Contents

1. Tasks and input parameters

You have asked to evaluate a website for one of the following companies. The company is an Insurance institution with 600 employees working in 6 departments

a. Loans, Mortgages, ATM, Foreign exchange, HR, Cybersecurity &IT
b. Has 30,000 customers, 10 branches.
c. Has Mitsubishi 300 PLC controllers and 50 Siemens controllers. The company's PLCs have the following age distribution: 33% under two years, 33% from 2 to 5 years and 33% over 5 years.

The company has a large web presence and would like to develop a new state of the art secure Website.
You have been asked to evaluate the following Web Server technologies areas for the new site.

1. Evaluate and compare web server technologies (commercial and open source)
    a. Authentication
    b. OS security
    c. Scripting features
    d. Response to availability attacks

2. Which Database technology would be the most secure for the needs? Review at least two suitable Database technologies.
    a. Injection attack protection
    b. Scripting attack
    c. Privilege escalation.
    d. Backup exposure

3. Evaluate the security vulnerabilities for the company's Operational Technology equipment.
    a. What the OT security vulnerabilities exist for their equipment
    b. Detail how would you test this security of this equipment?
    c. Discuss 4 areas of OT security that would be impacted by this?
    d. Describe the application of a suitable framework and standards. Prioritise 3 main areas and describe why you have selected those.

4. Data requirements
    a. What regulatory requirements are important for your specific sector?
    b. Clearly outline a plan for meeting the regulatory and data protection requirements.
    c. Outline which OWASP top 10 vulnerabilities which apply to your context. Rank the vulnerabilities according to your data, users and context.

2. Evaluating and comparing web server technology

2.1 Introduction

For any company, having an efficient and secure website is crucial, as it determines the attitude of customers to the company and builds its credibility. Therefore, the choice of web server technology cannot be underestimated.

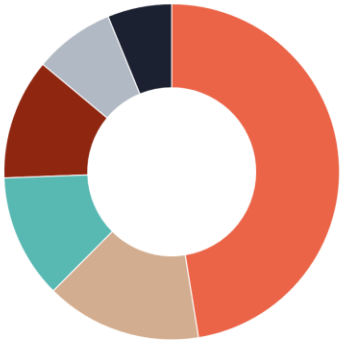
A web server is a component that provides static data, for example, a file, text, or image. These elements are returned as a reply to a request to the server. The application server, meanwhile, adds the context of business logic in order to compute responses for the web server.The principle of a web server can be described in the following steps: A web server stores the code and data of a website, which in turn responds to visitor requests. When a URL is entered, the user's browser performs the following actions:

- Identifies the IP address of the web server.
- It sends an HTTP query for data.
- The server gets the relevant data, often from a database.
- Sends the static content back to the browser.
- The browser then displays the content.

Web servers process static websites, but interactive websites often require an application server.The application server serves the role of increasing the capabilities of the web server by providing dynamic content, it executes application logic as well as business logic to deliver more meaningful data. It can also integrate with other systems. ('Web Server vs Application Server - Difference Between Technology Servers - AWS' 2025)

2.2 Quantitative evaluation of the web server technologies market

According to the data provided by the American company 6sense ('Best Web And Application Servers Software in 2025' 2025), as of 2025, there are more than 9 million companies in the world using Web And Application Servers. The current market situation is characterized by an uneven distribution of technologies, as there are more than a hundred different variants of server solutions, while only a couple of them are the most popular. The key solutions that are widely used are Nginx with a market share of 47 percent, LiteSpeed Web Server with 15 percent, and Apache and Apache HTTP Server with 12 and 11.6 percent. There are also some companies that use a Microsoft solution called IIS, which takes up about 8% of the market. A visualization of the market distribution is shown in Figure 1.



Technology	Market Share (Est.)	Customers
Nginx	47.44%	4,437,620
LiteSpeed Web Server	15.02%	1,404,993
Apache	11.95%	1,118,221
Apache HTTP Server	11.63%	1,088,064
Microsoft IIS	7.75%	725,193
Others	6.20%	580,094

Figure 1 Distribution of the server technology market ('Best Web And Application Servers Software in 2025' 2025)

Therefore, based on the above market analytics, it is reasonable to compare the most common and highly competitive solutions from a technical perspective. Analyzing them, it is possible to understand which solution is most suitable for the insurance company.

2.3 Technical evaluation

This section compares Nginx and Apache technologies and the solutions they provide. The comparison covers key areas such as authentication, OS security, scripting features, and potential response to availability attacks. Such characteristics are extremely important for the insurance business, hence the company's website is the first impression that customers get. Therefore, if the site is not working well, is unreliable, and has obvious problems, it can become a potential loss of customers for the insurance company at the very first stage.

2.3.1 Authentication

Authentication is a mechanism designed to control visitors to a web resource. Usually, this is performed by providing unique data such as a password and username and then accessing the resource using this data (Rick-Anderson 2022).

- Nginx provides authentication via HTTP Basic Authentication, OAuth, and also OpenID Connect. OAuth is a standard that provides for the use of one application or service to use another without additional user credentials, such as a password and login (‘What Is OAuth? | Microsoft Security’ 2025). There is also integration with external authentication servers. In practice, it is often used in combination with modules such as the Nginx Auth Request Module to get additional authentication features (‘NGINX Documentation’ 2025). It is worth noting that the company claims that basic authentication is convenient, but not as secure as other methods because the credentials will be sent as Base64 encoded text, which is not a strong encryption method. Therefore, it is recommended to consider switching to OpenID Connect (OIDC) for authentication. For production systems, the company recommends using OIDC(‘Set up basic authentication | NGINX Documentation’ 2025).
- The Apache server provides the following authentication options - basic authentication, Kerberos authentication, and Digest. Modules such as mod_authz_core, mod_auth_basic, and mod_auth_digest have been developed to improve authentication control.Among the supported mechanisms, it is also worth noting database authentication, in particular MySQL and PostgreSQL, as well as LDAP authentication that integrates with directory services (‘mod_authnz_ldap - Apache HTTP Server Version 2.4’ 2025).

It can be stated that Apache offers more built-in authentication modules, while Nginx provides a more flexible approach when integrating with external authentication providers. Therefore, these options should be taken into account at the stage of developing the design of the future website.

2.3.2 OS security

- Apache uses the process-driven model, creating multiple processes or threads to perform requests. Security modules include mod_security, which directly acts as a web application firewall (WAF), which is necessary to protect the system from existing threats (‘Apache Hardened Web Server - Documentation’ 2025) . The configuration provides for a very flexible and detailed configuration of security, although there is a risk of management difficulties, which creates high demands on staff. In general, it can be said that Apache is already a very well-tested solution if there is sufficient expertise to configure it (‘Security Tips - Apache HTTP Server Version 2.4’ 2025).
- Among the key points of Nginx in terms of OS security are the architecture that considers events as key points, and it also asynchronously handles requests, reducing resource usage and potential attack vectors. It is also worth noting the simplified configuration, as well as third-party security modules such as ModSecurity for WAF functions. Nginx's architecture lowers the surface area for attacks, and its simple structure helps maintain a secured environment (‘Inside NGINX: How We Designed for Performance & Scale – NGINX Community Blog’ 2015).

2.3.3. Scripting features

- Apache provides scripting features, including the following languages PHP (mod_php), Perl (mod_perl)(‘mod_perl: User’s guide’ 2025), and Python (mod_python) (‘PHP: Apache 2.x on Unix systems - Manual’ 2025). Since the scripts are already built into the server, it can simplify development and deployment, but it is worth noting that integrated modules can theoretically use more server resources, which is especially noticeable under heavy load.
- Nginx doesn't have its own built-in support for content processing, and thus it requires the use of FastCGI, uWSGI, or a backend application proxy (‘Module ngx_http_fastcgi_module’ 2025). This means that scripts are processed externally and can increase efficiency and scalability (‘Understanding and Implementing FastCGI Proxying in Nginx | DigitalOcean’ 2025).

Apache is more convenient for developers to write scripts, while Nginx requires additional settings for dynamic content.

Therefore, it can be assumed that Apache is a more convenient solution for developers, but at the same time it may be less efficient under heavy loads. At the same time, Nginx's approach may be more efficient, and this aspect should be taken into account from a security perspective.

2.3.4 Response to availability attacks

Availability is one of the key parameters of the CIA triad, so attacks directed against this parameter can have a significant impact on the evaluation of server cybersecurity (‘What is the CIA Triad and Why is it important?’ 2025).

- The Apache server can be potentially vulnerable to HTTP attacks and high connection load due to the aspects described in the previous sections, in particular, thread-based processing makes the server vulnerable to DDos attacks (‘Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project’ 2025). To mitigate this risk, the mod_evasive module can be used to dynamically block IP addresses. Mod_reqtimeout and mod_qos are also used (Muscat 2019). The Apache server architecture requires detailed configuration to effectively protect against denial of service attacks.
- Unlike Apache, Nginx is quite effective in handling large volumes of traffic due to its relatively lightweight, event-driven architecture. Protection against DDoS attacks can be implemented by slowing down the speed, limiting connections or requests (‘Mitigating DDoS Attacks with NGINX – NGINX Community Blog’ 2015). Therefore, considering this type of attack, Nginx can potentially be a more resilient solution.

2.3.5. Comparative table

Table 1 summarizes the main key points in comparing the two technologies.

Feature	Nginx	Apache
Authentication	Support for OpenID, OAuth, and external authentication	Availability of built-in authentication modules: Basic, Digest, Kerberos
OS security	Event-driven Single-threaded. Simplified configuration	Multi-process threaded model Needs extra security modules Complex configuration
Scripting features	Needs FastCGI, uWSGI or an external application server Higher efficiency and scalability	Native support for PHP, Perl, Python using built-in modules

Response to availability attacks	Processing high traffic with a speed limit and connection restriction, request queue. More resistant to DDos attacks.	Needs mod_evasive and other configurations for optimal DDoS protection Vulnerable to resource exhaustion

Table 1 Comparative table - Nginx vs Apache

To summarize the comparison, it can be concluded that for an insurance company, Nginx may be a better choice due to higher protection against DoS attacks that can potentially be performed by the company's competitors to intercept customers and show the unreliability of the business. The insurance company is characterized by high credibility and customer trust, so constant availability is very important. Nginx also supports OpenID and OAuth authentication and generally meets the business task.

