READINESS GUIDE

BISHOPFOX

RED TEAM READINESS

A QUESTION-DRIVEN PLANNING FRAMEWORK

WHO IS THIS GUIDE FOR?

CISOs and other security leaders considering Red Teaming

Organizations looking to improve their detection and response capabilities against real-world threats

Red Teaming is one of the most effective ways to measure the state of an organization's security posture. It often overturns assumptions about just how secure an organization really is.

By simulating the tactics and techniques used by actual adversaries, Red Teaming tests how well your organization can defend its most valuable assets, from business-critical systems to sensitive customer data-revealing hidden weaknesses and blind spots in your security program.

Red Teaming in a Nutshell:

Simulates real-world attacks to test your security posture.

Focuses on attack goals, like accessing crown jewels—not just finding vulnerabilities.

Most valuable if you're ready for it. This guide helps you assess that.

Asks key planning questions to align stakeholders and define scope.

Uses frameworks such as the 5/5/20/X to plan future red team operations and scenarios around your unique security posture.

What makes Red Team results so valuable?

The output of Red Team operations isn't just a list of issues or vulnerabilities that you need to address, Red Teams provide the full-attack narrative from your adversary's point of view—from initial entry to movement throughout your network, the methods used to bypass defenses, and the result of whether attack objectives were successful.

However, a Red Team exercise is only as valuable as the planning behind it. Poorly scoped or misaligned engagements can miss critical risks, produce misleading results, or cause unnecessary disruptions in your operations. To maximize the value of Red Teaming, organizations should prepare by: clarifying their objectives, defining the scope, and ensuring that key stakeholders are aligned.

This guide walks you through the critical planning questions you need to ask **before engaging in Red Teaming and includes a questionnaire↗ you and your team can use to maximize your next engagement.**

<h3 class="mb-2 text-headline-whisper uppercase text-bfx-seafoam-bright ">RED TEAM EXPERTISE A
INGENUITY</h3>
class="mt-8 text-copy prose prose-dark text-bfx-timberwolf "><p><strong>Battle-tested
Offensive Security Specialists </strong></p>
the brightest minds in offensive security with decades of proven experience successful
through even the most hardened defenses.</p>
<p><strong>Diverse Ethical Hacking Skillsets </strong></p>
<p>Assimilates a broad range of specialists into a unified engagement, ensuring that

WHAT IS RED TEAMING?

Red Teaming↗ is a specialized form of objective-based security testing that simulates real-world threat scenarios. Unlike traditional penetration testing↗, which systematically probes an entire network, application, or cloud environment to identify and exploit as many vulnerabilities as possible, Red Teaming focuses on specific attack objectives to test an organization's ability to detect, respond to, and recover from real-world attacks. Red Teams, when utilized properly, can provide significant value to the business in the form of strategic risk reduction, enhanced incident response, and greater alignment of the organization's security budget with true enterprise risks.

These objectives (also known as "trophies") vary depending on what is most important to the organization. These may include establishing a foothold on internal networks using external vulnerabilities, gaining unauthorized access to financial or other critical systems and data, or physically infiltrating a restricted area of a building or campus. To test defenses under realistic attack conditions, Red Teams are stealthy and mimic the strategies and tactics used by real adversaries across technical, physical, and social domains.

Red Team engagements generate evidence-based insights similar to those revealed in a real-world breach—but without the financial and reputational fallout. And unlike an attacker, a Red Team delivers a detailed report afterward, outlining their approach and providing actionable recommendations to harden the organization's defenses.

> "Red Teaming provides proof that cuts through all the hypothetical and subjective assumptions about what's secure and what's possible. It gives CISOs and security decision-makers crystal-clear, unadulterated ground truth to inform their security and budget strategies."
>
> — **TREVIN EDGEWORTH**
> RED TEAM DIRECTOR, BISHOP FOX

IS YOUR ORGANIZATION READY FOR RED TEAMING?

Now that you understand what Red Team is and what it isn't, are you ready to invest the time, money, and effort to deliver the most value to your organization?

As reference, Bishop Fox assesses Red Team readiness based on certain security maturity benchmarks:

A **strong security culture** where issues are addressed promptly.

