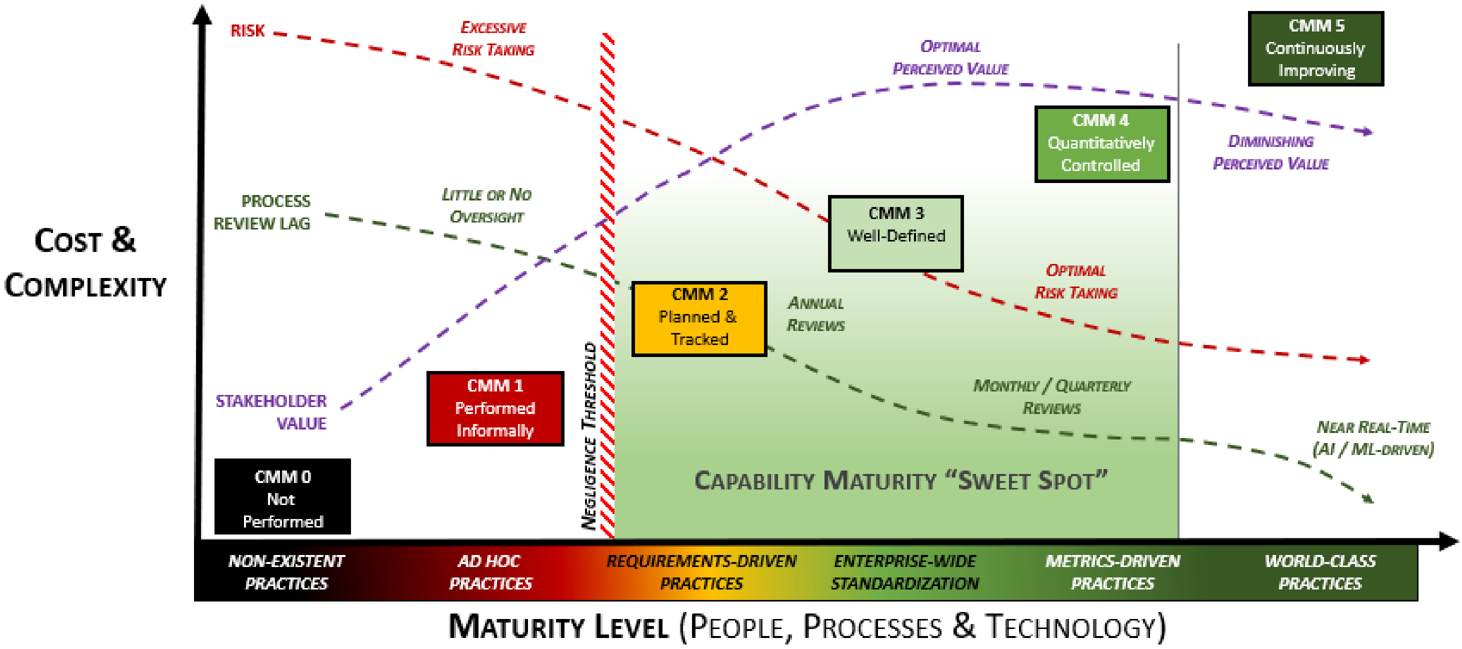
- Security Operations Center (SOC) Function
  - Provides 24/7 log monitoring and analysis capabilities to ensure situational awareness of incidents.
  - First line of defense in the Detect, Respond & Recover (DRR) process for incident response.
- Incident Response (IR) Function
  - Specialists in managing incidents / crisis that cover both technology and business considerations.
  - Second line of defense in the Detect, Respond & Recover (DRR) process for incident response.
  - Handles endpoint and network forensics.
- Security Architecture / Engineering Function
  - Specialists who identify, build and maintain secure baseline configurations for all technology assets.
  - Aligns with ACME's enterprise architects to ensure current and future technologies are capable of meeting ACME's security and compliance obligations.
  - Collaborates with IT and project teams to ensure secure practices are implemented by default.
- Endpoint Security Function
  - Specialists in securing endpoint devices, including mobile devices and collaborative tools.
  - Aligns with ACME's IT department to ensure current and future endpoint devices are properly configured and protected in accordance with ACME's standards.
  - Collaborates with engineering and other teams to perform "proof of concept" testing for emerging technologies on endpoint devices.
- Governance, Risk & Compliance (GRC) Function
  - Specialists in managing governance, risk and compliance operations.
  - Identifies applicable laws, regulations and industry frameworks that ACME must comply with.
  - Governs ACME's policies, standards and controls, in accordance with applicable laws, regulations and contractual obligations.
  - Assigns controls to appropriate stakeholders and provides an oversight function for control execution.
  - Governs ACME's risk register to maintain appropriate situational awareness of known risks and remediation efforts.
  - Conducts risk assessments and evaluates the effectiveness of proposed compensating controls.
  - Performs pre-production testing (e.g., control validation testing) to ensure control implementation is appropriate.
  - Provides cybersecurity and privacy-related consulting services to internal technology teams and business units.
- Threat Hunting / Red Team Function
  - Specialists in offensive cybersecurity threat management operations who identify potential threats and vulnerabilities across ACME's systems, applications and services.
  - Maintains threat intelligence feeds to stay alert to evolving Tactics, Techniques & Procedures (TTPs) of potential adversaries so that ACME is capable of detecting potential threats.
  - Performs penetration testing services to identify points of weakness across the enterprise.
- Vulnerability Management Function
  - Specialists in defensive cybersecurity threat management operations that focus on patch and vulnerability management.
  - Performs software and firmware patching for systems, applications and firmware.
  - Performs vulnerability scanning across the enterprise.
- Business Continuity / Disaster Recovery (BC/DR) Function
  - Specialists in managing incidents / crisis that require recovery and/or reconstitution.
  - Aligns with ACME's IT department to ensure current and future capacity is appropriate for ACME's business needs for both processing and recovery needs.
- Identity Access Management (IAM) Function
  - Specialists in managing digital access, through administering account profiles and credentials.
  - Governs Active Directory (AD) and account federation services to ensure ACME standards for secure identification and authentication are enforced.
- Secure Development Function

