Business Planning Essentials for Cybersecurity Professionals

COMPLIANCE FORGE

MISSION

- Determines **WHAT & WHY** in a straightforward, concise manner – this is the "Why our department exists" statement for the cybersecurity department.
- Missions are outcome-oriented. In the real world, missions are issued by a higher authority to a lower authority and are directive in nature.
- Generally starts with a "To…" statement since it is explicitly declaring what people / departments are here to do (e.g., "Our mission is to achieve XYZ…").
- Results of execution determine performance ratings for executive management (e.g., CIO, CXO, etc.).
- **EXAMPLE:** *To deliver high-quality, innovative cybersecurity services and solutions that reduce risk across ACME.*

VISION

- Communicates the concept of what the **IDEAL CONDITIONS** looks like in a perfect world – this is the visionary ***"What we want to be"*** statement for the cybersecurity department.
- Unlike mission statements, visions are meant to appeal to the lowest common denominator and should be easily understood by everyone. If you must explain it, it is a poorly constructed vision statement.
- Visions are meant to uplifting & inspiring to members of the broad organization - internal and external to the cybersecurity department.
- **EXAMPLE**: *We exist to create an environment where creativity, collaboration and security are seamless. In doing so, we will unlock ACME's unmeasurable potential to innovate at the speed of inspiration.*

STRATEGY

- **HIGH-LEVEL ACTION PLANNING** that is directly linked to the mission – establishes the big picture of **HOW** you are going to successfully accomplish your mission – this is the ***"What steps we need to take to achieve our mission"*** statement.
- This allows for the development of a thoughtfully-constructed course of action and the establishment of realistic objectives.
- Strategy statements do not have to be long. Business plans are the in-depth documents to implement a strategy through defining objectives, resourcing needs and assigning responsibilities.
- Results of execution determine performance ratings for senior cybersecurity leadership (e.g., CISO).
- **EXAMPLE**: *We will drive our initiatives by influencing key stakeholders throughout ACME to enable the implementation of high-quality, innovative information security services and solutions that reduce risk to ACME, our partners and our customers.*

OBJECTIVES

- Objectives are the short and mid-range goals that are arranged and prioritized to achieve the strategy.
- Objectives are often misunderstood to be missions or strategies, since objectives are the stepping stones that are needed to achieve success in accomplishing the strategy.
- Objectives are where you start getting into bullet point lists. While this list of objectives is "owned" by the CISO, the cybersecurity department heads are responsible for achieving these objectives in how their operations are conducted and budget is prioritized.
- In the real world, a RACI diagram is great to assign objectives so stakeholders are clear on their involvement and responsibilities.

OPERATIONS

- **MID-LEVEL ACTION PLANNING** that is directly linked to strategy – clarifies how the strategy will actually be accomplished.
- Operations transform strategy into actionable projects or initiatives that define resources that are required for tactics to successfully execute.
- Operations are "owned" by department heads and team leads are responsible for achieving these department-level objectives in how work is executed.
- Poor execution of operations will prevent or inhibit the successful execution of strategy.
- Results of operations execution determine performance ratings for mid-level management (e.g., GRC, Engineering, Operations, Incident Response, etc.).

TACTICS

- **LOW-LEVEL ACTION PLANNING** that is directly linked to operations – specifies how department-level objectives will be achieved on a day-to-day basis through staff assignments, processes and procedures.
- Tactics bring together the people, processes & technology to successfully accomplish tasks to achieve assigned objectives.
- Results of tactics execution determine performance ratings for individual contributors (e.g., risk analysts, engineers, architects, forensic analysts, etc.).