**NON-FUNCTIONAL REQUIREMENT** (NFR) specifies the quality attribute of a software system. They judge the software system based on Responsiveness, Usability, Security, Portability and other non-functional standards that are critical to the success of the software system. Example of nonfunctional requirement, *“how fast does the website load?”* Failing to meet non-functional requirements can result in systems that fail to satisfy user needs.

Non-functional Requirements allows you to impose constraints or restrictions on the design of the system across the various agile backlogs. Example, the site should load in 3 seconds when the number of simultaneous users are > 10000. Description of non-functional requirements is just as critical as a functional requirement.

Types:

* Usability requirement
* Serviceability requirement
* Manageability requirement
* Recoverability requirement
* Security requirement
* Data Integrity requirement
* Capacity requirement
* Availability requirement
* Scalability requirement
* Interoperability requirement
* Reliability requirement
* Maintainability requirement
* Regulatory requirement
* Environmental requirement

Eg.

1. Users must change the initially assigned login password immediately after the first successful login. Moreover, the initial should never be reused.
2. Employees never allowed to update their salary information. Such attempt should be reported to the security administrator.
3. Every unsuccessful attempt by a user to access an item of data shall be recorded on an audit trail.
4. A website should be capable enough to handle 20 million users with affecting its performance
5. The software should be portable. So moving from one OS to other OS does not create any problem.

| **Parameters** | **Functional Requirement** | **Non-Functional Requirement** |
| --- | --- | --- |
| What is it? | Verb | Attributes |
| Requirement | It is mandatory | It is non-mandatory |
| Capturing type | It is captured in use case. | It is captured as a quality attribute. |
| End-result | Product feature | Product properties |
| Capturing | Easy to capture | Hard to capture |
| Objective | Helps you verify the functionality of the software. | Helps you to verify the performance of the software. |
| Area of focus | Focus on user requirement | Concentrates on the user's expectation. |
| Documentation | Describe what the product does | Describes how the product works |
| Type of Testing | Functional Testing like System, Integration, End to End, API testing, etc. | Non-Functional Testing like Performance, Stress, Usability, Security testing, etc. |
| Test Execution | Test Execution is done before non-functional testing. | After the functional testing |
| Product Info | Product Features | Product Properties |

1. Privacy of information, the export of restricted technologies, intellectual property rights, etc. should be audited.

## Advantages of Non-Functional Requirement

Benefits/pros of Non-functional testing are:

* The nonfunctional requirements ensure the software system follow legal and compliance rules.
* They ensure the reliability, availability, and performance of the software system
* They ensure good user experience and ease of operating the software.
* They help in formulating security policy of the software system.

**Security**

Fundamentally, our society is more technologically reliant than ever before and there is no sign that this trend will slow. Personal data that could result in identity theft is now posted to the public on our social media accounts. Sensitive information like social security numbers, credit card information and bank account details are now stored in cloud storage services like Dropbox or Google Drive.

The fact of the matter is whether you are an individual, small business or large multinational, you rely on computer systems every day. Pair this with the rise in cloud services, poor cloud service security, smartphones and the Internet of Things (IoT) and we have a myriad of cybersecurity threats that didn't exist a few decades ago. We need to understand the difference between cybersecurity and information security, even though the skillsets are becoming more similar.

Governments around the world are bringing more attention to cybercrimes. GDPR is a great example. It has increased the reputational damage of data breaches by forcing all organizations that operate in the EU to:

* Communicate data breaches
* Appoint a data-protection officer
* Require user consent to process information
* Anonymize data for privacy

The trend towards public disclosure is not limited to Europe. While there are no national laws overseeing data breach disclosure in the United States, there are data breach laws in all 50 states. Commonalities include:

* The requirement to notify those affect as soon as possible
* Let the government know as soon as possible
* Pay some sort of fine

California was the first state to regulate data breach disclosures in 2003, requiring persons or businesses to notify those affected "without reasonable delay" and "immediately following discovery". Victims can sue for up to $750 and companies can be fined up to $7,500 per victim.

This has driven standards boards like the National Institute of Standards and Technology (NIST) to release frameworks to help organizations understand their security risks, improve cybersecurity measures and prevent cyber attacks.

Why is cybercrime increasing?

Information theft is the most expensive and fastest growing segment of cybercrime. Largely driven by the increasing exposure of identity information to the web via cloud services. But it is not the only target. Industrial controls that manage power grids and other infrastructure can be disrupted or destroyed. And identity theft isn't the only goal, cyber attacks may aim to compromise data integrity (destroy or change data) to breed distrust in an organization or government.

Cybercriminals are becoming more sophisticated, changing what they target, how they affect organizations and their methods of attack for different security systems.

Data breaches can involve financial information like credit card numbers or bank account details, protected health information (PHI), personally identifiable information (PII), trade secrets, intellectual property and other targets of industrial espionage. Other terms for data breaches include unintentional information disclosure, data leak, cloud leak, information leakage or a data spill.