APPENDIX A – CAPABILITY MATURITY MODEL (CMM) DEFINITIONS

The six (6) Security & Privacy Capability Maturity Model (SP-CMM) levels are:

- CMM 0 – Not Performed
- CMM 1 – Performed Informally
- CMM 2 – Planned & Tracked
- CMM 3 – Well-Defined
- CMM 4 – Quantitatively Controlled
- CMM 5 – Continuously Improving

For most organizations, the "sweet spot" for maturity targets is between CMM 2 and 4 levels. ACME's cybersecurity department strives for a baseline CMM3, but may dictate certain functions require a higher level of maturity, based on specific risks.



Negligence Considerations

Without the ability to demonstrate evidence of both due care and due diligence, an organization may be found negligent. In practical terms, the "negligence threshold" is between CMM 1 and CMM 2. The reason for this is at CMM 2, practices are formalized to the point that documented evidence exists to demonstrate reasonable steps were taken to operate a control.

Risk Considerations

Risk associated with the control in question decreases with maturity, but noticeable risk reductions are harder to attain above CMM 3. Oversight and process automation can decrease risk, but generally not as noticeably as steps taken to attain CMM 3.

Process Review Lag Considerations

Process improvements increase with maturity, based on shorter review cycles and increased process oversight. What might have been an annual review cycle to evaluate and tweak a process can be near real-time with Artificial Intelligence (AI) and Machine Learning (ML).

Stakeholder Value Considerations

The perceived value of security controls increases with maturity. However, perceived value tends to decrease after CMM 3 since the value of the additional cost and complexity becomes harder to justify to business stakeholders. Companies that are genuinely focused on being industry leaders are ideal candidates for CMM 5 targets to support their aggressive business model needs.

CMM 0 – Not Performed

This level of maturity is defined as "non-existence practices," where the control is not being performed.

- There are no identifiable work products of the process.

CMM 0 practices, or a lack thereof, are generally considered to be negligent. The reason for this is if a control is reasonably-expected to exist, by not performing the control that would be negligent behavior. The need for the control could be due to a law, regulation or contractual obligation (e.g., client contract or industry association requirement).

CMM 1 – Performed Informally

This level of maturity is defined as "ad hoc practices," where the control is being performed, but lacks completeness & consistency.

- Base practices of the process area are generally performed.
- The performance of these base practices may not be rigorously planned and tracked.
- Performance depends on individual knowledge and effort.
- There are identifiable work products for the process.

CMM 1 practices are generally considered to be negligent. The reason for this is if a control is reasonably-expected to exist, by only implementing ad-hoc practices in performing the control that could be considered negligent behavior. The need for the control could be due to a law, regulation or contractual obligation (e.g., client contract or industry association requirement).