A **functional vulnerability management** program.

An **established SOC** capable of responding to detections.

A **governance**, **risk**, and **compliance** (GRC) **team** that can act on control gaps.

Prior **experience with penetration testing** or other offensive security assessments.

Not Quite Ready?

If your organization isn't ready to make the leap from penetration testing to full-scale Red Teaming, Adversarial Controls Testing↗ offers a practical, cost-effective intermediate step to assess your detective and preventive controls for endpoint, network, and email. This collaborative approach blends Red Team offensive techniques using automated playbooks with real-time Blue Team defensive analysis to identify and resolve gaps.

You'll receive detailed test results for each area, along with an overall control score, helping you identify gaps and strengthen your defenses before committing to a full Red Team engagement.

KEY QUESTIONS TO ASK BEFORE A RED TEAM ENGAGEMENT

A successful Red Team operation starts with clarity. The better an organization defines its priorities and goals, the more valuable the insights will be. Before launching a Red Teaming engagement, organizations should answer the following critical questions to define objectives, scope, stakeholders, and operational parameters. Download our fillable worksheet↗ to gauge your organization's readiness and prepare for a Red Team operation.

What Are We Trying to Accomplish?

Unlike other security testing methods, a Red Team exercise is designed to assess how well an organization can detect, respond to, and recover from real-world attacks. Those attack scenarios are the specific objectives of the engagement.

For example, the test might aim to:

- **Cut power** to a factory
- **Delete a mortgage** from a system
- Execute an **unauthorized wire transfer**
- Access **customers' payment card data**
- **Physically enter the C-suite floor** of company headquarters

A strong Red Team will not stop after finding one way to achieve the goal. Instead, they will continuously test different tactics, techniques, and procedures (TTPs) to identify all possible paths to the target.

Key Planning Questions:

What are our desired outcomes – what are we trying to learn?

What are our 'crown jewels'? *Crown jewels are your most valuable assets— e.g. business-critical systems, customer data, or critical intellectual property.*

What trophies are we targeting for this exercise?

What known threats or adversaries are we most concerned about?

What scenarios or tactics should be tested? *e.g. ransomware, insider threats, backdoors in code.*

A Planning Framework

Best practice requires Red Teaming to be strategically planned and proactive, rather than request-driven and tactical.

It can be helpful to use a 5/5/20/X framework, as described below. The underlying approach is based on important principles of creating a plan to ensure your Red Team activities are strategically tailored and aligned to your organization's unique security posture and threat landscape.

This method sets the foundation for a short, medium, and long-term roadmap for Red Team operations to ensure you are covering the highest-risk attack scenarios. Use it to plan a series of scenarios, with each one focusing on one or more things from your list. For example, one Red Team engagement could focus on two of the top five threats, two of the five threat actors, and five to eight of the crown jewels.

A Breakdown of the 5/5/20/X Framework:

5 top threats to your organization

5 top threat actors targeting your industry

20 crown jewels (your critical assets)

X: your number of lines of business

Need help identifying the riskiest scenarios?
Check out our blog, Five Common Mistakes Attackers Love↗, to see the top five weaknesses that attackers repeatedly exploit—based on hundreds of Bishop Fox's Red Team engagements.

For a financial services organization, the following could be an example:

Top 5 Threats

- RANSOMWARE
- INSIDER THREATS
- SUPPLY CHAIN ATTACKS
- BUSINESS EMAIL COMPROMISE
- ETC.

Top 5 Threat Actors

- SCATTERED SPIDER
- LOCKBIT RANSOMWARE GROUP
- GHOST RANSOMWARE GROUP
- APT29
- ETC.

Top Crown Jewels

- RANSOMWARE
- ERP SYSTEM
- PAYMENT PROCESSING
- CORE BANKING PLATFORM
- COMPANY WEBSITE
- CRM PLATFORM
- ACTIVE DIRECTORY
- MFA (LIKE OKTA)
- DISASTER RECOVERY AND BACKUP INFRASTRUCTURE
- EMAIL SERVICES
- ETC.