Other factors driving the growth in cybercrime include:

* The distributed nature of the Internet
* The ability for cybercriminals to attack targets outside their jurisdiction making policing extremely difficult
* Increasing profitability and ease of commerce on the dark web
* The proliferation of mobile devices and the Internet of Things.

## What is the impact of cybercrime?

A lack of focus on cybersecurity can damage your business in range of ways including:

* **Economic costs:**Theft of intellectual property, corporate information, disruption in trading and the cost of repairing damaged systems
* **Reputational costs:**Loss of consumer trust, loss of current and future customers to competitors and poor media coverage
* **Regulatory costs:**GDPR and other data breach laws mean that your organization could suffer from regulatory fines or sanctions as a result of cybercrimes

All businesses, regardless of the size, must ensure all staff understand cybersecurity threats and how to mitigate them. This should include regular training and a framework to work with to that aims to reduce the risk of data leaks or data breaches.

Given the nature of cybercrime and how difficult it can be to detect, it is difficult to understand the direct and indirect costs of many security breaches. This doesn't mean the reputational damage of even a small data breach or other security event is not large. If anything, consumers expect increasingly sophisticated cybersecurity measures as time goes on.

## Examples of damages to companies affected by cyber attacks and data breaches

The amount of cyber attacks and data breaches in the recent years is staggering and it's easy to produce a laundry list of companies who are household names that have been affected.

Here's a few examples:

* **Equifax:**The Equifax cybercrime identity theft event affected approximately 145.5 million U.S. consumers along with 400,000-44 million British residents and 19,000 Canadian residents. Equifax shares dropped 13% in early trading the day after the breach and numerous lawsuits were filed against Equifax as a result of the breach. Not to mention the reputational damage that Equifax suffered. On July 22 2019, Equifax agreed to a settlement with the FTC which included a $300 million fund for victim compensation, $175m for states and territories in the agreement and $100 million in fines.
* **eBay:**Between February and March 2014, eBay was the victim of a breach of encrypted passwords, which resulted in asking all of its 145 million users to reset their password. Attackers used a small set of employee credentials to access this trove of user data. The stolen information included encrypted passwords and other personal information, including names, e-mail addresses, physical addresses, phone numbers and dates of birth. The breach was disclosed in May 2014, after a month-long investigation by eBay.
* **Adult Friend Finder:**In October 2016, hackers collected 20 years of data on six databases that included names, email addresses and passwords for The FriendFinder Network. The FriendFinder Network includes websites like Adult Friend Finder, Penthouse.com, Cams.com, iCams.com and Stripshow.com. Most of the passwords were protected only by the weak SHA-1 hashing algorithm, which meant that 99% of them had been cracked by the time LeakedSource.com published its analysis of the entire data set on November 14.
* **Yahoo:**Yahoo disclosed that a breach in August 2013 by a group of hackers had compromised 1 billion accounts. In this instance, security questions and answers were also compromised, increasing the risk of identity theft. The breach was first reported by Yahoo on December 14, 2016, and forced all affected users to change passwords, and to reenter any unencrypted security questions and answers to make them encrypted in the future. However, by October of 2017, Yahoo changed the estimate to 3 billion user accounts. An investigation revealed that users' passwords in clear text, payment card data and bank information were not stolen. Nonetheless, this remains one of the largest data breaches of this type in history.

# **Authentication and Authorization**

While often used interchangeably, authentication and authorization represent fundamentally different functions. In this article, we compare and contrast the two to show how they protect applications in complementary ways.

In simple terms, authentication is the process of verifying who a user is, while authorization is the process of verifying what they have access to.

Comparing these processes to a real-world example, when you go through security in an airport, you show your ID to authenticate your identity. Then, when you arrive at the gate, you present your boarding pass to the flight attendant, so they can authorize you to board your flight and allow access to the plane.

Here's a quick overview of the differences between authentication and authorization:

|  |  |
| --- | --- |
| Authentication | Authorization |
| Determines whether users are who they claim to be | Determines what users can and cannot access |
| Challenges the user to validate credentials (for example, through passwords, answers to security questions, or facial recognition) | Verifies whether access is allowed through policies and rules |
| Usually done before authorization | Usually done after successful authentication |
| Generally, transmits info through an ID Token | Generally, transmits info through an Access Token |
| Example: Employees in a company are required to authenticate through the network before accessing their company email | Example: After an employee successfully authenticates, the system determines what information the employees are allowed to access |

In short, access to a resource is protected by both authentication and authorization. If you can't prove your identity, you won't be allowed into a resource. And even if you can prove your identity, if you are not authorized for that resource, you will still be denied access.

### 1. Start With Security - Limit Scope

Factor security into every department of your business, including human resources, sales, accounting IT, etc. Start by limiting scope and securely disposing of personal information that your company doesn’t need to operate. For example, storing data after an online transaction is completed is unnecessary and leaves you at greater risk of losing sensitive customer data.

### 2. Train Employees on Security

General information security awareness programs for employees should include basic training on social engineering, which can convince users to unknowingly hand over sensitive information, like passwords, to criminals.

