anjuna®

Privacy by Default with Anjuna and the NIST Framework

The Importance of Cybersecurity

The world of technology is challenged to follow a new game plan for cybersecurity. We live in a world of internal and external vulnerabilities, where threat actors can obtain sensitive personal information, including Social Security, healthcare, and credit card data. The risk demands we handle customer intelligence with the most scrupulous means and mindfulness.

Unfortunately, the simple reality is that hackers only need access to a single aspect of the network, and your whole organization can be compromised via a lateral attack. One slip-up can harm your customers and your organization within minutes, as happened in the breach of Capital One.

Due to the pervasive nature of these threats, organizations must be more proactive and less *reactive*. Rather than merely waiting for hackers to gain access to your business and customer information, your teams must actively evaluate your cybersecurity strategy and resources and be ready to preemptively execute a powerful defense.

One of the most effective ways to reduce your attack surface is to adopt the National Institute of Standards and Technology (NIST) Framework. NIST is a unit of the U.S Commerce Department that promotes measurement standards. Ultimately, the NIST Framework can keep you and your company on the same page as you work to minimize security risks.

The NIST Framework: Basic Understanding

The NIST Framework was established in 2013 in response to former President Obama's executive order 13636 (titled Critical Infrastructure CyberSecurity). It ordered NIST to work with stakeholders in developing a voluntary framework to minimize cybersecurity risk to critical infrastructure. The NIST model serves as a valuable tool to standardize security in company frameworks.

The Framework's three components consist of Core, Implementation Tiers, and Profiles.

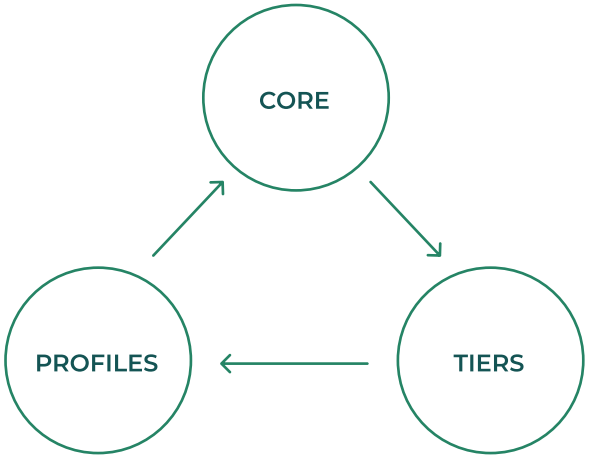


Figure 1: The circular and on-going relationship between the three components of the NIST Framework.

Core

Let's begin with the Core, which focuses on cybersecurity activities and outcomes that your organization can easily implement. It is designed to simplify the deployment of a multi-disciplinary team to communicate about cybersecurity technology initiatives in an easily comprehensible way.

The Core's functions include categories and subcategories covering the vast surface space of cybersecurity. For example, the five high levels of operations are Identify, Protect, Detect, Respond, and Recover, with a "rinse-and-repeat" cycle.