3 Overview and comparison of database technologies

A database is an organized collection of structured information or data that is stored in electronic form in a computer system. This database is usually managed by a database management system (DBMS) (‘What Is a Database?’ 2025).
The most common database technologies as of 2025 are Oracle, My SQL, PostgreSQL, and Microsoft SQL Server. Let's consider Oracle as the most popular database in the corporate sector, especially enterprise-level. PostgreSQL will be used as a comparison, as it is one of the most popular databases among developers and is also much more affordable for companies (Koshy 2022). Databases will be analyzed from the perspective of cybersecurity, in particular, on the following points: Injection attack protection, scripting attack, privilege escalation, backup exposure.

3.1 Injection attack protection

- Oracle recommends using variable binding and prepared statements to prevent SQL injections by separating code from data (‘Preventing SQL Injection’ 2025).Constant validation checks, in particular, with the help of a subprogram from the DBMS_ASSERT package (Alpern *et al.* 2025). Oracle Database Firewall offers real-time, proactive protection by tracking and blocking SQL injection attacks (‘SQL Firewall now built into Oracle Database 23ai’ 2025).
- PostgreSQL allows tracking key user roles by using sqlprotect.sql (Carter 2011). The DB also provides input shielding functions, such as functions such as quote_literal() or quote_ident(), which exist to securely process user input (‘9.4. String Functions and Operators’ 2025). There are no integrated firewall functions, so the responsibility is on technical executives to implement best practices. Also the way to protect PostgreSQL is through external security products such as EnterpriseDB's SQL/Protect firewall, which automatically detects injection attempts. This firewall further protects the server, and administrators can control the performance using database commands.

3.2 Scripting attack

Cross-site scripting, also known as XSS, is a type of vulnerability that is caused by the specifics of dynamically generated web pages. During such attacks, a script is sent to a web application that is activated when the user interacts with the browser, after which such scripts can steal data, including session credentials. This information can be further used for the purposes of the attacker (Allen *et al.* 2025).

- Oracle uses its own procedural language called PL/SQL. From the cybersecurity point of view, a significant advantage is the reduction of the risk of SQL injection by using bind variables and procedural logic. Another important factor is that the code can be wrapped (obfuscated) using Oracle's wrap utility to prevent unauthorized access or code substitution (‘Database PL/SQL User’s Guide and Reference’ 2025). Techniques such as Output Encoding and Input Validation are also used. Oracle also has a Database Vault feature that denies unauthorized access considering the security policies(‘Database Vault Administrator’s Guide’ 2025).
- PostgreSQL provides support for the following procedural languages (PL/pgSQL, PL/Perl, etc.), which can restrict the execution of arbitrary scripts and therefore might serve as a security function (‘Chapter 40. Procedural Languages’ 2025). Recommendations for using the privileges of the SECURITY DEFINER function. Because some functions can also be run with owner privileges, which can pose a security risk if used improperly (‘CREATE FUNCTION’ 2025).

In general, when comparing the 2 database technologies in this section, PostgreSQL may potentially be a more vulnerable technology due to the lack of functions for wrapping.

3.3 Privilege escalation

A privilege escalation attack is a form of cyberattack intended to gain unauthorized privileged access to a system. To do this, threat actor exploits human error, design flaws, or vulnerabilities in operating systems or Web apps. The tactic is closely connected to lateral movement when cybercriminals penetrate into the network to find and get access to valuable assets (‘What is Privilege Escalation? | CrowdStrike’ 2025).

- Oracle provides access control based on role-based access control, i.e. RBAC system. In this system, user privileges are determined by the user's role (‘Role-Based Access Control (Overview) - Oracle Solaris 11.1 Administration: Security Services’ 2025). Oracle Solaris Kernel has been designed to prevent privilege escalation, which occurs when a process is granted more permissions than it should have. In order to minimize this risk, all system modifications that could lead to possible vulnerabilities require full privileges. For example, only a process with full privileges can modify files or processes owned by the root user (UID=0). At the same time, the root user can modify his own files without additional privileges, and a non-root user must have full privileges to make changes to files owned by user_root (‘Prevention of Privilege Escalation - System Administration Guide: Security Services’ 2025). The Virtual Private Database (VPD) option enables security policies to be applied at the row level (‘Database Security Guide’ 2025).
- Postgresql supports the option of row-level security or RLS. It provides restricted access to data based on user attributes. Enabling and disabling row security, as well as adding a policy to a table, is the sole privilege of the table owner (‘5.9. Row Security Policies’ 2025).There is also a sepgsql option that supports mandatory label-based access control (MAC) that works according to SELinux policies. It can be assumed that this option may be useful in architectures that use a Linux environment, but not for Windows (‘F.38. sepgsql — SELinux-, label-based mandatory access control (MAC) security module’ 2025).

It is worth noting that PostgreSQL has some existing vulnerabilities to this type of threat, in particular, CVE-2020-25695 indicates a serious vulnerability in PostgreSQL versions include 10 through 14 (‘NVD - cve-2020-25695’ 2025). Oracle at the same time may also have problems in particular in the Oracle Virtualbox environment - CVE-2024-21111 (‘NVD - cve-2024-21111’ 2025). Therefore, it cannot be said that both systems are perfectly resistant to attacks, but they have sufficient mechanisms to counteract them.

3.4 Backup exposure

Any data that the company stores, processes or collects must be permanently protected and additionally backed up in case of unauthorized access or loss of the primary database. In the

context of the insurance industry, this is very important because the company operates with large amounts of sensitive information, such as bank accounts, claims, personal information of users, etc. Considering the comparable database technologies in this context, the following points can be noted.

- Oracle offers a comprehensive and integrated approach to data backup, including options such as Transparent Data Encryption (TDE). This allows to encrypt sensitive data, which is present in large amounts in the insurance industry (Duraiswamy *et al.* 2025). Among the key features offered for the data backup and recovery process are the following:Recovery Manager (RMAN), Oracle Enterprise Manager Cloud Control, Zero Data Loss Recovery Appliance (Jashnani *et al.* 2025).
- PostgreSQL provides the following functionality: the use of backup types: pg_dump, WAL-archiving, PITR (Point-in-Time Recovery). This requires more manual management, relying on WAL for PITR.At the same time, it should be noted that there is no native backup encryption, meaning that it is necessary to use external tools and configure it correctly (‘Backup and Restore’ 2012).

Therefore, comparing the two technologies, it can be assumed that Oracle is better for data backup and potentially more secure, as it offers automated, encrypted backups, while PostgreSQL requires external tools for encryption.

Relying on external tools creates a potentially vulnerable point for attackers if a low-quality solution is used or configured incorrectly.

3.5 Comparative table

Based on the information provided in this section, the following comparison of the main differences between the functionalities is presented in Table 2

Feature	Oracle	PostgreSQL
Injection attack protection	Uses variable binding, prepared statements, and the DBMS_ASSERT package. Oracle Database Firewall offers real-time protection against SQL injections. Stronger integrated protection	Tracking the main user roles with sqlprotect.sql Using functions like quote_literal() and quote_ident() to process input data securely. Lack of an integrated firewall, dependence on third-party tools
Scripting attack	Using PL/SQL, variable binding, and output encoding to prevent XSS Database Vault blocks unauthorized access	Supports PL/pgSQL and other languages, but does not have wrapping/obfuscation features

Privilege escalation	Role-based access control (RBAC) and the Solaris kernel protect against unauthorized privilege changes A virtual private database (VPD) uses security policies at the row level	Support for Row-Level Security (RLS) and SELinux-based security options such as sepgsql RLS controls access to data based on user attributes
Backup exposure	Transparent data encryption (TDE), RMAN, and automatic recovery Integrated and encrypted backup solutions reduce the risk of data breaches Complex backup tools such as RMAN and Zero Data Loss Recovery Appliance	It must be configured manually for backup types (pg_dump, WAL) and PITR No built-in encryption, external tools are required to protect backups Possible risk of exposure caused by using external tools to encrypt backup

Table 2 Comparative table - Oracle vs PostgreSQL

In conclusion, it can be said that Oracle offers better protection in terms of cybersecurity in general, considering the most basic functionality that is available to the user without the use of third-party solutions and resources. The use of third parties and services is a potential surface for supply chain attacks -no built-in encryption in PostgreSQL. The key factor that makes the Oracle database a better solution for an insurance company is data encryption and backup. As the availability of information and its security is critical for the existence of the insurance business, especially in terms of the potential threat of ransomware attacks.

4 Assessment of security vulnerabilities for the company's operational technology equipment.

Assessment of the current operational technology equipment plays a critical role in maintaining a stable and predictable cybersecurity situation in the company. The company has 350 PLC controllers that can potentially have vulnerabilities in a range of situations. In addition, the company has a large workforce of 600 people and 6 departments, which means that a large number of physical devices such as laptops, network equipment, and IoT devices, must also be included in the security scope. Although these devices are not OT in the classical sense, if they are in the same network as controllers and other parts of OT, then these devices should also be considered through the prism of cybersecurity, as attackers can use them as entry points for an attack.