Training your users on how to spot a phishing email that appears to be sent from a trusted source or how to spot a spoofed website that has a slightly altered domain name can reduce your organization’s risk of a data breach.

### 3. Inventory Devices and Eliminate Exposure to External Networks

Any industry has certain devices that contain sensitive information that shouldn’t be connected to and exposed to external networks. Start by making a list of your hardware, software, data, apps, etc. that contain or may provide access to sensitive data, then determine which should be isolated.

For example, the manufacturing and critical infrastructure sector has industrial control systems that are used to control equipment and machines that shouldn’t ever be connected to the Internet, even through another network, as they can be compromised by a malicious hacker.

### 4. Encrypt Sensitive Data

The FTC recommends encrypting sensitive stored data and in-transit data using methods like TLS/SSL (Transport Layer Security/Secure Sockets Layer) encryption, data-at-rest encryption or an iterative cryptographic hash.

Mapping your encryption strategy to ensure data is secured at all stages, as it’s sent to servers and locations, can help your organization close security gaps. Ensure proper encryption configuration, since improper configuration can make apps vulnerable to attacks.

### 5. Use Secure Remote Access Methods

It should be standard for users to access networks remotely via a Virtual Private Network (VPN) that allows users to securely send and receive data over the Internet. But further securing VPN logins with two-factor authentication should also be standard, as credentials are easily stolen or guessed.

Two-factor authentication requires another method to verify your identity, after using a password. Using a mobile authenticator app, a user can securely log into their VPN by approving a push notification.

Devices that connect to networks remotely via VPN must also be updated to the latest software versions in order to reduce the risk of vulnerabilities and malware that can be introduced to corporate networks. Endpoint security solutions with device insight, analysis and remediation can identify outdated devices and help administrators quickly update them.

### 6. Strong, Non-Default Passwords…Plus 2FA

It should go without saying but isn’t always the case, especially in large organizations with many moving parts and different account owners - use unique, strong passwords for each account, and always change the default password on any login. Password managers can help you generate new passwords every login, or remember them for you.

Establish and enforce password change policies (number and type of characters, number of days to change them, stricter policies for admins, etc.). Malicious hackers use brute force attacks that attempt millions of character combinations to guess your password, often cracking weak ones in a matter of minutes.

And of course, using two-factor authentication in conjunction with a strong, unique password is essential for complete access security. Enable a solution that allows you to set a lockout and fraud policy, which locks a user out after too many unsuccessful login attempts and notifies admins of fraud, guarding against potential brute force attacks.

### 7. Enact the Principle of Least Privilege

Role-based access control limits the amount of permissions or access to certain network resources and data based on job function. The idea of least privilege is that a user only has the bare minimum needed to complete their job. This can reduce risks associated with stolen passwords, as a malicious hacker has a smaller chance of getting access to everything.

For example, contractors do not need access to systems that contain credit cardholder data in order to log their hours for billing. Separate and limit access to either account.

Limiting access can be easier with the ability to set custom security policies and controls, such as those that block login attempts from certain IP addresses, locations, anonymous networks and more.

### 8. Implement Network Segmentation

By classifying sensitive data and related IT assets/systems, and then restricting access to these systems, you can achieve network segmentation. The principle is, the compromise of one system shouldn’t easily lead the compromise of another, protecting against lateral movement if a malicious hacker should gain entry.

Separating different systems can work for security solutions too. For example, a more secure authentication setup should involve one primary authentication method sent over one channel (username and password sent over Internet), and a secondary authentication method/channel (push notification sent over mobile authenticator app).

If a remote attacker taps into your Internet connection, then they can easily steal your password, and your second form of authentication - if delivered over the same channel. Learn more about out-of-band authentication.

### 9. Keep System Logs

Logging the activity of systems can help security auditors and investigators find the source of any issues. Monitoring network traffic allows organizations to pinpoint any anomalous behavior, even that of authorized users, to identify a potential compromise of a user’s account.

### 10. Update Software to Avoid Vulnerability Exposure

Get a patch management system in place and maintain awareness of new vulnerabilities, which can quite literally pop up nearly every day. Adobe Flash releases notifications very often, sometimes even off-schedule from the typical Patch Tuesday to address critical vulnerabilities being exploited in the wild.

### 11. Implement the following web security suggestions

* Implement HTTPS and redirect all HTTP traffic to HTTPS.
* Help prevent cross-site scripting attacks by implementing the x-xss-protection security header.
* This goes without saying, use **strong passwords** that employ a combination of lowercase and uppercase letters, numbers, special symbols, etc. Use a program such as KeyPass to generate and store strong passwords.

OWASP stands for the Open Web Application Security Project, an online community that produces articles, methodologies, documentation, tools, and technologies in the field of web application security.

### The Top 10 OWASP vulnerabilities in 2020 are:

* Injection
* Broken Authentication
* Sensitive Data Exposure
* XML External Entities (XXE)
* Broken Access control
* Security misconfigurations
* Cross Site Scripting (XSS)
* Insecure Deserialization
* Using Components with known vulnerabilities
* Insufficient logging and monitoring