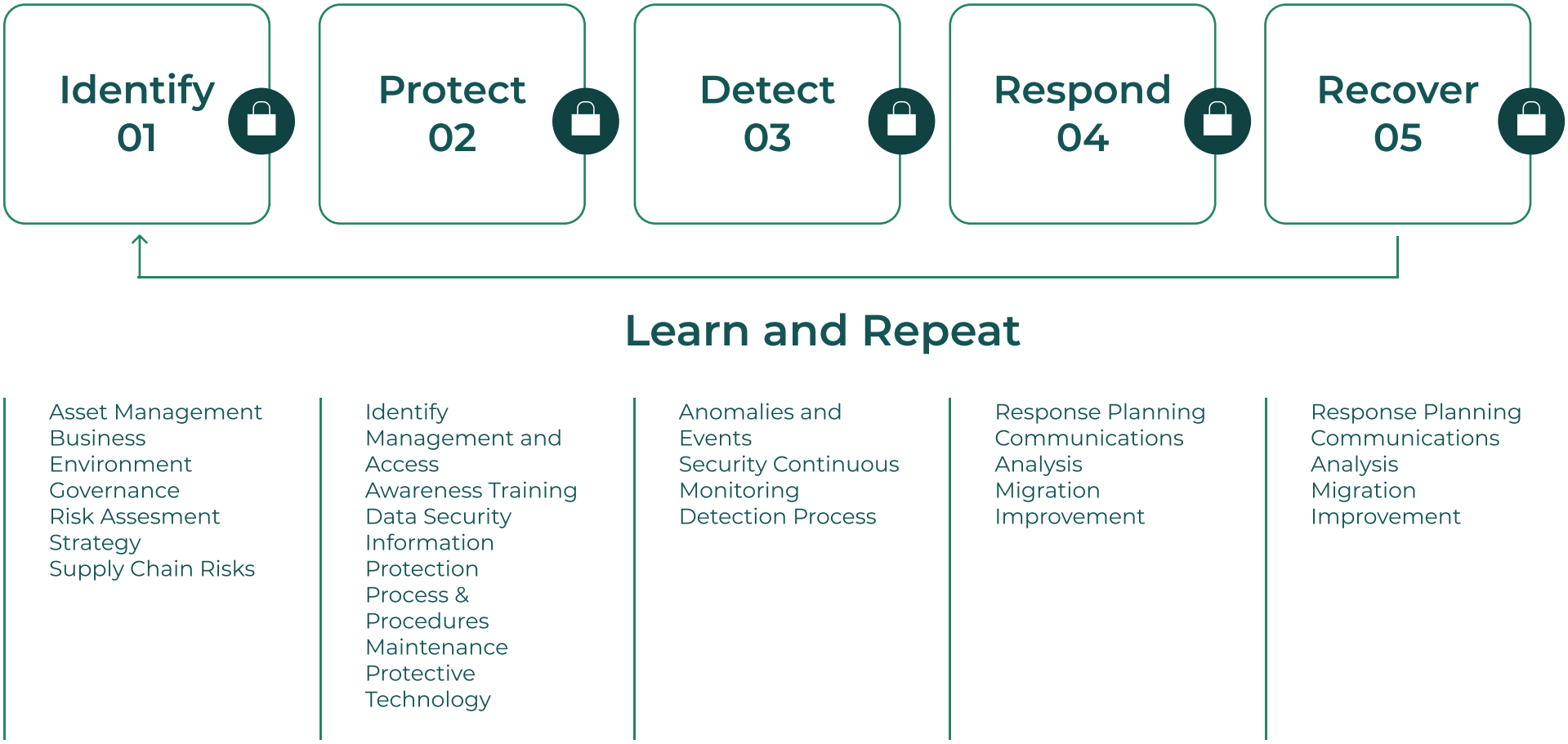


Figure 2: The five stages of the Core function in the Framework.

Anjuna Privacy Platform Tiers

There are four NIST Framework tiers on the Anjuna Privacy Platform: Partial, Risk-Informed, Repeatable, and Adaptive.

These tools determine whether your risk management policies map to the NIST Framework. Using the Anjuna Privacy platform we can help your company improve your posture in the many core frameworks of NIST implementation.

To the right is the expanded definition and explanation of how Anjuna can help your security posture. With our privacy platform you can take back control.

