PINE
RISK MANAGEMENT

# Pine Risk Management:

## Security Integrity & Improvement

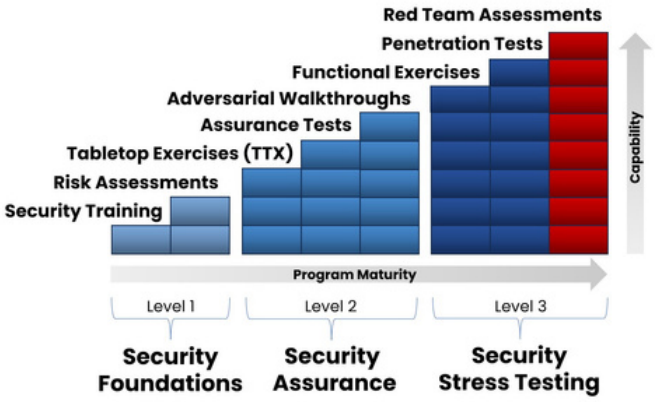
Isn't it time your security was as strong as your vision? We are your partners in security integrity, testing, and improvement. Our comprehensive approach validates your controls, identifies gaps, and partners with you to create stronger security, protecting people, companies.

## Why Red Teaming?

Understanding the Need for Effective Security

Absolute security is a myth. Companies spend thousands, often millions, to build customized physical and cyber security systems to protect their people, property, assets, facilities, and reputation. The most common security system consists of at least two dozen overlaid security controls. These controls can be categorized into people, technology, and processes. But do these controls work? Are they properly configured? Do they interface with each other effectively?

Security Integrity & Improvement Spectrum




Do you know whether your security works?

Wouldn't you like to know whether your security budget is well-spent? If your security program is deterring and preventing incidents?

## Our Approach

Informed Decision-Making for Better Business

At Pine Risk Management, we believe that better decisions lead to better business. Effective Risk Management reduces uncertainty, increases confidence, and brings your business peace of mind.

Through threat modeling, risk assessments, functional exercises, and red teaming, we offer control performance data, validation of your control integrity, and assessment of your actual security posture. This approach stress-tests controls, reveals the severity of vulnerabilities, and offers solutions to your unique security concerns.

**Our Services:**

- **Security Foundations**
- **Security Assurance**
- **Security Stress Testing**

Proactive security testing uncovers unknown unknowns, proposes mitigation tactics, and helps prioritize every dollar of your security spend.

# The Benefits of Our Services

The 10 Cs of Effective Security

We help develop and support security strategies through the 10 Cs of effective security programs. From compliance to counterintelligence, budget allocation to security awareness, Pine Risk Management is your partner in security program development, improvement, assurance, and maturity.

1. **Confidence**
   The knowledge that your security system will work during an incident or when faced with a real adversary.
2. **Corrective Action**
   Opportunity to proactively fix gaps in your layers of security.
3. **Compliance**
   Comply with laws, regulations, certifications, and industry-leading practices.
4. **Cost Savings**
   Avoid breaches, incidents, lawsuits, and expensive but ineffective security controls.
5. **Credibility**
   Demonstrate to stakeholders and clients that you take security seriously and have taken steps to protect their interests.
6. **Capacity Building**
   Increase the capability and readiness of your security team to respond to real-world threats.
7. **Creativity**
   The standard security solutions no longer stop determined adversaries. Red teaming is the catalyst for creativity in security.
8. **Conditioning**
   Practice makes perfect. Condition a strong security response, and improve capabilities and confidence through conditioning.
9. **Collaboration**
   Enhance teamwork and communication among your security, IT, and facilities teams through joint red team exercises.
10. **Culture**
    Build a security-focused culture within your organization, where all employees understand and prioritize security.

## Ready to Enhance Your Security?

We are your partners in the security integrity testing and improvement journey. We make security simpler, more accessible, and attainable for all through research, education, and consulting with a throughline of excellence in everything we do. We are here to help you protect and profit.