4.1 Current OT vulnerabilities

OT means Operational Technology Security, which includes technologies and practices that serve to protect the integrity, availability and security of systems involved in the management of industrial processes and critical infrastructure. OT systems include programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, and distributed

control systems (DCS). Such systems are used for the operation and safety of production facilities and various industrial sites ('What is OT Security? | IBM' 2024).
The following are the major vulnerabilities that may affect PLCs from Mitsubishi and Siemens:
1) Vulnerabilities of legacy systems
Older PLCs (more than five years old) usually do not have security updates or encryption mechanisms, making them vulnerable to known exploits.
2) Not enough secure communication protocols
PLCs that use older communication protocols (e.g., Modbus, DNP3) without encryption are vulnerable to data interception or manipulation ('Modbus, DNP3 and HART | Infosec' 2025).
3) Poor authentication: Default credentials or credentials that are not secure
4) Lack of firmware updates: A large number of outdated PLCs may not receive timely firmware updates, leaving them vulnerable to new threats and use by threat actors.
Mitsubishi controllers could potentially have one of the previously identified vulnerabilities:

- CVE-2023-6942, which is that authentication can simply be bypassed due to its absence for important functions in several Mitsubishi Electric FA engineering software products ('NVD - cve-2023-6942' 2025).
- Buffer overflow vulnerability in Mitsubishi Electric MELSEC iQ-F series PLCs CVE-2023-1424. This vulnerability could potentially lead to a buffer overflow in Mitsubishi Electric MELSEC iQ-F series PLCs, which could cause a denial of service condition or potentially remote code execution ('NVD - cve-2023-1424' 2025).
- Another example is CVE-2022-25162, which is a flaw in the input validation of Mitsubishi Electric MELSEC iQ-F series PLCs that allows attackers to cause a temporary denial of service ('NVD - CVE-2022-25162' 2025).

Siemens controllers are also not perfectly protected and have a number of vulnerabilities, in particular:

- CVE-2022-38465, which means that global private keys can be obtained in Siemens SIMATIC S7-1500 PLCs, and malware can be installed and potentially gain full control over the device ('NVD - cve-2022-38465' 2025).
- Vulnerability CVE-2021-40368 is that Siemens SIMATIC S7-400 processors do not properly process packets sent to port 102, allowing attackers to create conditions for denial of service ('NVD - cve-2021-40368' 2025).

Therefore, it can be stated that the current OT equipment of an insurance company can be potentially vulnerable to attacks by competitors or criminals. When accessing PLS equipment, controllers can be disabled in a variety of ways - physically applying the wrong voltage, injecting malicious code, creating persistent backdoors to changing transaction limits, etc.

4.2 Security testing methods

In order for the security methods to be effective, it is necessary to refer to the frameworks and standards created for this purpose, in particular in the insurance sector. Frameworks were created based on best practices and on the analysis of many incidents and relevant experience. This approach is relevant and justified for an insurance company due to the specifics of the data it uses. In this case, it is appropriate to use the NIST framework, which provides detailed processes and procedures for the efficient identification, assessment and further action on risks and threats. Considering that this is a matter of OT, it is worth referring to NIST SP 800-82 Rev. 3, which describes the context of Operational Technology (OT) Security (Stouffer *et al.* 2023).

- The first step is the assessment (identification phase). The purpose is to identify the assets, threats, vulnerabilities and potential impacts on the OT systems. It is necessary to assess the assets, threats, vulnerabilities and potential impacts on the OT systems.It is important to categorize assets by criticality (e.g., systems that control security functions). Also, it is necessary to categorize the equipment depending on its age and

the software deployed on it. It is necessary to conduct a comprehensive audit with consideration of all existing and potential risks. After categorizing the devices, it is worth considering the definition of EOL (‘End of Life of expiring products - Mitsubishi Electric Factory Automation - Germany’ 2025), which is originally end-of-life, i.e. products that are no longer supported by the manufacturer and are not intended for use. In practice, this means no support and therefore the product becomes vulnerable to potential attackers because potential vulnerabilities or CVEs (‘CVE security vulnerability database. Security vulnerabilities, exploits, references and more’ 2025) will not be fixed. There are many platforms where found and confirmed vulnerabilities of products from various manufacturers are freely available (‘CVE - CVE’ 2025). Identify any ongoing threats, such as unauthorized access, malware, or insider threats. To do this, it is possible to use such OT-compatible tools as, for instance, Tenable. ot, Nozomi Networks. An example of using such tools is shown in Figure 2.

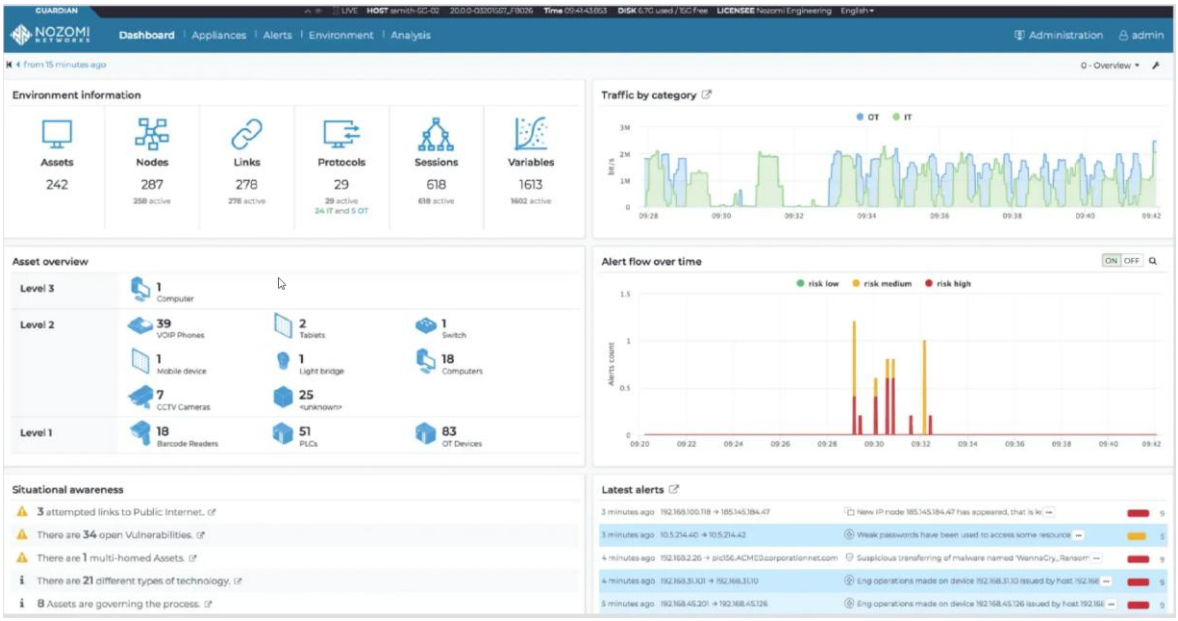


Figure 2 Example of using Nozomi to detect vulnerabilities and monitor OT equipment (‘Guardian | OT Network Monitoring’ 2025)

- The second phase is protection. This is done in order to apply security controls adapted to OT systems. It is important to implement network segmentation between the IT environment and the OT environment, since, as mentioned earlier, any end devices on a shared network can become a bridge for potential attackers to OT equipment. Strict access control (role-based access, multi-factor authentication) has to be set up. Also, it is necessary to ensure that the software is up to date. In case the equipment is no longer supported - which is quite likely for all PLCs more than 5 years old - they should be replaced or phased out. Also some solutions allow the protection of PLCs with internal logic code. In particular, such a method as Scan Time Code (STC) detects abnormal code behaviour in real-time by monitoring its execution time. Other methods include preventing device manipulation and suppressing alarms. Therefore, it can be used for testing equipment and its subsequent monitoring (‘PLC Code Vulnerabilities and Attacks: Detection and Prevention’ 2025).
- Another phase is to Protect (agains potential threats). For this purpose, systems such as intrusion detection or prevention systems (IDS/IPS) can be used, for example, Snort, Suricata with ICS signatures. It is also necessary to monitor system logs in order to detect any unusual activity, such as failed authentication attempts, or attempts to do so after working hours, etc. For this purpose, automated security information and event management (SIEM) solutions are recommended. Examples of such tools include

Splunk, Rapid 7, etc. It is worth noting that Splunk has many features that were developed specifically for the banking sector and financial transactions, which is very important in the insurance industry. In particular, thanks to a permanently tracked identifier in the logs for each transaction, company employees can monitor end-to-end flows and identify potential bottlenecks without the need for APM tools. An example is shown in Figures 3 and 4 .

username	account_number	RiskScore	total_acc_instructed_amount	total_acc_transactions	unique_ref	instructed_amount	instructed_currency	avg_delta_time_hours	tnx_above_
rmccoy52	EU10212905	27	40000-45000	4	306b3c35-5a5d-4c48-8697-bb9311a90d0b	735	EUR	92.23	
rmccoy52	EU10212905	8	40000-45000	4	c4697a8c-3ac3-8fc1-6c21-c8fe4dab6ae0	11240.6	EUR	92.23	
rmccoy52	EU10212905	41	40000-45000	4	ca0a18c8-74b4-8f66-1bfe-f1c4b7da7001	205.8	EUR	92.23	
rmccoy52	EU10212905	49	40000-45000	4	eff56dc4-6b49-61a7-35cc-6543093b62f7	31703	EUR	92.23	
efoxiv	EU10337030	8	30000-35000	4	13078953-4c4e-6361-4433-9d540c763c90	8300.6	EUR	108.22	
efoxiv	EU10337030	29	30000-35000	4	40eef5bb-044a-a36c-2fc6-9bb0537028c0	11681.6	EUR	108.22	

Figure 3 Example of using Splunk (‘40 Ways to Use Splunk in Financial Services’ n.d.)