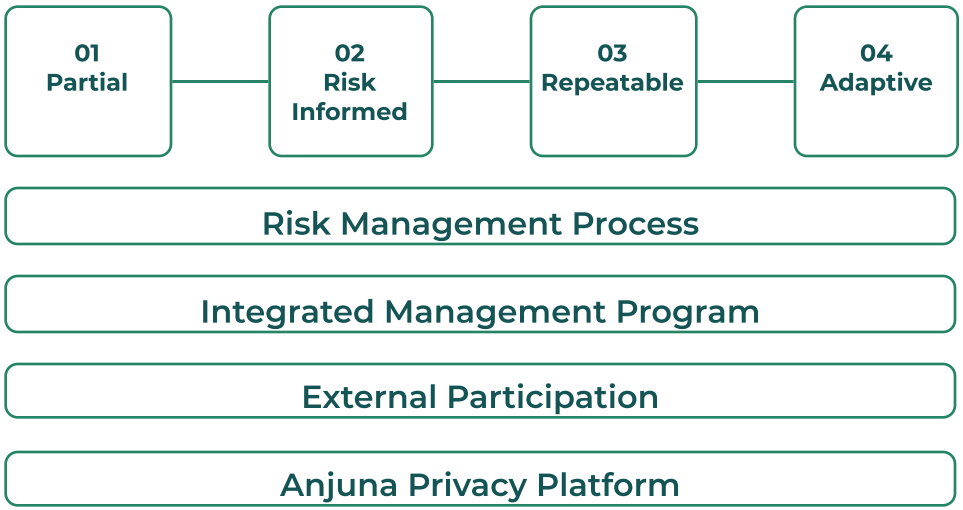


Figure 3: Each tier in the Framework designates the level of mitigation of cybersecurity risks.

1. **Partial**
   - Tier 1 covers businesses with no security processes in place. Businesses in Tier 1 are classified as not having much cyber maturity at all. Companies on this tier tend to fail at prioritizing cybersecurity settings appropriately. At this level, they should make efforts to understand and properly address cybersecurity risks. Tier 1 is a great starting point if you want to have a process in protecting PII, for example. By leveraging Anjuna Security technology, you can take a basic step in reducing your attack surface by hiding your application process in a secure enclaves.

2. **Risk-Informed**
   - Tier 2 is for businesses that may understand risks and are currently addressing some compliance requirements; however, they may not be addressing all the security concerns or policies across the entire business. In Tier 2, you are taking your security more seriously. With our Anjuna policy manager you can now build attestation into your process and protecting your critical Key Management systems and your front end applications.

3. **Repeatable**
   - Tier 3 is for businesses that have executive-approved risk management and cybersecurity best practices in place. Businesses in this category are generally more prepared for cybersecurity threats, risks, and addressing vulnerabilities in their environment. Businesses in Tier 3 can now move into more advanced CI/CD deployment of their applications with secure enclaves and drive change in a more real-time, proactive manner, rather than always taking a reactive approach.

4. **Adaptive**
   - Businesses in Tier 4 will utilize advanced adaptive cybersecurity practices. Adaptive security is an approach to cybersecurity that analyzes behaviors or events to help protect from or adapt to threats before they happen. The adaptive tier allows businesses to continuously assess risk and automatically provide proportional enforcement that can be dialed up or down based on past experiences and current industry best practices. When customers reach the Adaptive stage, they can employ Tiers 3 + 4 to build a security policy that reduces the complexity of their cybersecurity programs. This approach minimizes their attack surface and the risk from internal and external actors.

Cybersecurity Profiles

The NIST Framework contains profiles that help an organization identify opportunities for improving its current cybersecurity posture. These profiles are a snapshot of the organization's requirements and objects, risk profile, and available resources. By comparing them against a "target" profile, organizations can better understand which improvements are needed to eliminate cybersecurity risks.

Figure 4: Opporutunities for organizational improvements to cybersecurity can be quickly identified and mapped with the use of the NIST Framework.

Deploying privacy in a CI/CD platform minimizes your attack surface when you're building a new cloud or on-premises environment. Security by default is the ideal state. A DevSecOps approach enables building an environment compliant with NIST controls. The following section addresses the importance of the NIST Framework.