CMM 2 – Planned & Tracked

This level of maturity is defined as "requirements-driven practices," where the expectations for controls are known (e.g., statutory, regulatory or contractual compliance obligations) and practices are tailored to meet those specific requirements.

- Performance of the base practices in the process area is planned and tracked.
- Performance according to specified procedures is verified.
- Work products conform to specified standards and requirements.

CMM 2 practices are generally considered to be "audit ready" with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control. CMM 2 practices are generally targeted on specific systems, networks, applications or processes that require the control to be performed for a compliance need (e.g., PCI DSS, HIPAA, NIST 800-171, etc.).

It can be argued that CMM 2 practices focus more on compliance over security. The reason for this is the scoping of CMM 2 practices are narrowly-focused and are not organization-wide.

CMM 3 – Well-Defined

This level of maturity is defined as "enterprise-wide standardization," where the practices are well-defined and standardized across the organization.

- Base practices are performed according to a well-defined process using approved, tailored versions of standard, documented processes.
- Process is planned and managed using an organization-wide, standardized process.

CMM 3 practices are generally considered to be "audit ready" with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control. Unlike CMM 2 practices that are narrowly focused, CMM 3 practices are standardized across the organization.

It can be argued that CMM 3 practices focus on security over compliance, where compliance is a natural byproduct of those secure practices. These are well-defined and properly-scoped practices that span the organization, regardless of the department or geographic considerations.

CMM 4 – Quantitatively Controlled

This level of maturity is defined as "metrics-driven practices," where in addition to being well-defined and standardized practices across the organization, there are detailed metrics to enable governance oversight.

- Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance.
- Performance is objectively managed, and the quality of work products is quantitatively known.

CMM 4 practices are generally considered to be "audit ready" with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control, as well as detailed metrics enable an objective oversight function. Metrics may be daily, weekly, monthly, quarterly, etc.

CMM 5 – Continuously Improving

This level of maturity is defined as “world-class practices,” where the practices are not only well-defined and standardized across the organization, as well as having detailed metrics, but the process is continuously improving.

- Quantitative performance goals (targets) for process effectiveness and efficiency are established, based on the business goals of the organization.
- Continuous process improvement against these goals is enabled by quantitative feedback from performing the defined processes and from piloting innovative ideas and technologies.

<u>CMM 5 practices are generally considered to be “audit ready” with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control and incorporates a capability to continuously improve the process</u>. Interestingly, this is where **Artificial Intelligence (AI)** and **Machine Learning (ML)** would exist, since AI/ML would focus on evaluating performance and making continuous adjustments to improve the process. However, AI/ML are not requirements to be CMM 5.

Summary of CCM vs Organization Size Considerations

The following table summarizes the high-level expectations for small/medium/large organizations to meet each level of maturity.

Maturity Level	Small Organizations	Medium Organizations	Large Organizations
SP-CMM 0	▪ Lack of processes would be considered negligent behavior. This is generally due to a lack of a cybersecurity and privacy program. ▪ [NEGLIGENT]		It is unlikely for a large organization to completely ignore cybersecurity and privacy requirements.
SP-CMM 1	▪ IT support focuses on reactionary “break / fix” activities and are ad hoc in nature. ▪ IT support is likely outsourced with a limited support contract. ▪ [LIKELY NEGLIGENT]	▪ Internal IT staff exists, but there is no management support to spend time or budget on security / privacy controls that leads to ad hoc control implementation. ▪ Focus is on general IT operations without clear standards that implement secure systems and processes. ▪ [LIKELY NEGLIGENT]	
SP-CMM 2	▪ Internal IT role(s) has clear requirements and is supported to meet applicable cybersecurity / privacy compliance obligations; or ▪ The outsourced IT provider is properly scoped in its support contract to address applicable compliance obligations.	▪ IT staff have clear requirements to meet applicable compliance obligations. ▪ There is most likely a dedicated cybersecurity role or a small cybersecurity team.	
SP-CMM 3	▪ There is a small IT staff that has clear requirements to meet applicable compliance obligations. ▪ There is likely a very competent leader (e.g., security manager / director) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.	▪ IT staff have clear requirements to meet applicable compliance obligations. ▪ In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.). ▪ There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.	
SP-CMM 4	It is unrealistic for a small organization to attain this level of maturity.	▪ IT staff have clear requirements to meet applicable compliance obligations. ▪ In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.). ▪ There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization. ▪ Business stakeholders are made aware of the status of the cybersecurity and privacy program (e.g., quarterly business reviews to the CIO/CEO/board of directors). Situational awareness is made possible through detailed metrics.	
SP-CMM 5	It is unrealistic for a small or medium organization to attain this level of maturity.		▪ IT staff have clear requirements to meet applicable compliance obligations. ▪ In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.). ▪ There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization. ▪ Business stakeholders are made aware of the status of the cybersecurity and privacy program (e.g., quarterly business reviews to the CIO/CEO/board of directors). Situational awareness is made possible through detailed metrics. ▪ The organization has a very aggressive business model that requires not only IT, but its cybersecurity and privacy practices, to be innovative to the point of leading the industry in how its products and services are designed, built or delivered. ▪ The organization invests heavily into developing AI/ML technologies to made near real-time process improvements to support the goal of being an industry leader.