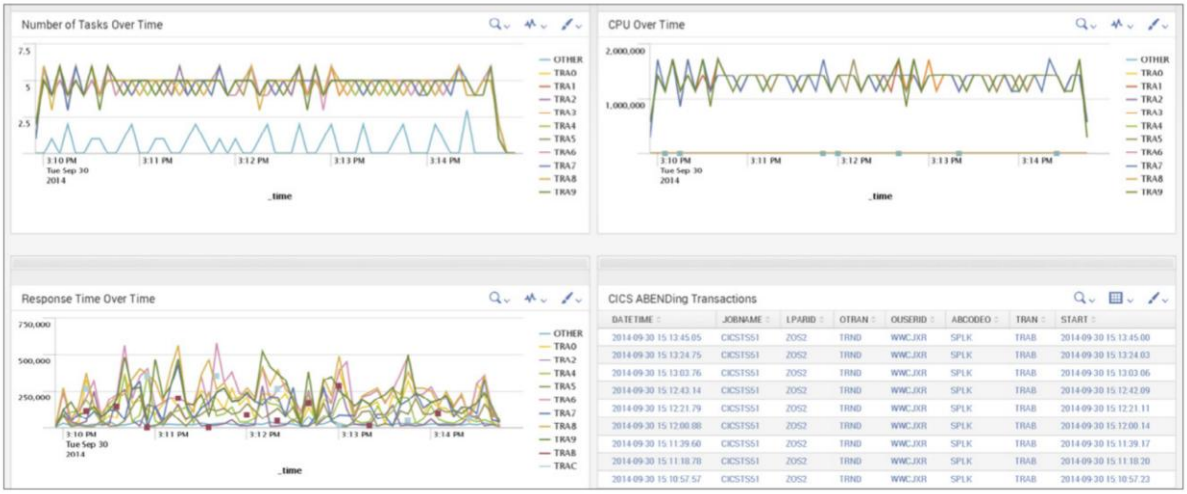


Figure 4 Example of using Splunk for monitoring traces and transactions in real-time (‘40 Ways to Use Splunk in Financial Services’ n.d.)

.

As can be seen, Splunk provides the ability to monitor various processes in real-time (Splunk Enterprise Security), which is especially important for an insurance company, in particular, transactions. The Splunk ITSI (IT Service Intelligence) feature helps to monitor insurance policies and IT infrastructure. Track Customer Information Control System (CICS) transactions and gain visualization of overall performance, and resource usage, and can be used in order to compare with previous data for trend analysis. For example, if there is an unusual

peak in transaction activity or if they occur outside of business hours, this may be an indicator of an incident. As a preventive measure and to test the strength of the system, penetration tests should also be performed. These tests can help to simulate a real attack, which will help determine whether the current security system is working well or not. In particular, such tests should focus on older equipment, in particular PLCs that are 5 years old or older, as there is a higher chance of finding public CVEs that have not been patched by the equipment manufacturer. If such equipment is found, it should be immediately reported to the management (‘What is penetration testing? | What is pen testing?’ 2025).

4.3 Areas affected by OT security

The key areas of OT security that could potentially be vulnerable include:

- Operational continuity, when any disruption to OT systems can stop critical operations and therefore end business continuity, which can critically affect the business's continuity and impact revenue or cause losses. If the company cannot respond to insurance claims of clients even for several business days, this may be a potential ground for violation of regulatory requirements.
- Security of the entire network: if OT devices are compromised, they can pose security risks to employees and customers. For example, if an attacker gains access to the equipment and overheats it due to changes in software settings, it can lead to a fire in the server room or the entire building and cause a threat to the life and health of the staff.
- Data integrity and confidentiality: if access is unauthorized, it can lead to data manipulation and loss of integrity.
- Compliance issues: problems with OT equipment and security can lead to failure to pass a regulatory audit and lead to loss of reputation and significant fines.

4.4 Application of the appropriate legal and regulatory framework and standards

Considering the organizational context of the company, the following standards and frameworks can be applied to enhance OT security:

- NIST (CSF) 2.0. In general, this framework is one of the most widely used on the market today, including in the insurance industry. The previous section (4.2 Security testing methods) described the practical application of the NIST framework with practical steps. It is worth noting that the use of this framework allows the company to potentially pass audits for compliance with regulatory standards required of insurance companies in the European Union. The main structural elements are shown in Figure 5, while a separate publication, NIST SP 800-82r3, considers directly ensuring the security of OT systems, including risk management and security control.

Figure 5 NIST CSF Functions

A security risk assessment in the context of OT can also be conducted through NIST SP 800-39. The process according to the framework is shown in Figure 6.

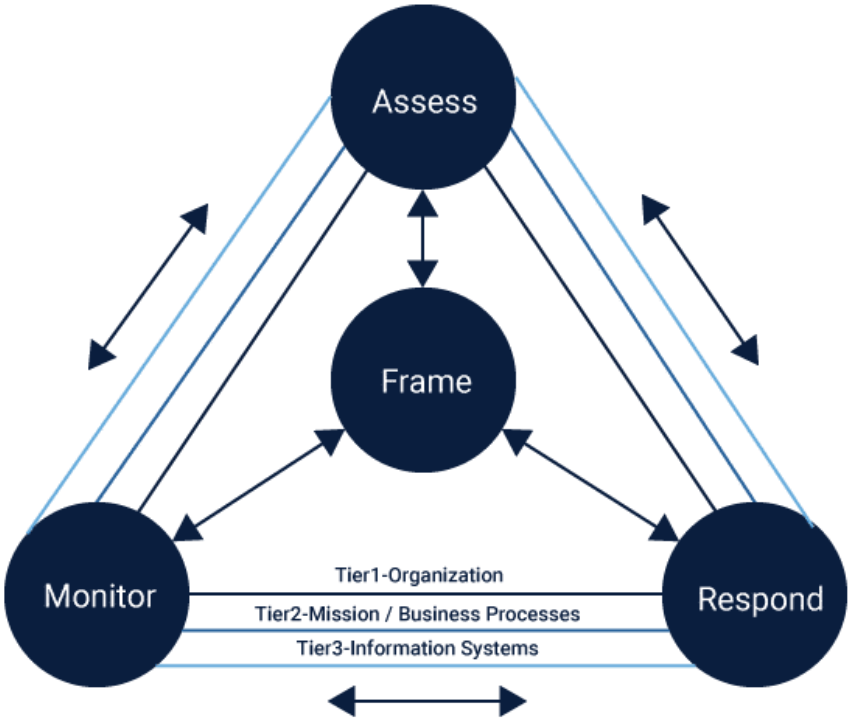


Figure 6 NIST Risk Assessment Process (Technologies 2019)

- Also important will be the application of the ISA/IEC 62443 series of standards: which were specifically designed to provide security for industrial automation and control systems, which is applied to the presented PLC equipment from Siemens and Mitsubishi. The ISA/IEC 62443 standard improves OT security by creating a cybersecurity framework. It emphasizes risk management, defense in depth, and network segmentation with zones to prevent cyberattacks ('IEC 62443 Standard: Enhancing Cybersecurity for Industrial Automation and Control Systems' 2025). Examples of standards from this series that have been applied to insurance are shown in Figure 7.

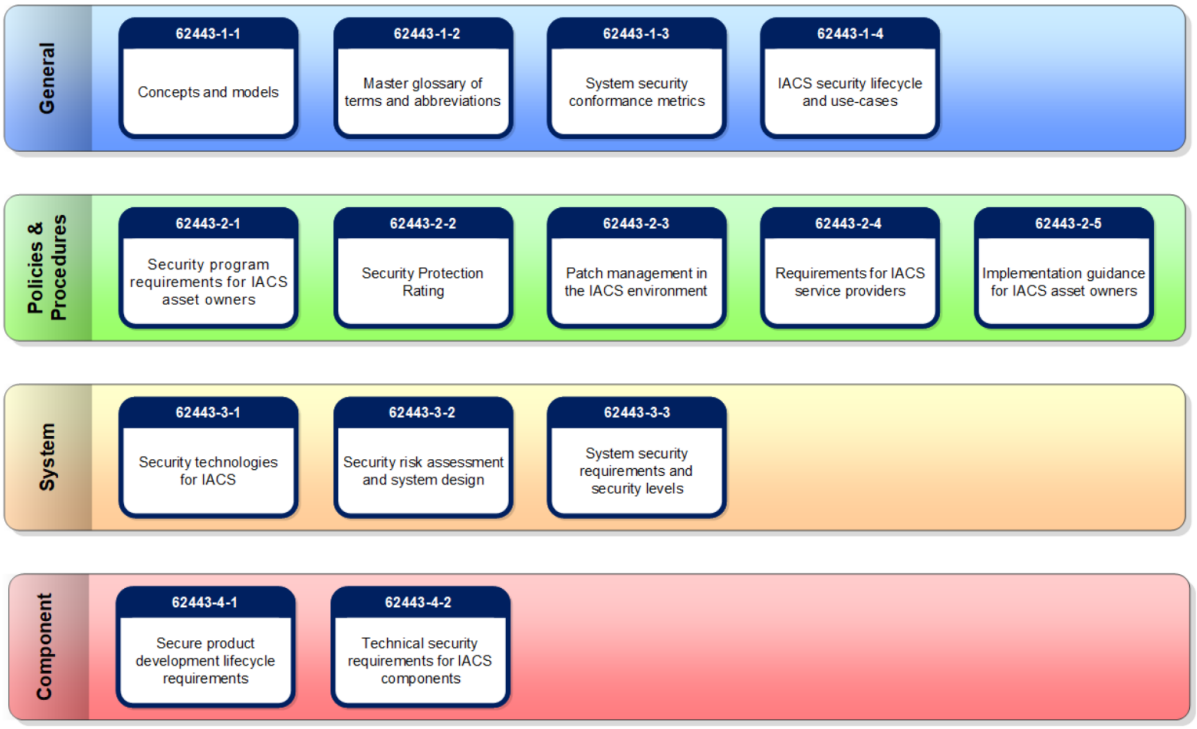


Figure 7 ISA/IEC 62443 Series of standards (Cosman 2025)

