**Executive summary**

This section provides a bird’s eye view of the assessment, its objective, and its findings. It should provide a quick snapshot of the extent of the organization’s vulnerability level and its [cyber security posture](https://sprinto.com/blog/what-is-security-posture/). The executive summary includes:

* Scope of assessment
* A summary of the findings (with a graph)
* Number and severity of vulnerabilities discovered
* Minor vulnerabilities
* Exceptions/blind spots

**Scan results**

The scan results provide high-level details on the vulnerabilities discovered. For every vulnerability identified, the following are highlighted:

* Vulnerability type
* CVSS score
* Severity
* The affected area
* Details of the vulnerability
* Impact

**Details of tests performed**

This section presents specifics about the methodology, tools, and tests performed for identifying and assessing vulnerabilities. It covers:

* Test performed (for example, SQL injection test, cross-site scripting test etc.)
* Purpose of the scan/test/tool
* Testing environment details
* Methodology

**Findings**

Findings give an account of the discoveries from vulnerability assessments and pen tests and include the following details:

* Description of findings
* Supporting evidence or Proof of concept – how was the issue discovered
* Any additional reference links that helped with drawing conclusions

**Risk Assessment Profile**

Based on the findings, [risk assessments](https://sprinto.com/blog/risk-management-automation/) are carried out to draw conclusions on the organization’s risk profile. The severity, likelihood, and impact of vulnerabilities is taken into account to note down:

* Risk scores against vulnerabilities
* Prioritization of vulnerabilities based on risk scores

**Remediation planning**

This is the corrective action plan to address the prioritized vulnerabilities. It includes:

* Actionable steps to be initiated—policy changes, changes in configurations, etc.
* Intended outcomes
* Timeline for correction
* The parties responsible for remediation

**Benefits of vulnerability assessment report**

Vulnerability assessment reports facilitate a shared understanding of the [security gaps](https://sprinto.com/blog/security-assessment-guide/) and compliance checks that indicate possible vulnerabilities in the existing system. These are proactive tools for organizations to save costs associated with security breaches and present opportunities that can help build brand credibility.

The following are a few benefits of a vulnerability reports:



**Protection from cyber threats**

VAPT reports highlight the hidden weaknesses in security posture that hackers can take advantage of. They are great tools to stay abreast of security incidents and minimize the likelihood or impact of advanced cyber threats (for example, zero-day attacks).

**Compliance**

VAPT is considered a cybersecurity best practice that companies need to adopt to protect sensitive data. Periodic VAPT reports are, therefore, necessary to ensure compliance with several regulatory frameworks such as PCI DSS, [ISO 27001](https://sprinto.com/blog/iso-27001-compliance/), [HIPAA](https://sprinto.com/blog/hipaa-compliance/), and NIST that require a proactive approach toward safeguarding sensitive data.

**How Sprinto can help here:**

Sprinto sends you automated alerts when VAPT reports are due. You can also leverage Sprinto’s network to work with vetted VAPT partners and meet mandatory scan requirements for different compliance frameworks. [See how this can be done on Sprinto](https://sprinto.com/get-a-demo/)

**Better incident management**

Early identification and remediation of vulnerabilities lead to fewer escalations. It also helps amend and update incident management plans based on risk awareness. As teams start understanding the vulnerabilities that can be exploited it gives rise to a structured approach to strategies regarding response and remediation.

Checkout: [Top 9 Risk Assessment Tools in 2023](https://sprinto.com/blog/risk-assessment-tools/)

**Improved market perception**

Cybersecurity is a key concern for most clients today. Conducting frequent VAPT scans and sharing reports can be a quick way to demonstrate your commitment towards security-consciousness. This can not only improve the trust organizations have in the market but can shorten the sales cycle with enterprise clients.

**Closing thoughts**

VAPT reports are a crucial component of compliance. It helps paint a picture of an organization’s cybersecurity posture while also fulfilling an essential mandate for several compliance requirements. A compliance automation platform like [Sprinto](https://sprinto.com/) can help you managing numerous compliance related tasks such as gathering insights from VAPT reports and taking corrective steps among many others.

The platform sends you periodic reminders when VAPT scans and reports are due and serves as a single source of truth while monitoring your security and compliance status. Sprinto supports 15+ compliance frameworks and integrates with over 100 SaaS solutions to extend the scope of compliance.