Visit **PineRisk.com** for more information and to start your journey towards a more secure organization.

PINE
RISK MANAGEMENT

PINE
RISK MANAGEMENT

# Security Foundations

## Building a Strong Security Base

## Risk Assessments

### Identifying and Prioritizing Vulnerabilities

Risk assessments are essential for identifying vulnerabilities, understanding potential threats, and evaluating their impact. This process helps prioritize time and resources to protect the most critical assets and address the main threats to the organization. A security risk assessment involves evaluating vulnerability, threat, and impact (or asset, or consequence).

Understanding where to focus time and effort to mitigate vulnerabilities and protect the most important assets is essential. No security team can mitigate all risks, but a Security Risk Assessment helps prioritize the most significant ones.


## The Benefits of Our Approach

### Effective Risk Management

At PRM, we help you build a strong security foundation through rigorous risk assessments and strategic training. Our approach ensures that you allocate your resources to the most significant threats first.

**Benefits List:**

- Identify Vulnerabilities: Recognize weak points in your security.
- Evaluate Threats: Understand potential threats to your organization.
- Prioritize Actions: Focus on the most critical risks.
- Enhance Security Posture: Strengthen overall security measures.
- Create a Security-Aware Culture: Ensure all employees are prepared and aware.

**Effective risk management reduces uncertainty, increases confidence, and brings your business peace of mind.**

## Risk Assessment

### Process

1. **Identify Assets**
2. **Evaluate Threats**
3. **Assess Vulnerabilities**
4. **Determine Risk**
5. **Implement Controls**

## Security Training

### Empowering Your Team

While risk assessments are crucial, security training programs for employees at all levels help create a security-aware culture. Training ensures that everyone understands their role in maintaining security and can recognize potential threats.

Security training complements risk assessments by ensuring that all team members are prepared and aware.

## Strengthen Your Security Foundations

Strengthening your security foundations is the first step towards building a resilient organization. Pine Risk Management is here to support you with comprehensive risk assessments and strategic training programs.

Visit **PineRisk.com** for more information and to start your journey towards a more secure organization.

PINE
RISK MANAGEMENT

# Security Assurance

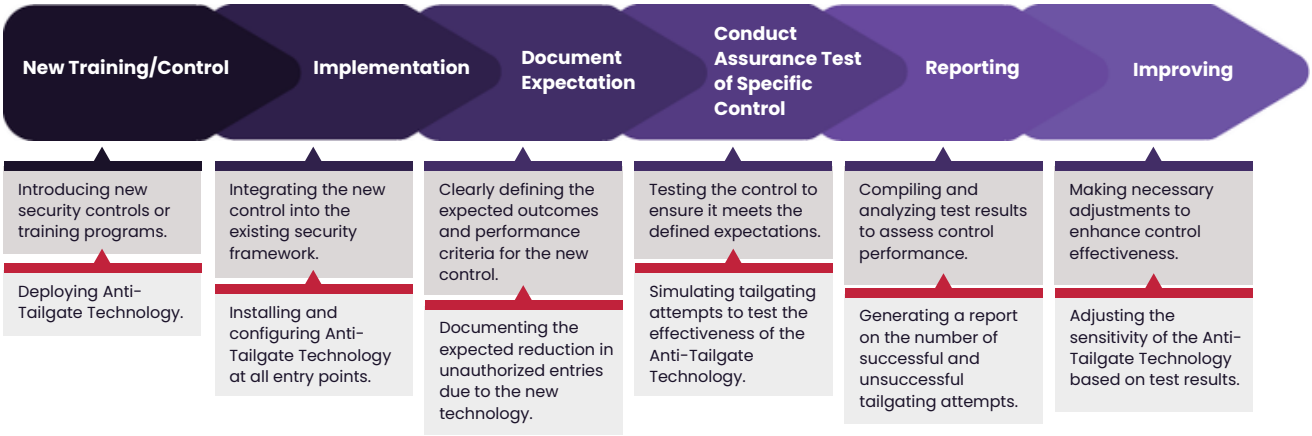
## Ensuring Your Security Measures Work

Security assurance validates the effectiveness of your security measures, ensuring they work as intended when faced with real threats. This continuous process helps maintain robust security through regular testing and improvement.

