

# Annual Penetration Testing for Cyber Resilience



In today's fast-paced digital world, cyber threats evolve daily, and even the most robust defenses can leave vulnerabilities unnoticed. Annual penetration testing is a critical step in building resilience by uncovering hidden risks and strengthening your organization's ability to anticipate, withstand, respond to, and recover from cyberattacks.

This checklist will guide you through the essential steps to ensure your organization's IT systems and data are secure.

## Steps to Strengthen Cyber Resilience with Penetration Testing

### ANTICIPATE

#### Understand the Difference Between Vulnerability Assessments and Penetration Testing:

- Vulnerability assessments identify potential weaknesses, while penetration testing simulates real-world attacks to exploit those vulnerabilities.

**Why:** Knowing the purpose of each helps you choose the right approach for your organization's needs.

#### Define Your Testing Objectives:

- Determine whether you need a broad vulnerability assessment or a targeted penetration test (e.g., cloud, internal, external, or application testing).

**Why:** Clear objectives ensure the testing aligns with your organization's risk profile and compliance requirements.

#### Prioritize Critical Systems:

- Focus on systems that store sensitive or mission-critical data, such as customer information, financial records, or intellectual property.

**Why:** Protecting high-value assets reduces the impact of potential breaches.

#### Engage Qualified Professionals:

- Work with certified cybersecurity experts who follow industry standards like OWASP, NIST, or PCI DSS.

**Why:** Expertise ensures accurate testing and actionable recommendations.

### WITHSTAND

#### Simulate Real-World Attack Scenarios:

- Include tests for phishing, ransomware, and insider threats to evaluate how well your defenses hold up under pressure.

**Why:** Realistic scenarios reveal gaps in your security posture.

#### Test Across Multiple Layers:

- Conduct tests for cloud environments, external networks, internal systems, wireless networks, and web applications.

**Why:** Comprehensive testing ensures vulnerabilities are identified across your entire IT environment.

#### Validate Security Controls:

- Assess the effectiveness of firewalls, intrusion detection systems, and access controls.

**Why:** Testing ensures your existing defenses are functioning as intended.

# Annual Penetration Testing for Cyber Resilience



## RESPOND

### Review and Prioritize Findings:

- Create a step-by-step plan to address identified vulnerabilities, including timelines and responsible parties.

**Why:** A clear plan ensures timely and effective resolution of issues.

### Develop a Remediation Plan:

- Conduct tests for cloud environments, external networks, internal systems, wireless networks, and web applications.

**Why:** Comprehensive testing ensures vulnerabilities are identified across your entire IT environment.

### Test Your Incident Response Plan:

- Use the penetration test to evaluate how your team responds to simulated breaches.

**Why:** Identifying gaps in your response plan helps improve readiness for real incidents.

## RECOVER

### Implement Fixes and Retest:

- Address vulnerabilities and conduct follow-up testing to verify they've been resolved.

**Why:** Retesting ensures issues are fully remediated and no new risks were introduced.

### Document Findings and Actions:

- Keep detailed records of vulnerabilities, remediation steps, and results to support compliance and future strategy.

**Why:** Documentation helps refine future tests and strengthens your overall security posture.

### Monitor for Emerging Threats:

- Use insights from the test to enhance ongoing monitoring and threat detection efforts.

**Why:** Continuous improvement is key to staying resilient in a dynamic threat landscape.

## Types of Penetration Testing to Consider

### 1. Cloud Pen Testing:

Focuses on securing cloud-based operations by identifying misconfigurations, insecure APIs, and exposed sensitive information.

**Why:** As cloud infrastructure grows, so do the threats targeting it.

### 3. Internal Testing:

Evaluates threats from within, such as compromised employee accounts or accidental security gaps.

**Why:** Protects against insider breaches and lateral movement.

### 5. Application or Web App Testing:

Identifies vulnerabilities in web applications and APIs to prevent unauthorized access or data leaks.

**Why:** Web applications are frequent targets for cybercriminals.

### 2. External Testing

Simulates how an attacker might exploit vulnerabilities in your external network perimeter.

**Why:** Crucial for assessing risks from outside your organization.

### 4. Wireless Testing:

Ensures Wi-Fi access points and devices are protected from unauthorized access or attacks like man-in-the-middle.

**Why:** Wireless networks are common entry points for attackers.

### Take control of your cybersecurity today.

Uncover hidden risks and strengthen your defenses with an annual penetration test from Rehmann Technology Services. Build a stronger, safer future — schedule your assessment now at [rehmann.com](https://rehmann.com).

**Rehmann**