Lines of Business

- RETAIL BANKING
- MORTGAGES/ LENDING
- DIGITAL/ONLINE BANKING
- TRADING AND INVESTMENT
- COMMERCIAL BANKING
- INSURANCE

2 What is the Scope of the Engagement?

Once objectives are set, the scope defines the boundaries: when the test will happen, how it will begin, and what parts of the attack surface will be included.

Key Planning Questions:

What is the timeframe?
(Note that if you are hiring an outside firm, Q4 is the busiest time for these resources; Q1 or Q2 may offer better availability.)

—

Should the Security Operations Center (SOC) be aware or unaware of the test?

—

Will this engagement be zero knowledge, partial knowledge, or full knowledge?

—

Will the test simulate an external attack or start from an assumed breach?

—

What aspects of your attack surface will be included?
(The best Red Team exercises involve the entire attack surface–digital, physical, and social/human—to replicate the approach of a real adversary, who will use any means available to reach their objective. However, sometimes that won't be practical or possible.)

—

Are any systems or attack types off-limits?
(Some organizations restrict tests on certain production environments or critical business functions.)

Who Should Be Involved in Defining the Scope?

Some organizations limit scope-setting to the CISO, while others include business unit leaders, security teams, and legal stakeholders—especially when the Red Team exercise targets specific business functions. Engaging these stakeholders can reveal valuable insights, such as potential worst-case scenarios they want to test or their biggest security concerns.

To prepare, you might ask:

- **What is your nightmare scenario?**
- **How could we simulate it to help you defend against it?**

Who Needs to Know About the Test?

The Trusted Insider Group (TIG) consists of individuals who know about the Red Team operation and can help manage any issues that arise. To maintain the realism of the exercise, they must keep the test plans strictly confidential.

Ensuring that key decision-makers are in the loop before launching an exercise helps prevent costly misunderstandings. Bishop Fox has encountered cases where a company's CISO was not aware of an active Red Team exercise—leading to unnecessary panic and even derailing the test altogether. Whatever your Red Teaming plans, always ensure your CISO is in the loop.

Standard TIG Members:

- CISO (or equivalent security leader)
- SOC leader/point of contact
- Offensive security lead

Additional TIG members (depending on focus):

- Line of business leader (if testing a specific department)
- Physical security leader/building point of contact (for physical intrusion testing)
- HR representative (for insider threat scenarios)
- Cloud expert (if testing cloud environments like Azure, AWS, or GCP)

Key Planning Questions:

Who needs to be informed about the Red Team exercise?

Have all necessary stakeholders been briefed in advance?

Have we clearly communicated the need for confidentiality—both before and during the engagement?

4 What Are the Rules of Engagement?

Defining clear engagement parameters ensures that **Red Team testing is realistic AND controlled**. Without well-defined rules, Red Team operations can cause operational disruptions or even legal trouble.

Key Planning Questions:

What risks should be mitigated in advance?
(E.g. production system impact, legal concerns)

During what hours will testing occur?

How will initial access be attempted?
(E.g. phishing, social engineering, physical access)

How often will the team communicate and through what channels?

What is the deconfliction process if the Red Team is detected?

Are legal authorization letters in place for physical tests?

READY TO PUT YOUR DEFENSES TO THE TEST?

Are You Prepared to Face the Adversary?

Red Teaming is more than a test—it's a transformative experience that reveals the true resilience of your security program. By thinking like an attacker, you gain unparalleled insight into how your defenses perform under real-world pressure. But the value of this simulation hinges on smart planning, stakeholder alignment, and clearly defined objectives.

Whether you're protecting financial systems, sensitive data, or critical infrastructure, this guide has equipped you with the foundational questions to ask, frameworks to apply, and operational considerations to weigh. Now it's time to put that knowledge into action.

If you're ready to take the next step, whether through a full-scale Red Team operation or a stepping-stone like Adversarial Controls Testing, make sure you're partnering with a team that understands both the stakes and the strategy.

Contact Bishop Fox today
to start planning your **Red Team engagement**.

ABOUT BISHOP FOX

Bishop Fox is the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments.

LEARN MORE AT BISHOPFOX.COM