Risk Measurement and Reporting Policy Example

This document presents example content and in some cases context or scope guidance for the policy outline elements. Note that this isn't intended to represent comprehensive or universally relevant content as every organization will need to establish policies that reflect their objectives, tolerances, and constraints.

- **Governance**
  - Roles & Responsibilities
    - *Business Decision Makers - own the risk and are responsible for decisions regarding risk acceptance.*
    - *CISOs - are responsible for providing to Decision Makers the most accurate and reliable risk information available given current constraints.*
  - Reporting frequency
    - Board: *Quarterly.*
    - Org executive team: *Quarterly or every other month. (Note: This would typically[1] involve more details than are included in the board report.)*
    - LOB management teams: *Monthly (detail tailored to teams).*
  - Risk appetite **
    - Risk appetite development: *Must be defined and approved at the executive level of the organization (board or chief executive level). Criteria must be established that enable identification of the crown jewels of the organization.*
    - KRI threshold development: *Must be explicitly aligned with Risk Appetite.*
    - KPI threshold development: *Must be explicitly aligned with Risk Appetite.*
    - Response level definitions: *Levels of response must be defined for loss exposures of certain levels*

** These policy elements are established later during a RiskLens Quantitative Cyber Risk Management Program buildout.

- **Metrics**
    - Risk
        - Data
            - Asset management: *Complete and accurate asset information must be maintained at all times for assets determined to be crown jewels. (Note: Organizations may want to establish less stringent requirements for the remainder of their assets.)*
            - Threat landscape: *Threat activity must be actively monitored, and those data must be made available for risk analysis purposes. Periodic updates must be made to an established set of 'threat profiles.'*
            - Control conditions: *The results of periodic testing of an established set of controls must be made available for risk analysis purposes.*
        - Analysis
            - Model: *Risk measurement must be performed using a model that has been formally approved.*
            - Scoping: *All risk analyses are required to have a clearly defined loss event scenario scope containing (at a minimum) the Asset at risk, a Threat Actor, and a Threat Effect.)*
            - Data requirements: *All data applied to risk measurements must be calibrated to account for uncertainty. This includes both subject matter expert estimates as well as estimates based on empirical data. All input values must be accompanied by a description of the data's source.*
            - Analyst proficiency: *All individuals who are empowered to measure (or "rate") risk must have attended an approved risk analysis training program and achieved certifications defined.*
            - Technology requirements: *Technologies used to provide risk measurements must be evaluated for reliability and approved by the CISO.*
            - Analysis confidence reporting: *All analyses that are less rigorous in nature (I.e., triage-level data gathering) must be labeled as such when being provided to decision-makers.*
            - When cost-benefit analyses are required: *A risk-based cost-benefit analysis must be performed whenever the cost of proposed control improvements exceeds $100,000.*
            - Quality control*: All risk analysis results must be reviewed by a second qualified risk analyst. In addition, on a quarterly basis four risk analyses performed in the last quarter must be randomly selected for a thorough evaluation. Any evidence of foundational weaknesses in analysis method must be corrected.*

- **Risk management**
  - Data
    - Variance levels: *Data related to non-compliant control conditions (I.e., variant conditions) must be systematically gathered and reported.*
    - Losses
      - Actual: *Loss magnitude data must be captured for any availability loss event that exceeds one hour of business process down time, for any confidentiality breach that involves more than 1,000 customer records or sensitive corporate strategic data or intellectual property.*
      - Near Misses: *Forecasted potential loss must be captured for any near misses that would otherwise have qualified for reporting, as defined above. (Note: near misses are defined as loss events that would have occurred if not for circumstances arising that cannot be relied on in the future.)*
  - Analysis
    - Root cause analysis: *Root cause analyses must be performed on any non-compliant conditions found on crown jewel assets. These conditions, their root causes, and related action plans must be included in Board, executive, and management reporting. (Note: organizations may wish to broaden the scope of when root cause analyses are performed.)*