## Security Assurance Lifecycle

The Continuous Process of Security Assurance

The security assurance lifecycle is an ongoing process that involves implementing, testing, and improving security controls. This lifecycle ensures that security measures remain effective and aligned with industry standards and frameworks like NIST CSF, CMMC, ISO 31000, and ISO 27000.




## Our Security Assurance Services

Tailored Solutions for Comprehensive Security

We offer three specific services under our Security Assurance category, designed to validate and enhance your security measures.

| Service 1: **Tabletop Exercises (TTX)** | Service 2: **Assurance Tests** | Service 3: **Adversarial Walkthroughs** |
|---|---|---|
| **Description:** Simulated scenarios to test and improve organizational response to various security incidents. | **Description:** Real-world tests of specific controls, such as new implementations or training programs. These hyper-targeted pen tests /stress tests ensure the improvement /control is working effectively. | **Description:** Controlled simulations of adversarial activities to identify vulnerabilities and improve defense mechanisms. These white-box assessments involve walking through the site and performing red teaming activities without being covert, often with a member of the security team. |
| **Example:** Conducting a tabletop exercise to prepare for a potential cyber attack, involving key stakeholders to discuss and plan the response. | **Example:** Testing the effectiveness of Anti-Tailgate Technology by simulating tailgating attempts and evaluating the results. | **Example:** Walking through a facility to identify vulnerable doors and technology, with a security team member observing and understanding the vulnerabilities. |

Assurance testing and adversarial walkthroughs provide real-world insights into your security measures, helping you identify and fix vulnerabilities effectively.

## Frameworks and Standards

Aligning with Industry Standards

Aligning your security assurance activities with established frameworks and standards ensures comprehensive and effective security management. These frameworks provide guidelines for best practices in risk management and security assurance.

Adhering to frameworks like NIST CSF, CMMC, ISO 31000, and ISO 27000 helps ensure your security measures are robust and industry-compliant.

| Framework | Description |
|---|---|
| **NIST CSF** | A framework for improving critical infrastructure cybersecurity. |
| **CMMC** | A cybersecurity standard for defense contractors to protect sensitive information. |
| **ISO 31000** | Guidelines for risk management practices. |
| **ISO 27000** | Standards for information security management systems (ISMS). |

## The Benefits of Security Assurance

Why Continuous Assurance Matters

Continuous security assurance provides numerous benefits, including:

**Benefits:**

- **Validation of Controls:** Ensure your security measures are effective.
- **Identification of Gaps:** Discover and address weaknesses in your security.
- **Enhancement of Compliance:** Meet industry standards and regulatory requirements.
- **Improvement of Security Posture:** Strengthen your overall security framework.
- **Building Confidence:** Gain assurance that your security can withstand real threats.

Regular security assurance activities help maintain a high level of security and readiness against potential threats.

## Strengthen Your Security Assurance

Implementing a robust security assurance program is crucial for maintaining effective security measures. Pine Risk Management provides comprehensive security assurance services to help you validate, test, and improve your security controls.

Visit **PineRisk.com** to learn more about how we can help you enhance your security assurance.

PINE
RISK MANAGEMENT

PINE
RISK MANAGEMENT

# Security Stress Testing

## Fortifying Your Security with Stress Testing

Practice, Prevent, and Proactively Secure

## Stress testing

Stress testing is crucial for verifying the effectiveness of security programs by pushing each layer to its limits and identifying vulnerabilities before adversaries can exploit them. Our collaborative red teaming approach helps validate your controls and uncover assumptions, ensuring your security measures are effective and reliable.