Appendix B – Strengths, Weaknesses, Opportunities & Threats (SWOT) Analysis

[summarize the strategic takeaways from the SWOT analysis]

The SWOT analysis performed by the cybersecurity leadership team identified a few historical issues that need to be addressed, as well as possible opportunities. From a business planning perspective, the department's leadership needs to address a few strategic issues:

- Control standardization across the enterprise is needed to ensure appropriate laws, regulations and contractual obligations are met, including having the appropriate evidence of due care and due diligence to support external scrutiny (e.g., CMMC audit).
- The dynamic nature of stakeholders within ACME's business units requires an aggressive stakeholder engagement program. This will both identify stakeholders and also educate those stakeholders on cybersecurity processes.
- Objective prioritization must be adopted and enforced, since everything cannot be a priority. Management support of Service Level Agreements (SLAs) for cybersecurity services will help address this.
- Appropriate skill-set resourcing needs to be addressed, either through organic maturation (professional development training) or augmentation through additional staffing.
- In order to remove the cybersecurity department from being viewed as a "roadblock" or impediment to project implementation, ACME needs to be included early on in the SDLC process. This requires both architectural and project management involvement early in the Information Assurance Program (IAP) to help ensure that security and privacy principles are identified and incorporated by design and by default.

Summary of SWOT Business Planning Considerations

[summarize the SWOT analysis as it pertains to people, processes and technology]

Key highlights from SWOT to keep in mind from a People, Processes and the IT department (PPT) perspective include:

- **PEOPLE**
    - Internal To The Cybersecurity Department
        - There is a shared passion among members of the team and this has led to a technically-strong and motivated team - they are proud of what they do and want people to respect their abilities.
        - Within ACME, the team has strong, ongoing collaboration which helps ensure situational awareness is maintained among team members.
        - ACME team members feel the department is under-resourced – they do not have the appropriate skillsets/personnel for all the work that they are responsible for performing.
        - There are "human firewalls" who impact the department's situational awareness for ACME's evolving business requirements. These individuals horde knowledge.
    - External To The Cybersecurity Department
        - Cybersecurity department leadership is perceived as being "incapable of saying no," which leads to a lack of prioritization, since everything is a priority.
        - External stakeholder mapping is incomplete or outdated.