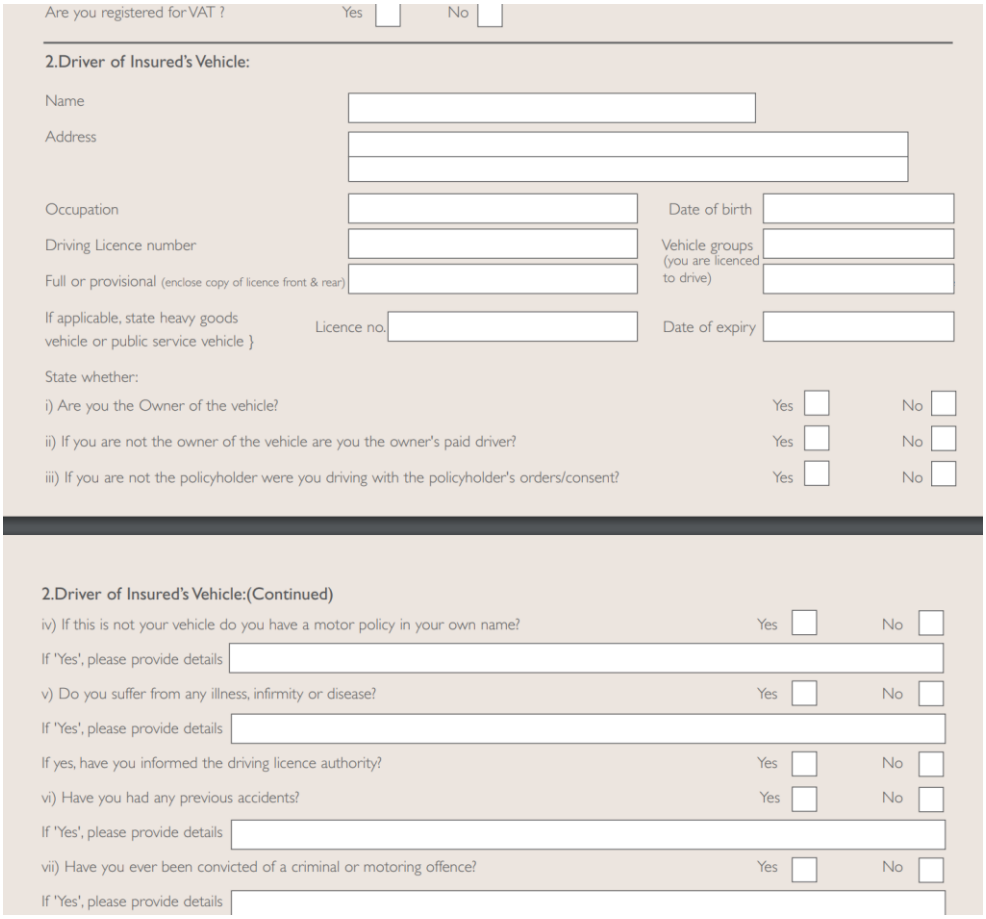
- It is also worth noting that in the case of implementing any new projects, management frameworks should also be applied to the company's business processes. One of the most versatile, which is also suitable for the insurance industry, is Prince 2 (‘What Is PRINCE2? The Definition, History & Benefits | UK’ 2025).
- One of the key standards for information security, which is also relevant to the operational environment, is ISO/IEC 27001. It focuses on risk analysis, incident management, and information security, which ensures a consistent and secure approach to information management (‘ISO/IEC 27001:2022’ 2025).

5 Data compliance. OWASP vulnerabilities.

5.1 Regulatory Requirements. PII, SPII in the insurance industry.

The insurance industry is a quite complex sector in terms of cybersecurity, especially when it comes to storing, processing and transmitting information. An insurance company interacts with a huge amount of Personally identifiable information (PII) and Sensitive PII. PII is information that is associated with a specific person and can identify them in one way or another. At the same time, sensitive personal information may include particularly sensitive data such as bank account, biometric data, passport information, etc (‘What is Personally Identifiable Information (PII)? | IBM’ 2022).

As an example of the information processed by the company, the analysis can be narrowed down to car insurance and what data is processed in Ireland. The following examples in Figures 8 and 9 show the form for filling out a car insurance claim and what information can be collected. It can be said that quite a large amount of various information is collected, which can be very useful for potential attackers.



Are you registered for VAT ? Yes No

2.Driver of Insured's Vehicle:

Name

Address

Occupation Date of birth

Driving Licence number Vehicle groups (you are licenced to drive)

Full or provisional (enclose copy of licence front & rear)

If applicable, state heavy goods vehicle or public service vehicle } Licence no. Date of expiry

State whether:

i) Are you the Owner of the vehicle? Yes No

ii) If you are not the owner of the vehicle are you the owner's paid driver? Yes No

iii) If you are not the policyholder were you driving with the policyholder's orders/consent? Yes No

2.Driver of Insured's Vehicle:(Continued)

iv) If this is not your vehicle do you have a motor policy in your own name? Yes No

If 'Yes', please provide details

v) Do you suffer from any illness, infirmity or disease? Yes No

If 'Yes', please provide details

If yes, have you informed the driving licence authority? Yes No

vi) Have you had any previous accidents? Yes No

If 'Yes', please provide details

vii) Have you ever been convicted of a criminal or motoring offence? Yes No

If 'Yes', please provide details

Figure 8 Motor Accident Form RSCLA3000 ('Motor Accident Form RSCLA3000.pdf' n.d.)

Motor Accident Report Form

THIS FORM MUST BE COMPLETED BY THE POLICYHOLDER AND/OR THE AUTHORISED DRIVER
PLEASE HELP US TO HELP YOU BY:
- MAKING SURE THE INFORMATION YOU GIVE IS AS TRUTHFUL AND ACCURATE AS POSSIBLE
- COMPLETING ALL THE RELEVANT SECTIONS OF THIS FORM
- REMEMBERING TO SIGN AND DATE THIS FORM

RSA

Claim reference

Declaration

1. I/We hereby declare that the below statement and information furnished by me/us or on my/our behalf are true and complete in every respect
2. I/We have disclosed all information in my/our possession
3. I/We am aware that it is a CRIMINAL offence to defraud, or to attempt to defraud an insurer and that should I/we do so I/we may be prosecuted
4. I/We understand that RSA may seek information from other insurance companies or industry databases to check the information that I/we have provided
5. I/We understand that RSA will pass the information on this claim (and any incident of which I/we may provide details) to Insurance Link and other industry databases where it would be available to other insurance companies
6. I/We also understand, in response to any searches related to such information provided, Insurance Link and other insurance companies may pass onto RSA information it has received about other incidents involving anyone insured under the policy.

Signature(s) (Insured) Date ___/___/____

Signature(s) (Driver if different) Date ___/___/____

If you are completing this form for information purposes only rather than submitting a formal claim under your policy please tick this box

RSA Insurance Ireland DAC records and data are kept and used in accordance with the Data Protection Act.

PLEASE COMPLETE THIS FORM USING BLOCK CAPITALS.

1. Insured:

Policy number

Name

Address

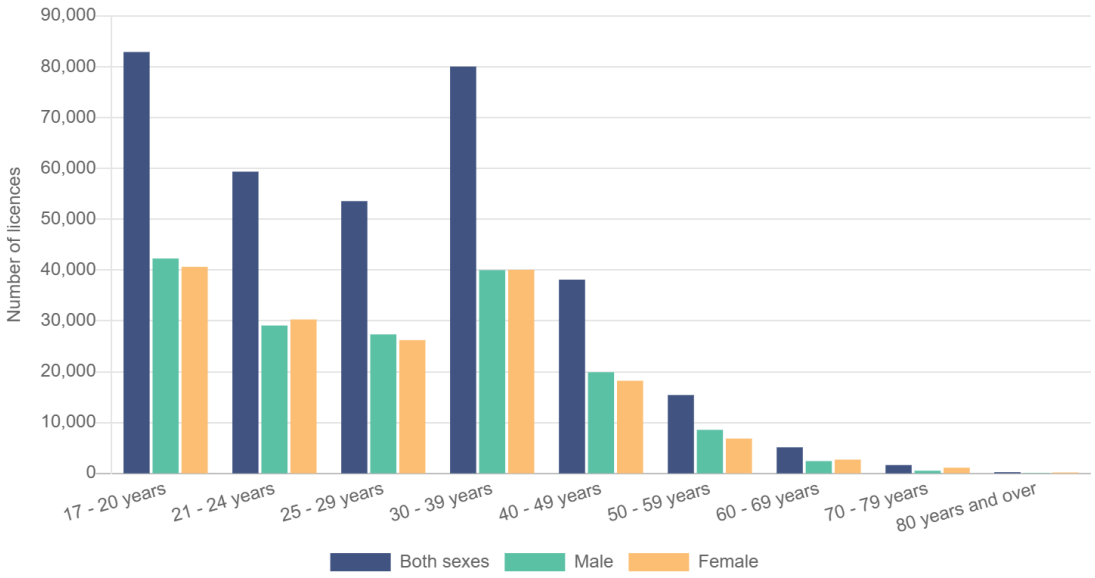
Telephone numbers Home Work Mobile

Occupation

Email address

Figure 9 Motor Accident Form RSCLA3000('Motor Accident Form RSCLA3000.pdf' n.d.)

Insurance companies also collect information not only at the stage of complaints but also when making an offer to a potential client. For example, it can be information such as the number of fines, driver's age, etc. Later, this information is collected to form the cost of the insurance policy and is taken into account in the company's algorithms. In parallel, the company can also take into account open data, such as the distribution of drivers by age or the number of violations in a particular region (and, accordingly, the chance of a further accident). Examples of such data are shown in Figures 10 and 11.