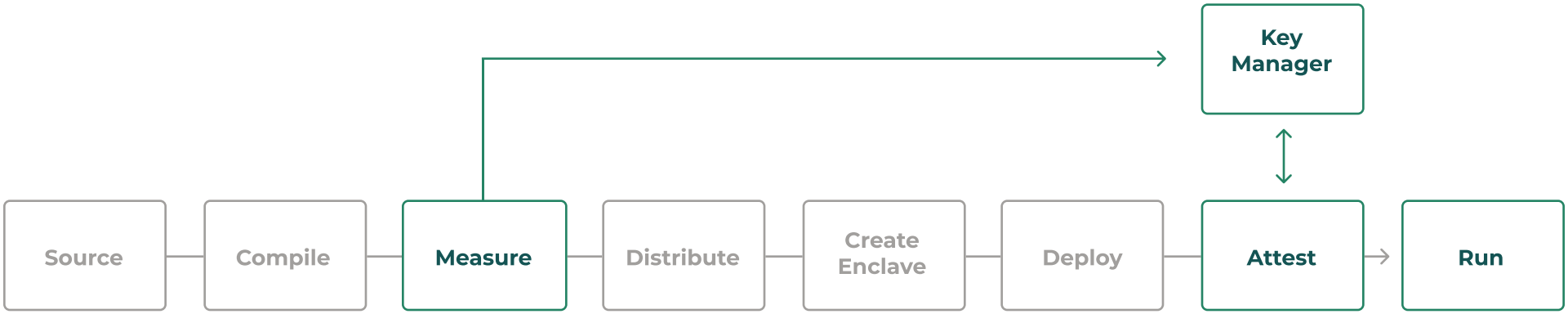


Figure 5: DevSecOps allows for an NIST-compliant environment while minimizing the overall attack surface.

Importance of the NIST Framework

The NIST Framework provides a uniform set of guidelines and principles that all companies can use to improve their cybersecurity posture. The Framework makes it easier for you to design a customized, comprehensive cybersecurity strategy, rather than piecing together a patchwork of solutions.

A stringent Framework helps your organization manage a significant number of cybersecurity risks efficiently and flexibly.

The NIST Framework can help properly align information security programs; for example, the Maritime Bulk Liquids Transfer Program used the NIST Framework to:

- Identify business priorities and compliance requirements
- Conduct risk assessments
- Determine gaps between the Current State and Target State Profiles
- Create a road map to reduce many cybersecurity risks

The NIST Framework can solve a variety of cybersecurity issues within your organization. It can help convince leadership to implement specific management procedures that minimize cybersecurity risk.

Beyond this, the NIST Framework helps all key stakeholders get on the same page. It can even convince C-suite executives to allocate additional funds in this year's budget to patch up cybersecurity risks tactically.

The Framework is a well-designed structural skeleton that you can mold and shape to promote objective progress toward your cybersecurity goals. NIST can hold your team accountable and help ensure that your infrastructure can withstand hackers and other cybercriminals.

Getting Started with Anjuna Security

How does Anjuna Security help you embark on implementing the NIST Framework?

The NIST Framework's flexibility helps your organization employ the best technologies to meet its cybersecurity needs. Anjuna Security has enabled privacy by default—whether in a cloud, on-premises, or hybrid environment. Anjuna® Confidential Computing software enables Confidential Computing by unleashing the power of secure enclaves to deliver the building blocks needed to implement a secure framework that follows NIST recommendations. The Framework helps reduce your surface attacks and maximizes the use of available technologies using a single runtime binary. Anjuna Security is an essential prerequisite to maximizing your organization's success.

It is vital that you agree on the means of measuring the effectiveness of NIST implementation. Overall effectiveness depends on your organization's goals and approach to its use.

Although you will want to develop quantitative metrics to accurately measure effectiveness, NIST itself does not provide specific recommendations. By using Anjuna Security, however, you can build measures into your development process to ensure you are secure from the first time you deploy.

Finally, stay committed. It can be easy to consider moving on from the NIST Framework if you aren't quickly seeing the expected results. We encourage you to stick with it—even if you face resistance from key stakeholders. By continuing to measure your progress, you will inevitably see positive results.

Learning more about the NIST Framework

The NIST Framework and Anjuna Security can be the ideal solution that enables your organization to minimize its cybersecurity risk. To learn more about the NIST Framework, visit its website by clicking here. Using this quick guide and resources on the NIST website you can take control of your environment and gain peace of mind by quickly securing your organization.