## Our Services

We offer three key services in this category

- **Functional Exercises**
- **Penetration Testing**
- **Red Teaming**

## Red Teaming Benefits:

Gaining Answers, Building Awareness, and Securing Advantage

**Answers:** Understand who will target you, how they will target you, and whether they will succeed. (Use a Threat Model Graphic to illustrate these insights.)

**Awareness:** Uncover hidden vulnerabilities and understand your weaknesses before adversaries do. Awareness leads to strategic advantage.

**Advantage:** Maintain competitive advantage over your competitors and your adversaries by proactively mitigating risks and maintaining a robust security posture.

Red teaming uncovers critical information at every step of the threat model

Gain actionable recommendations and valuable insights through comprehensive red team assessments, enhancing your overall security strategy.

## Red Teaming
Simulated Attacks & Worst-Case Scenarios

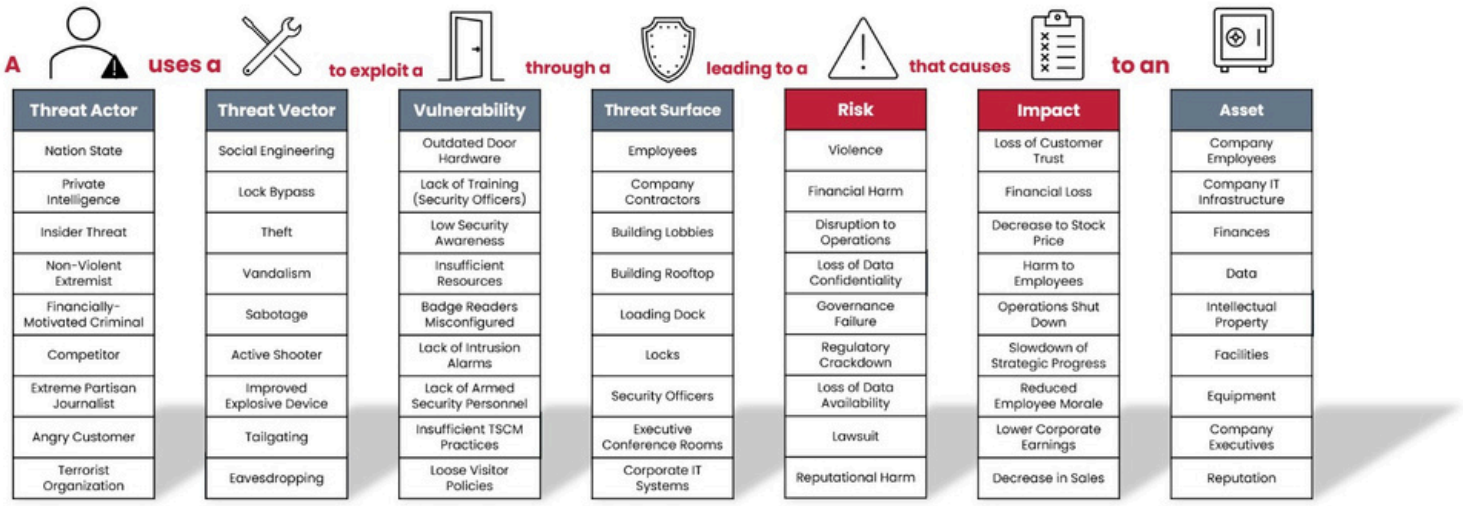
Red teaming involves full-scope assessments to evaluate your security from an adversary's viewpoint. Whether you want to know if an outside can breach your defenses, or if you want to join us for the fun of the assessment to see your program from an adversary's standpoint, our red team assessments answer questions and give security leaders the knowledge and confidence to stay a step ahead.

## Three Types of Red Team Assessments

| Security Improvement | Counterintelligence | Budget Allocation |
|---|---|---|
| **Goal:** Improve Security by Stress-Testing Security Controls | **Goal:** Proactively Protect from Advanced Adversaries | **Goal:** Return on Investment (ROI) For Security Spend |

## Bring your Threat Models to Life

Can your security withstand real-world situations?
Test, practice, and improve your defenses with red teaming




## Functional Exercises
Preparing for Real-World Incidents

Functional exercises involve realistic simulations to test your security measures. These exercises help prepare your team for actual attack scenarios, ensuring that everyone knows their role and can respond effectively.

