***Executive*** *template Use Cases:*

* ***Author****: CTI Team*
* ***Audience****: Executive*
* ***Key******Decisions****: Resource allocation; Evaluate options to mitigate risks to the organization.*
* ***Decision-Enabling Data Points****: Analysis of change in the cyber landscape that is relevant and impactful to organization; Estimate of how the trend may evolve; Key variables that could have an impact on the trend.*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*The* ***mandatory*** *fields in this template are denoted with an asterisk (\*), e.g., Report Date, Report Title, Executive Summary, and Key Points. However, most fields are* ***optional*** *and can be removed/adjusted for external sharing.*

***Criticality****: This field communicates the urgency of the report and helps prioritize for recipients. Criticality’s selections are: FYSA, Low, Medium, High, Critical.*

**<Report Date\*>**   **< Criticality\*>**

**Report Title\***

# **Executive Summary\***

This should be a brief narrative explaining the significance of the report to senior leadership. This should focus on the decision the CTI summary is supporting and the change in circumstances that makes this timely and actionable.

This should focus on:

• Bottom Line Up Front (BLUF): The single largest takeaway from the CTI analysis.

• What is the new information.

• Why it is important for the audience to understand this now.

• What is the trend and why it is significant for the decision maker.

This section should **not** summarize the underlying reports used to create the analysis.

The Executive Summary should not be longer than 2–3 paragraphs, according to best practices.

# **Key Points\***

This section should clearly lay out:

* The trend in question.
* The reason it is important.
* The key decision/risk/opportunity it presents.

# **Assessment**

This section needs to lay out several things.

* What is the trend that is being assessed?
* What is the historical baseline?
* What is the new information that creates a need to understand this now?
* Why is this relevant to your consumer?
* For example: does it have the potential to undermine existing security controls? Does it have the potential to undermine earnings in each geographic region? Does it present an opportunity to move into a new market space?
* What does the new normal likely look like if no action is taken?
* What key variables can impact the trend (both positively and negatively) should they change from current available information?

# **Outlook**

* This section should provide an analysis of both the impact and what key points of leverage the company must disrupt or take advantage of the trend. This should focus on what key variables can impact the trend (both positively and negatively) should they change from current available information and which of those variables are within the constituent's control.

# **Key Intelligence Gaps**

* Brief bullet summary of additional information the CTI team is seeking to further evaluate risk. Call out explicit gaps in understanding and what will change assessment because you don’t have information yet.

# **Probability Matrix**

We recommend that analysts properly express and explain uncertainties associated with major analytic judgments.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Almost no chance | Very unlikely | Unlikely | Roughly Even Chance | Likely | Very likely | Almost certain(ly) |
| 01–05% | 05–20% | 20–45% | 45–55% | 55–80% | 80–95% | 95–99% |

# **Intelligence Requirements**

Brief citation of CTI requirements(s) addressed by this report.

# **Feedback**

Provide a point of contact (e.g., an email address) for customer feedback on the published CTI report, such as whether the report addressed the customers’ Intelligence Requirements, how the report could be more actionable, additional Intelligence Requirement questions to answer, etc.

|  |  |
| --- | --- |
| Data Sources: | * Cite external CTI Report with hyperlink if available. * Cite Internal Telemetry sources provided by the SOC as needed. This field is not designed to preserve telemetry data and should only include data necessary to justify the analytic assessments. |