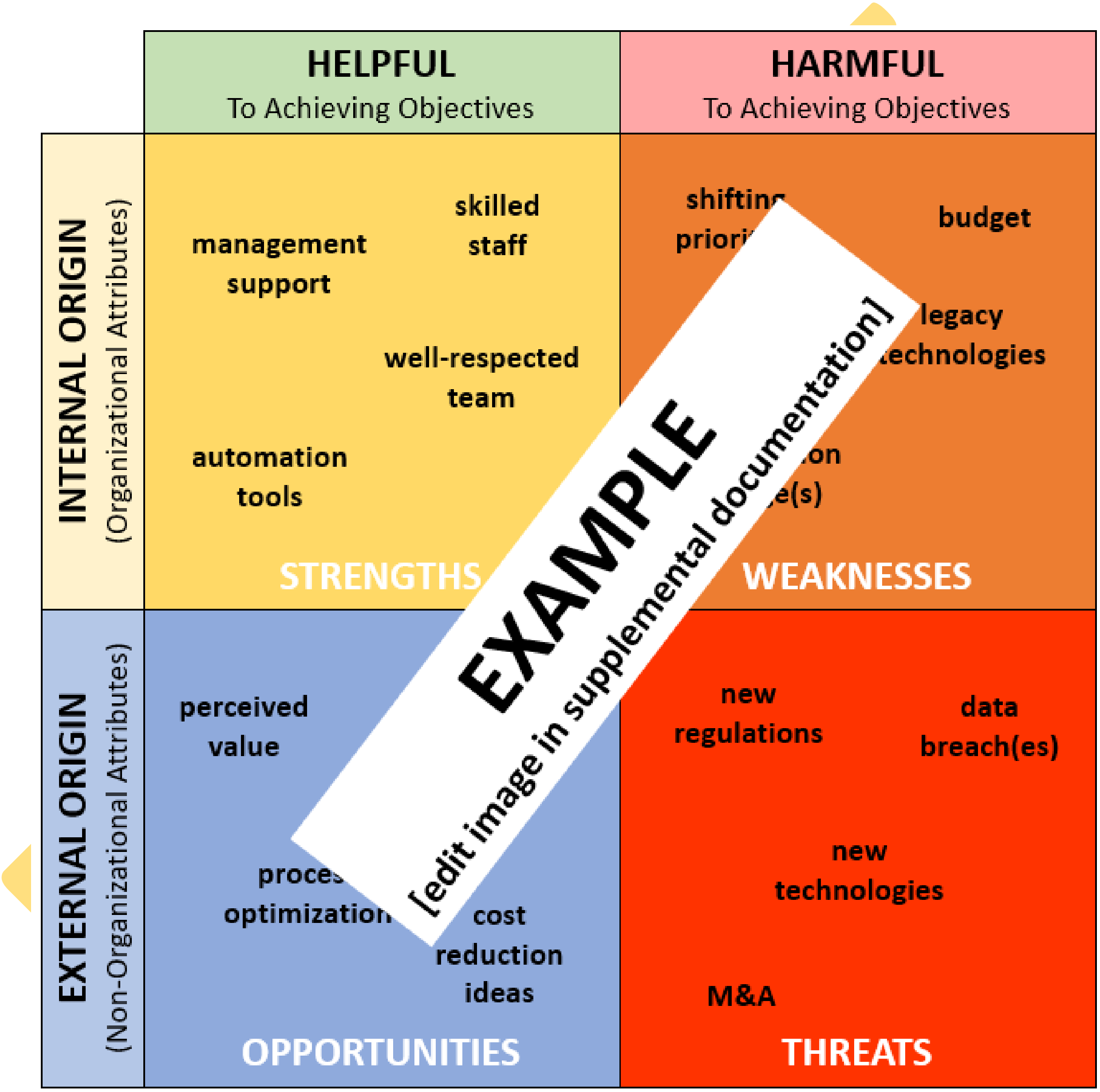
- **PROCESSES**
    - Internal To The Cybersecurity Department
        - Process documentation does not exist. Templates and documentation are needed (e.g., Standardized Operating Procedures (SOPs), Data Flow Diagrams (DFDs), etc.).
        - Intake process needs to be developed that will prioritize and manage the inbound requests.
        - There is a lack of SLAs for the types of work the department performs for other ACME stakeholders in the IT department and Lines of Business (LOB).
    - External To The Cybersecurity Department
        - Prioritization is based on "who complains the loudest," as compared to rational discourse that comes from a risk-based approach to prioritization and expectations management.
        - There is a lack of standardization for hardening (e.g., CIS Benchmark or STIG configurations), which are used to secure technology platforms. This makes enforcing standards difficult.

- **TECHNOLOGY**
    - Internal To The Cybersecurity Department
        - There is no current method to track and manage the intake of requests. This is more of an operational support queue need to improve efficiency, as compared to ServiceNow ticketing.
    - External To The Cybersecurity Department

- The lack of a standardized framework to define and describe risk is a weakness that affects ACME operations.
- There is a perceived lack of strategy when it comes to acquisition decisions. The ACME teams wants to have a “sanity check” option that raises legitimate security concerns to the appropriate levels.
- The lack of system lifecycles hinders ACME’s ability to get in front of project involvement for resource planning.

SWOT Analysis

[perform a SWOT analysis with key cybersecurity department personnel to determine the department’s specific strengths, weaknesses, opportunities and threats]



Strengths

From the SWOT analysis, the following attributes were identified as strengths (internal to the cybersecurity department):

- Team members have a shared passion for the technical side of cybersecurity, which encourages professional growth.
- ACME has skilled professionals with subject matter expertise.
- There is strong collaboration between ACME team members.
- The adoption of automation tools is beneficial and is making work processes more efficient.

Weaknesses

From the SWOT analysis, the following attributes were identified as weaknesses (internal to the cybersecurity department):

- There is lack of standardized documentation within the department, which leads to ad hoc processes.