**Functional exercises turn theoretical plans into practical readiness.**

## Penetration Testing
Identifying and Mitigating Vulnerabilities

Penetration testing involves real-world tests of specific controls, such as new implementations, safeguards for high-value assets, or new training programs. These targeted tests ensure that your controls are working as expected.

**Penetration tests provide a deep dive into your security measures, identifying vulnerabilities and ensuring effective controls.**

PINE
RISK MANAGEMENT

PINE
RISK MANAGEMENT

# Service Offerings

## Bespoke Solutions for Your Business Needs

At Pine Risk Management, we understand that each business has unique security challenges. Our bespoke solutions are designed to meet you where you are, whether you're just starting to build your security program or looking to enhance an existing one. Our comprehensive approach includes everything from foundational training to advanced red team assessments, ensuring that your security posture is robust and resilient.

Red team assessments are the key to unlocking your security potential.

**Our services** are designed to provide you with the confidence you need to operate securely. We offer **four levels** of service, each tailored to meet the specific needs of your organization. From security improvement training and risk assessments to advanced stress testing and red team assessments, our goal is to help you manage risks effectively and communicate your security status to stakeholders.

| Service Level | Security Foundations | Security Assurance | Security Stress Testing |
|---|---|---|---|
| *Services* | *Security Training*<br>*Security Risk Assessments* | *Tabletop Exercises (TTX)*<br>*Adversarial Walk Through*<br>*Assurance Tests* | *Functional Exercises*<br>*Penetration Tests*<br>*Red Team Assessments* |
| 1 Ad-Hoc | **Customize Your Security Solutions** | | |
| 2 Standard | **4 Per Year** | **4 Per Year** | **2 Per Year** |
| 3 Elevated | **4 Per Year** | **6 Per Year** | **4 Per Year** |
| 4 Enterprise | **6 Per Year** | **12 Per Year** | **6 Per Year** |

PINE
RISK MANAGEMENT

| Customizable Security Solutions | Standard | Elevated | Enterprise |
|---|---|---|---|
| GSOC Capability and Improvement Assessment | Yes | Yes | Yes |
| Threat Model Reports | Yes | Yes | Yes |
| Scenario Development for Exercises and Training | Yes | Yes | Yes |
| Advanced Security Training | Yes | Yes | Yes |
| Executive Protection Assessments | Yes | Yes | Yes |
| Vulnerability Management | Yes | Yes | Yes |
| Deterrence and Prevention Report | Yes | Yes | Yes |
| Annual Assurance Report | Yes | Yes | Yes |
| Protective OSINT Intelligence Scan | Yes | Yes | Yes |
| Risk Acceptance Governance, Templates, and Management | | Yes | Yes |
| Live Security Assurance Dashboard | | Yes | Yes |
| Adversarial OSINT Scan | | Yes (annual) | Yes (semi-annual) |
| High-Risk Program Tests (Supply Chain, Mail Screening, Weapons Screening, Event Security) | | Yes | Yes |
| Assessments of Data Centers, PoP, CoLo, and other communications infrastructure | | Yes | Yes |
| Site-Specific Geographic Risk Reports | | Yes | Yes |
| Applied Critical Thinking (Analytical Red Teaming / Groupthink Mitigation) Workshop | | Yes | Yes |
| Counterintelligence Assessments | | | Yes |
| Insider Threat Detection Assessments | | | Yes |
| Oversight of Vendor-Managed Tests (including contract language, training, and test management) | | | Yes |
| Risk Register | | | Yes |
| Compliance Assistance | | | Yes |
| TSCM Capability Assessment | | | Yes |
| Site-by-Site Assurance Scorecards | | | Yes |