© Road Safety Authority (RSA)
https://data.cso.ie/table/ROA04

Figure 10 Number of learner permit driving licenses by age group and gender ('Driving Licenses Driver and Vehicle Testing Transport Hub - Central Statistics Office' 2025)

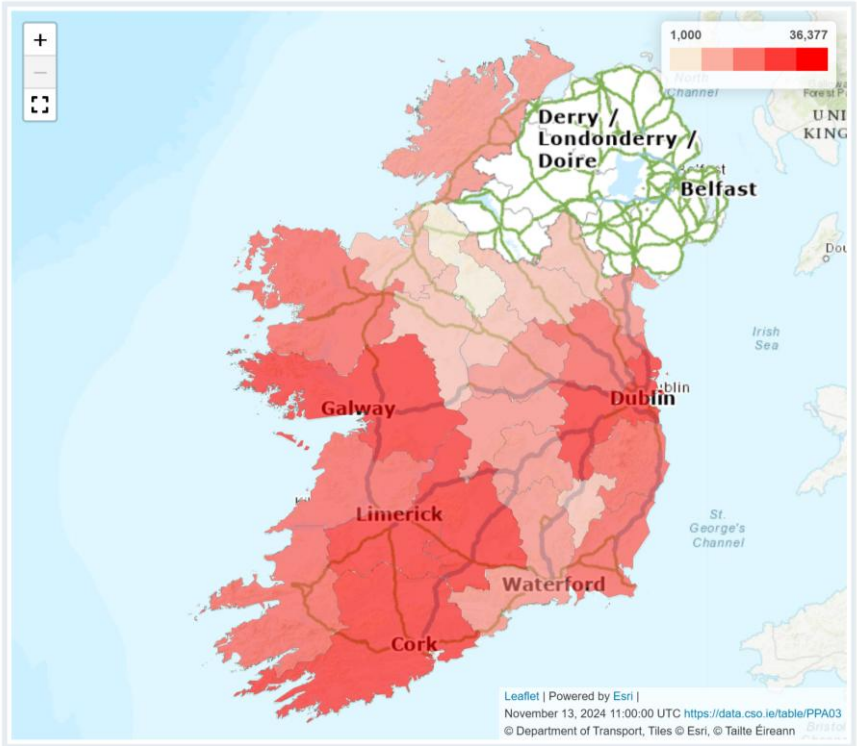


Figure 11 Number of drivers with penalty points applied (in a year) ('Penalty Points Penalty Points Transport Hub - Central Statistics Office' 2025)

If the company operates in the legal framework of the European Union, it must comply with a number of standards, among which the main ones are the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Central Bank of Ireland Regulations (in the case of Irish law), Insurance Distribution Directive (IDD).

- GDPR. This is a general European standard that defines the framework within which stored and intended information is processed within the European Union. Failure to comply with the regulation may result in a fine of EUR 20,000,000 or 4% of the total annual global turnover. Individuals also have the right to file private lawsuits on their own. Companies may also suffer reputational losses in case of non-compliance ('The GDPR and key challenges faced by the insurance industry' n.d.).
- PCI DSS (Payment Card Industry Data Security Standard). PCI DSS (Payment Card Industry Data Security Standard) - includes a set of security standards designed to protect payment card information during processing, storage and transmission. The standard applies to all companies that process payment card data, including insurance companies. Insurance companies must comply with the PCI DSS requirements when processing insurance claims or acting as financial services, ensuring a secure payment environment ('The PCI DSS | IT Governance Europe Ireland' 2025).
- An important standard is also the IDD, Insurance Distribution Directive, which sets out regulatory requirements for the distribution of insurance products. For a company operating in Ireland, this type of regulation should also be taken into account ('Insurance Distribution Directive (IDD) - EIOPA' 2017).

5.2 Regulatory compliance plan

The regulatory compliance plan (GDPR, PCI DSS, IDD, and Central Bank of Ireland regulations) should be implemented as follows.

- Requirements of the European GDPR standard. It is necessary to implement privacy and consent management policies in insurance operational processes. This is required to ensure compliance with data protection regulations. It is essential to encrypt sensitive data, such as medical data, customer addresses, and other data that is essential for insurance. Provide mechanisms for protecting the rights of data subjects, including correcting and deleting data at the request of the client. Have a breach response plan in place that allows for incidents to be reported within 72 hours ('General Data Protection Regulation (GDPR) Compliance Guidelines' 2025).
- PCI DSS standard. It is necessary to use data encryption (public key based algorithms) and tokenization for any operations with financial data. Also, multi-factor authentication is essential for customer security. Regular security testing and compliance maintenance should be ensured through audits, once or several times a year ('Standards' n.d.).
- Insurance Product Distribution (IDD) involves providing clear information about the company's policies, training programs for all employees (carried out by a compliance officer and a security awareness officer). Monitoring of compliance, including formal complaint processes that may be received from customers ('insurance distribution - FCA Handbook' 2025).
- As the company is based in Ireland, it is regulated by the Central Bank of Ireland. It is necessary to ensure compliance with risk management policies, financial processes, including capital adequacy requirements, liquidity, etc. The company's financial department must ensure accurate reporting. Consumer protection should be documented in the company's policies ('Themed Inspections | Central Bank of Ireland' 2025).

All of the above standards have a number of requirements that may be separate from each other, but may also overlap, and therefore it makes sense to conduct a gap analysis to optimize the time allocation of the SAO, CISO, and other involved employees. Since compliance status is often the result of an audit, a company should conduct internal audits to keep its cybersecurity

maturity up to date. To do this, it is necessary to use existing frameworks like the NIST - CSF Maturity Model. The model visualization is shown in Figure 12.

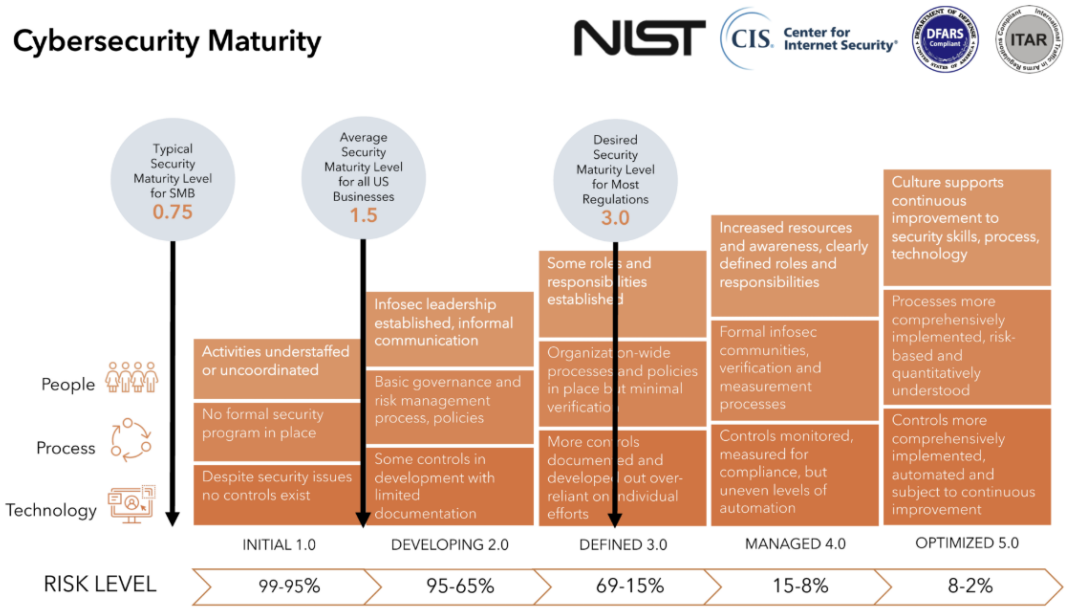


Figure 12 Maturity assessment levels according to the NIST framework (cinchws 2022)

This infographic shows the level of security maturity from 0 to 5, the higher the maturity level, the lower the potential risks for the company. As can be seen, the desired maturity level for most regulations is 3. Since the company is engaged in insurance activities and interacts with a relatively large number of regulations, it makes sense to strive to achieve and or maintain this level, hence using it as a KPI and indicator of potential audit passing (cinchws 2022).

5.3 Top 10 OWASP vulnerabilities

Given the highly dynamic nature of cybersecurity vulnerabilities and risks, it is worth focusing on those that are identified as the most critical, and therefore have a high impact and or likelihood. Such risks are reported by the OWASP organization (Open Web Application Security Project), which focuses on web-based security (‘What is OWASP? What is the OWASP Top 10?’ 2025a). OWASP identifies the 10 most important risks that should be considered in the context of an insurance company and the changes that should be made accordingly.

5.3.1 Broken Access Control

This type of vulnerability means that access control is granted too broadly, thereby violating the principle of least privilege. Access controls can be bypassed by changing URLs, API requests, or internal states. Incorrect CORS configurations allow unauthorized users to access the API.

Preventive measures include denying access by default, checking for record ownership, limiting the speed of API access, and others. As an example of this type of vulnerability, a recent case that is also relevant to insurance can be mentioned. Fidelity Investments Life Insurance experienced a data breach of more than 77,000 customer records caused by unauthorised access (‘Fidelity Data Breach Exposed Info of 77,000 Clients’ 2024).

5.3.2 Cryptographic Failures

This type of potential vulnerability is related to the protection of data during transmission and storage. This applies to sensitive information within the insurance industry, such as medical records, financial information, accident data, etc. These vulnerabilities have a direct impact on GDPR compliance. An example in the insurance sector is an individual who fined an insurance company in New York almost 10 million dollars for poor user data protection, which led to the

leakage of more than 70 thousand personal data of customers. In other words, first and foremost, it is about data encryption, so it is necessary to follow the best practices in terms of backup procedures and encryption of information (read 2024).

5.3.3 Injection

This type of vulnerability includes SQL injection attacks that can be applied to the insurance company's web resources, including the website. Therefore, special attention was given to the selection of technologies for the future website. In case of a successful injection, attackers can gain access to the customer database, which is a critical aspect in the case of an insurance company.

One of the recent examples of such attacks was the incident with the International Civil Aviation Organization (ICAO). The incident occurred in January 2025 and affected 12 thousand people. Data such as name, employment history, emails, etc. were leaked. The attack was caused by a SQL injection (PKWARE 2025).

5.3.4 Insecure Design

This type of problem is associated with errors at the product design stage that lead to security vulnerabilities. Typically, common problems include a lack of threat modelling, weak architecture, and a lack of quality testing. In the case study under consideration, the distribution of PLC controllers depending on their age can potentially lead to this type of problem. For example, if the network is incorrectly segmented at the logical and or physical level. This can create a vulnerable architecture for the insurance company at the stage of making changes. One of the most recent examples was this month's incident in the United States with the insurance company Allstate. An insecure design led to the leakage of hundreds of thousands of user data, including driver's license plates (‘N.Y. AG files complaint in Allstate data breach - Insurance News | InsuranceNewsNet’ 2025).