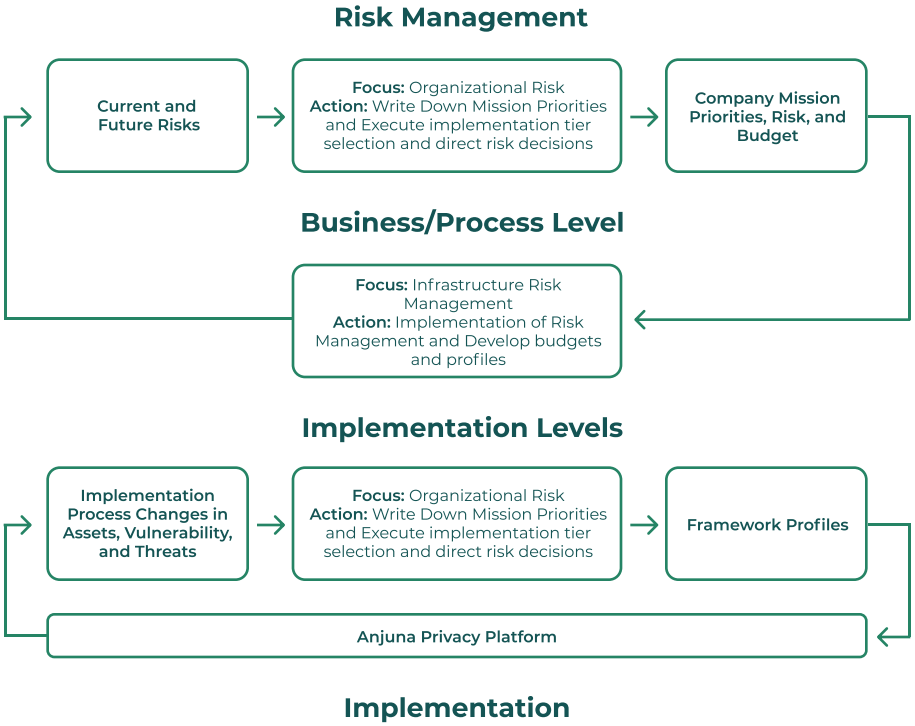
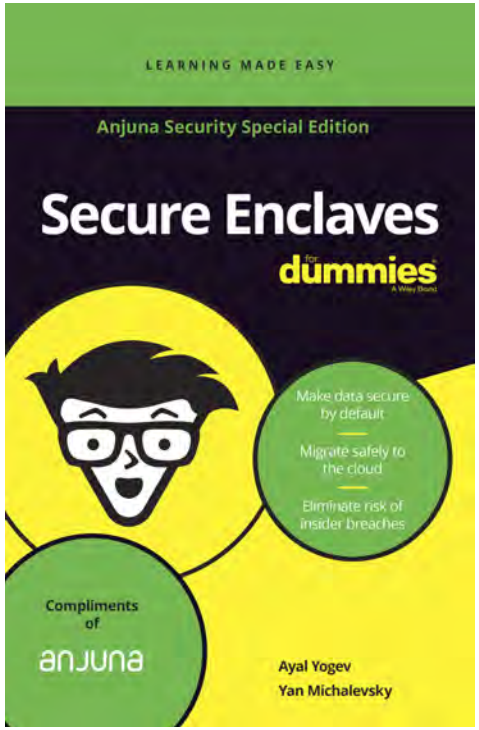


Figure 6: The NIST Framework seeks to ensure agility and security throught all levels of the organization.



Anjuna Security Resources for Everyday People

At Anjuna Security we focus on educating you about the importance of building security by default. Our founders have written a complimentary eBook about Secure Enclaves.

Find out how you can design a path to a secure cloud migration and eliminate the risk of an insider breach within your environment.

Click here to read Secure Enclaves for Dummies.

About Anjuna

Anjuna Security makes the public cloud secure for business. Software from Anjuna Security effortlessly enables enterprises to safely run even their most sensitive workloads in the public cloud. Unlike complex perimeter security solutions easily breached by insiders and malicious code, Anjuna leverages the strongest hardware-based secure computing technologies available to make the public cloud the safest computing resource available anywhere.

anjuna.io | info@anjuna.io | 650-501-0240