1. Mission & Business Impact Metrics

Measure whether security preserves enterprise objectives.

- **Mission Disruption Hours (MDH)**
  - Total hours of degraded or unavailable mission-critical services attributable to security events
- **Revenue / Cost Impact per Incident**
  - Direct and indirect financial loss per security event (including recovery and opportunity cost)
- **Safety or Legal Exposure Events**
  - Count of incidents triggering regulatory reporting, legal action, or physical harm risk
- **Critical Process Availability (%)**
  - Uptime of designated mission-critical processes across cyber, physical, and personnel domains
- **Executive Risk Acceptance Rate**
  - Percentage of high-risk decisions formally accepted vs. remediated

---

2. Risk Reduction & Control Effectiveness

Measure whether controls actually change risk.

- **Risk Exposure Trend**
  - Net change in quantified enterprise risk over time (not number of findings)
- **Control Failure Rate**
  - Percentage of incidents where a control existed but failed operationally
- **Cross-Domain Control Coverage (%)**
  - Proportion of critical risks mitigated by coordinated cyber, physical, and personnel controls
- **Time to Risk Mitigation (TTRM)**

  - Median time from risk identification to effective mitigation
- **Repeat Incident Rate**
  - Percentage of incidents recurring within the same risk category

---

3. Detection, Response & Recovery Outcomes

Measure operational performance under real conditions.

- **Mean Time to Detect (MTTD)**
  - Time from event occurrence to confirmed detection across all security domains
- **Mean Time to Contain (MTTC)**
  - Time from detection to isolation or neutralization of threat
- **Mean Time to Recover (MTTR)**
  - Time to restore normal operations after containment
- **Escalation Accuracy Rate**
  - Percentage of incidents escalated at the correct severity level on first assessment
- **Incidents Managed Without Business Interruption (%)**

---

4. Governance & Decision Quality

Measure whether governance produces disciplined outcomes.

- **Risk Decisions with Documented Tradeoffs (%)**
  - Proportion of major security decisions explicitly addressing cost, usability, and mission impact
- **Policy Exception Burn-Down Rate**
  - Net reduction of approved exceptions over time
- **Unauthorized Risk Acceptance Events**
  - Decisions taken without proper authority or governance review

- **Board / Executive Action Closure Rate**
  - Percentage of security-related directives completed on schedule
- **Time from Incident to Governance Action**

---

5. Integration & Coordination Metrics

Measure whether security functions act as a system.

- **Cross-Domain Incident Involvement Rate**
  - Percentage of incidents requiring cyber, physical, personnel, or legal coordination
- **Unified Identity Coverage (%)**
  - Proportion of workforce, contractors, and partners governed under a single identity authority
- **Joint Exercise Performance Score**
  - Outcomes from tabletop and live exercises spanning multiple security domains
- **Information Sharing Latency**
  - Time for relevant intelligence to reach all impacted security functions
- **Fragmentation Index**
  - Number of parallel, uncoordinated responses to a single incident

---

6. Resilience & Preparedness

Measure readiness before failure occurs.

- **Critical Dependency Mapping Coverage (%)**
  - Proportion of mission-critical processes with documented system, facility, and personnel dependencies
- **Backup and Recovery Success Rate**
  - Percentage of successful restorations during testing or real events

- **Exercise-Identified Gap Closure Rate**
  - Findings closed before the next exercise cycle
- **Single-Point-of-Failure Count**
  - Remaining unmitigated SPOFs in critical workflows
- **Continuity Plan Invocation Success (%)**

---

7. Culture & Human Risk Outcomes

Measure behavior, not training completion.

- **Privileged Access Misuse Incidents**
- **Insider Risk Events per 1,000 Personnel**
- **Policy Violation Severity Trend**
- **Security-Related Disciplinary Actions with Root Cause Addressed (%)**
- **Time to Revoke Access Post-Separation**

---

8. Cost Efficiency & Resource Alignment

Measure whether security investment matches risk.

- **Cost per Risk Unit Reduced**
  - Security spend relative to quantified risk reduction
- **High-Cost / Low-Impact Control Ratio**
- **Automation Leverage (%)**
  - Percentage of detections and responses executed without manual intervention
- **Security Spend as % of Protected Asset Value**
- **Operational Security OpEx vs. Incident Loss Ratio**