5.3.5 Security Misconfiguration

Incorrectly configured system security settings can potentially lead to problems such as enabled services that are not needed, default data (passwords, settings, etc.), and default user and file permissions. In the case of an insurance company, access should be granted clearly in accordance with the duties of employees and their positions. An example of incidents due to misconfiguration in the insurance industry was the Vertafore Data Breach a few years ago. The company was a technology provider for insurance companies. As a result, at least 40,000 users from various insurance organizations across the country discovered the data leak. The databases were incorrectly configured, in particular, it was allowed to move particularly important files that were moved to another directory. This should not have happened if the configuration was correct (Team 2021).

5.3.6 Vulnerable and Outdated Components

The software and hardware part of the company's equipment may become outdated. As previously described in this report on the example of PLCs, outdated links lead to potential problems because they may no longer be supported by the vendor, firmware may not be updated, and CVEs can be a potential tool for attackers.

5.3.7 Identification and Authentication Failures

Authentication mechanisms can be a potentially vulnerable link for any company, including the insurance industry. Common problems include weak passwords, improper session management, lack of MFA, etc.An example of such an individual was the Anthem Data Breach, when, thanks to successful phishing, access data to the database was stolen and there was no MFA, which could have become the second layer of protection against attackers (‘Cyber Case Study: Anthem Data Breach - CoverLink Insurance - Ohio Insurance Agency’ 2025).

5.3.8 Software and Data Integrity Failures

This type of vulnerability is related to the integrity of the software product and its dependence on third-party tools, such as plug-ins, modules, libraries, etc. For example, an unprotected CI/CD pipeline is a potential access point for attackers. As a result, they can take advantage of

it to compromise the system (‘A08 Software and Data Integrity Failures - OWASP Top 10:2021’ 2025).
That's why in the previous sections of this report, Oracle database and NGINX were chosen as the technology for the company's new website as they have less dependence on third-party modules.

5.3.9 Security Logging and Monitoring Failures

One of the major problems is that many companies do not invest enough effort in leak detection when using web applications. Therefore, the average detection time can be more than six months, which is enough to cause significant damage to the reputation and business continuity of an insurance company. For example, copying customer databases, etc (‘What is OWASP? What is the OWASP Top 10?’ 2025b). The key to preventing these problems is sufficient monitoring measures and established attack response and recovery procedures, including the use of (NIST) 800-61r2 (‘A09 Security Logging and Monitoring Failures - OWASP Top 10:2021’ 2025). To increase the speed of response, it is also worthwhile to conduct an awareness program among employees so that any indicators of an attack are responded to at all levels, not just the security team within the insurance company. Such a program can be prepared and initiated by the SAO or CISO.

5.3.10 Server-Side Request Forgery (SSRF)

This type of attack allows attackers to make requests from the server to internal or external services, so information or access to internal networks can be compromised. Such problems (SSRF) can occur when a web application receives remote resources directly without validating the URL given by the user (‘A10 Server Side Request Forgery (SSRF) - OWASP Top 10:2021’ 2025). An example of such an attack is the Capital One leak in 2019. The attack lasted almost 4 months before it was noticed. Since the company's focus was on financial and credit activities, the case is also applicable to the insurance industry. It was caused by the fact that a former AWS employee was arrested for data leakage and accused of using server-side request forgery (SSRF) against the AWS infrastructure that stored Capital One's customer data (‘AWS Shared Responsibility Model: Capital One Breach Case Study’ 2025).This leak is also interesting from the perspective of the concept of separation of responsibility when using the cloud. One of the key conclusions of this leak is the need to use a well-configured WAF for the company's processes, which is worth applying as a practice for the case under consideration.
As a result of reviewing the OWASP top 10 vulnerabilities, it can be said that they are relevant to the insurance industry. Therefore, when developing and implementing a new company website, as well as when updating OT equipment, it is necessary to consider these vulnerabilities and best practices to avoid or mitigate them.

6 References

5.9. Row Security Policies [online] (2025) *PostgreSQL Documentation*, available: https://www.postgresql.org/docs/17/ddl-rowsecurity.html [accessed 21 Feb 2025].

9.4. String Functions and Operators [online] (2025) *PostgreSQL Documentation*, available: https://www.postgresql.org/docs/17/functions-string.html [accessed 17 Feb 2025].

'40 Ways to Use Splunk in Financial Services' (n.d.).

A08 Software and Data Integrity Failures - OWASP Top 10:2021 [online] (2025) available: https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/#factors [accessed 28 Mar 2025].

A09 Security Logging and Monitoring Failures - OWASP Top 10:2021 [online] (2025) available: https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/ [accessed 28 Mar 2025].

A10 Server Side Request Forgery (SSRF) - OWASP Top 10:2021 [online] (2025) available: https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/ [accessed 28 Mar 2025].

Allen, R., Chatterjee, A., Cho, C., Czarski, C., Dietrich, C.M., Farrell, H., Galdamez, A., Godfrey, J., Grasshoff, F., Millan, M.G., Morneau, V., Muench, S., Muller, R., Nagy, F., Ravva, S., Rayner, A., Rokitta, C., Sewtz, M., Straub, J., Synders, J., Wolf, P., and Jennings, T. (2025) Understanding Cross-Site Scripting Protection [online], *Oracle Help Center*, available: https://docs.oracle.com/en/database/oracle/apex/24.1/htmdb/cross-site-scripting-protection.html#GUID-EBB112AB-766E-4383-AA3A-0971561E8042 [accessed 18 Feb 2025].

Alpern, D., Agrawal, S., Baer, H., Castledine, S., Chang, T., Cheng, B., Dani, R., Decker, R., Iyer, C., Kruglikov, A., Le, N., Li, W., Llewellyn, B., Raney, T., Rajagopalan, R., Stocks, I., Wetherell, C., Wolicki, S., Viswanathan, G., Yang, M., and Morin, L. (2025) PL/SQL Dynamic SQL [online], *Oracle Help Center*, available: https://docs.oracle.com/en/database/oracle/oracle-database/19/lnpls/dynamic-sql.html#GUID-7E2F596F-9CA3-4DC8-8333-0C117962DB73 [accessed 17 Feb 2025].

Apache Hardened Web Server - Documentation [online] (2025) available: https://docs.rockylinux.org/guides/web/apache_hardened_webserver/ [accessed 17 Feb 2025].

Apache HTTP Server 2.4 Vulnerabilities - The Apache HTTP Server Project [online] (2025) available: https://httpd.apache.org/security/vulnerabilities_24.html [accessed 17 Feb 2025].

AWS Shared Responsibility Model: Capital One Breach Case Study [online] (2025) available: https://www.appsecengineer.com/blog/aws-shared-responsibility-model-capital-one-breach-case-study [accessed 28 Mar 2025].

Backup and Restore [online] (2012) *PostgreSQL Documentation*, available: https://www.postgresql.org/docs/8.1/backup.html [accessed 21 Feb 2025].

Best Web And Application Servers Software in 2025 [online] (2025) *6sense*, available: https://www.6sense.com/tech/web-and-application-servers [accessed 17 Feb 2025].

Carter, G. (2011) 'Protecting_PostgreSQL_Against_SQL_Injection_Attack'.

Chapter 40. Procedural Languages [online] (2025) *PostgreSQL Documentation*, available: https://www.postgresql.org/docs/17/xplang.html [accessed 18 Feb 2025].

cinchws (2022) 'Are you prepared to defend your law firm against cyberthreats?', *Strategic Technology Solutions*, available: https://stspartner.com/are-you-prepared-to-defend-your-law-firm-against-cyberthreats/ [accessed 24 Mar 2025].

Cosman, E. (2025) Structuring the ISA/IEC 62443 Standards [online], available: https://gca.isa.org/blog/structuring-the-isa-iec-62443-standards [accessed 23 Feb 2025].

CREATE FUNCTION [online] (2025) *PostgreSQL Documentation*, available: https://www.postgresql.org/docs/17/sql-createfunction.html [accessed 18 Feb 2025].

CVE - CVE [online] (2025) available: https://cve.mitre.org/ [accessed 17 Feb 2025].

CVE Security Vulnerability Database. Security Vulnerabilities, Exploits, References and More [online] (2025) available: https://www.cvedetails.com/index.php [accessed 17 Feb 2025].

Cyber Case Study: Anthem Data Breach - CoverLink Insurance - Ohio Insurance Agency [online] (2025) available: https://coverlink.com/case-study/anthem-data-breach/ [accessed 28 Mar 2025].

Database PL/SQL User's Guide and Reference [online] (2025) available: https://docs.oracle.com/cd/B19306_01/appdev.102/b14261/wrap.htm [accessed 18 Feb 2025].

