Alerting is either not available or only available within security-specific technologies.

Reporting requirements, including all required programs, operational, and executive metrics trends and forecasts are well-defined and monitored for internal and external stakeholders. Reports and metrics include an indication of compliance with defined policy and standards, treatment plans, and organizational performance standards. Key risk areas are identified and follow automated or validated report generation.

Custom reporting is available as a service or as an on-premises solution, or both. This may be performed internally or outsourced to a managed reporting provider. The output from the automated, proactive controls enforce policy and manage risk. An executive dashboard is in place and includes the highest-risk root causes, remediation activities, and organizational performance.

Deviations from configuration requirements and associated service impacts are measured and tracked.

Data from the configuration process along with security incidents and threat intelligence are used to prioritize release or risk mitigation strategies as needed.

Contextual metrics and measures are usually derived directly from the processes and tools described in two additional processes described in this standard:

Program: metrics are higher-level metrics meant to gauge the effectiveness and influence the direction of the VPN program and its underlying policy.

Executive: metrics provide additional clarity and often identify specific areas of risk or other data points which highlight specific VPN program needs or expected outcomes and/or business support or funding.

Program:

- Percentage of assets tested and categorized by type or asset
- Percentage of vulnerabilities with criticality scores
- Percentage of vulnerabilities categorized by type or asset

Metrics:

- Track visibility and trending of security-related events
- Track data breach trends and impact
- Track incident response times and resolution rates
- Track security-related costs and savings
- Track compliance and regulatory requirements
- Track customer satisfaction and feedback
- Track operational and financial performance

Executive:

- High-level risk score with visual interactive elements
- Top three most vulnerable vulnerabilities
- Top three reasons for exclusion or other data points which highlight specific VPN program needs or expected outcomes and/or business support or funding.