Database Security Guide [online] (2025) available: https://docs.oracle.com/cd/E11882_01/network.112/e36292/vpd.htm#DBSEG251 [accessed 21 Feb 2025].
Database Vault Administrator's Guide [online] (2025) available: https://docs.oracle.com/cd/B32267_01/server.102/b25166/dvintro.htm#DVADM70088 [accessed 18 Feb 2025].
Driving Licenses Driver and Vehicle Testing Transport Hub - Central Statistics Office [online] (2025) available: https://www.cso.ie/en/releasesandpublications/hubs/p-transo/transporthub/driverandvehicletesting/drivinglicenses/ [accessed 23 Feb 2025].
Duraiswamy, S., Hwa, M., Iyer, S., Kalyanasundaram, S., Kethana, L., Knaggs, P., Koyfman, A., Lim, D.-Y., Lee, A., Lindsey, A., Mir, R., Mulagund, G., Philips, A., Ramakrishna, P., Saha, S., Thornton, P., Wahl, P., Yuan, L., Youn, P., and Huey, P. (2025) Introduction to Transparent Data Encryption [online], *Oracle Help Center*, available: https://docs.oracle.com/en/database/oracle/oracle-database/18/asoag/introduction-to-transparent-data-encryption.html#GUID-62AA9447-FDCD-4A4C-B563-32DE04D55952 [accessed 21 Feb 2025].
End of Life of Expiring Products - Mitsubishi Electric Factory Automation - Germany [online] (2025) available: https://de.mitsubishielectric.com/fa/de_en/service/EOL [accessed 17 Feb 2025].
F.38. Sepgsql — SELinux-, Label-Based Mandatory Access Control (MAC) Security Module [online] (2025) *PostgreSQL Documentation*, available: https://www.postgresql.org/docs/17/sepgsql.html [accessed 21 Feb 2025].
Fidelity Data Breach Exposed Info of 77,000 Clients [online] (2024) *PLANADVISER*, available: https://www.planadviser.com/fidelity-data-breach-exposed-info-77000-clients/ [accessed 28 Mar 2025].
General Data Protection Regulation (GDPR) Compliance Guidelines [online] (2025) *GDPR.eu*, available: https://gdpr.eu/ [accessed 24 Mar 2025].
Guardian | OT Network Monitoring [online] (2025) available: https://www.nozominetworks.com/products/guardian [accessed 22 Feb 2025].
IEC 62443 Standard: Enhancing Cybersecurity for Industrial Automation and Control Systems [online] (2025) *Fortinet*, available: https://www.fortinet.com/resources/cyberglossary/iec-62443 [accessed 23 Feb 2025].
'Inside NGINX: How We Designed for Performance & Scale – NGINX Community Blog' (2015) available: https://blog.nginx.org/blog/inside-nginx-how-we-designed-for-performance-scale [accessed 17 Feb 2025].
Insurance Distribution - FCA Handbook [online] (2025) available: https://www.handbook.fca.org.uk/handbook/glossary/G3492i.html [accessed 24 Mar 2025].
Insurance Distribution Directive (IDD) - EIOPA [online] (2017) available: https://www.eiopa.europa.eu/browse/regulation-and-policy/insurance-distribution-directive-idd_en [accessed 23 Feb 2025].
ISO/IEC 27001:2022 [online] (2025) *ISO*, available: https://www.iso.org/standard/27001 [accessed 23 Feb 2025].
Jashnani, P., Weill, K., Ashdown, L., Bednar, T., Beldalker, A., Chien, T., Dilman, M., Fogel, S., Guzman, R., Haisley, S., Hu, W., Hwang, A., Joshi, A., Krishnaswamy, V., Lee, J.W., Moore, V., Olagappan, M., Panteleenko, V., Ranganathan, S., Sanchez, F., Smith, K.D., Srihari, V., Susairaj, M., Stewart, M., Wertheimer, S., Yang, W., Zijlstra, R., and P, R. (2025) Introduction to Backup and Recovery [online], *Oracle Help Center*, available: https://docs.oracle.com/en/database/oracle/oracle-database/19/bradv/introduction-backup-recovery.html#GUID-014F80B5-9A80-4CDB-B282-3FD0C3610FC9 [accessed 21 Feb 2025].
Koshy, S.M. (2022) Top 10 Most Popular Databases Use in 2025 | Zuci Systems [online], available: https://www.zucisystems.com/blog/most-popular-databases/ [accessed 17 Feb 2025].
'Mitigating DDoS Attacks with NGINX – NGINX Community Blog' (2015) available: https://blog.nginx.org/blog/mitigating-ddos-attacks-with-nginx-and-nginx-plus [accessed 17 Feb 2025].
Mod_authnz_ldap - Apache HTTP Server Version 2.4 [online] (2025) available: https://httpd.apache.org/docs/2.4/mod/mod_authnz_ldap.html [accessed 17 Feb 2025].

Modbus, DNP3 and HART | Infosec [online] (2025) available: https://www.infosecinstitute.com/resources/scada-ics-security/modbus-dnp3-and-hart/ [accessed 22 Feb 2025].
Mod_perl: User's Guide [online] (2025) available: https://perl.apache.org/docs/2.0/user/index.html [accessed 17 Feb 2025].
Module Ngx_http_fastcgi_module [online] (2025) available: https://nginx.org/en/docs/http/ngx_http_fastcgi_module.html#example [accessed 17 Feb 2025].
'Motor Accident Form RSCLA3000.pdf' (n.d.) available: https://www.rsagroup.ie/sites/default/files/Motor%20Accident%20Form%20RSCLA3000.pdf?utm_source=chatgpt.com [accessed 23 Feb 2025].
Muscat, I. (2019) Mitigate Slow HTTP GET/POST Vulnerabilities in the Apache HTTP Server [online], *Acunetix*, available: https://www.acunetix.com/blog/articles/slow-http-dos-attacks-mitigate-apache-http-server/ [accessed 17 Feb 2025].
NGINX Documentation [online] (2025) available: https://docs.nginx.com/ [accessed 17 Feb 2025].
NVD - Cve-2020-25695 [online] (2025) available: https://nvd.nist.gov/vuln/detail/cve-2020-25695 [accessed 21 Feb 2025].
NVD - Cve-2021-40368 [online] (2025) available: https://nvd.nist.gov/vuln/detail/cve-2021-40368 [accessed 22 Feb 2025].
NVD - CVE-2022-25162 [online] (2025) available: https://nvd.nist.gov/vuln/detail/CVE-2022-25162 [accessed 22 Feb 2025].
NVD - Cve-2022-38465 [online] (2025) available: https://nvd.nist.gov/vuln/detail/cve-2022-38465 [accessed 22 Feb 2025].
NVD - Cve-2023-1424 [online] (2025) available: https://nvd.nist.gov/vuln/detail/cve-2023-1424 [accessed 22 Feb 2025].
NVD - Cve-2023-6942 [online] (2025) available: https://nvd.nist.gov/vuln/detail/cve-2023-6942 [accessed 22 Feb 2025].
NVD - Cve-2024-21111 [online] (2025) available: https://nvd.nist.gov/vuln/detail/cve-2024-21111 [accessed 21 Feb 2025].
N.Y. AG Files Complaint in Allstate Data Breach - Insurance News | InsuranceNewsNet [online] (2025) available: https://insurancenewsnet.com/innarticle/n-y-ag-files-complaint-in-allstate-data-breach [accessed 28 Mar 2025].
Penalty Points Penalty Points Transport Hub - Central Statistics Office [online] (2025) available: https://www.cso.ie/en/releasesandpublications/hubs/p-transo/transporthub/penaltypoints/penaltypoints/ [accessed 23 Feb 2025].
PHP: Apache 2.x on Unix Systems - Manual [online] (2025) available: https://www.php.net/manual/en/install.unix.apache2.php [accessed 17 Feb 2025].
PKWARE (2025) Data Breach Report: January 2025 Edition [online], *PKWARE®*, available: https://www.pkware.com/blog/data-breach-report-january-2025-edition [accessed 28 Mar 2025].
Preventing SQL Injection [online] (2025) available: https://docs.oracle.com/cd/F40609_01/pt859pbr1/eng/pt/tpcd/task_PreventingSQLInjection-0749b7.html [accessed 17 Feb 2025].
Prevention of Privilege Escalation - System Administration Guide: Security Services [online] (2025) available: https://docs.oracle.com/cd/E26505_01/html/E27224/privref-20.html [accessed 21 Feb 2025].
read, M.K. 2 min (2024) New York Fines Geico, Travelers $11.3M for Pandemic-Era Breaches [online], *Yahoo Finance*, available: https://www.cybersecuritydive.com/news/new-york-fines-geico-travelers/734045/ [accessed 28 Mar 2025].
Rick-Anderson (2022) Security Authentication <authentication> [online], available: https://learn.microsoft.com/en-us/iis/configuration/system.webserver/security/authentication/ [accessed 17 Feb 2025].
Role-Based Access Control (Overview) - Oracle Solaris 11.1 Administration: Security Services [online] (2025) available: https://docs.oracle.com/cd/E26502_01/html/E29015/rbac-1.html [accessed 21 Feb 2025].
Security Tips - Apache HTTP Server Version 2.4 [online] (2025) available: https://httpd.apache.org/docs/2.4/misc/security_tips.html [accessed 17 Feb 2025].

Set up Basic Authentication | NGINX Documentation [online] (2025) available: https://docs.nginx.com/nginx-instance-manager/admin-guide/authentication/basic-auth/set-up-basic-authentication/ [accessed 17 Feb 2025].
SQL Firewall Now Built into Oracle Database 23ai [online] (2025) available: https://blogs.oracle.com/cloudsecurity/post/sql-firewall-now-built-into-oracle-database-23c [accessed 17 Feb 2025].
'Standards' (n.d.) *PCI Security Standards Council*, available: https://www.pcisecuritystandards.org/standards/ [accessed 24 Mar 2025].
Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., and Thompson, M. (2023) *Guide to Operational Technology (OT) Security*, NIST SP 800-82r3, National Institute of Standards and Technology (U.S.), Gaithersburg, MD, available: https://doi.org/10.6028/NIST.SP.800-82r3.
Team, F.I. (2021) 'Misconfiguration Results in Two Vertafore Data Breaches', *Flashpoint*, available: https://flashpoint.io/blog/misconfiguration-results-in-two-vertafore-data-breaches/ [accessed 28 Mar 2025].
Technologies, C. (2019) 'How to make sense of Cybersecurity Frameworks', *Cuelogic An LTI Company*, available: https://www.cuelogic.com/blog/cybersecurity-frameworks [accessed 23 Feb 2025].
'The GDPR and key challenges faced by the insurance industry' (n.d.).
The PCI DSS | IT Governance Europe Ireland [online] (2025) available: https://www.itgovernance.eu/en-ie/what-is-the-pci-dss-ie [accessed 23 Feb 2025].
Themed Inspections | Central Bank of Ireland [online] (2025) available: https://www.centralbank.ie/regulation/consumer-protection/compliance-monitoring/themed-inspections [accessed 24 Mar 2025].
Understanding and Implementing FastCGI Proxying in Nginx | DigitalOcean [online] (2025) available: https://www.digitalocean.com/community/tutorials/understanding-and-implementing-fastcgi-proxying-in-nginx [accessed 17 Feb 2025].
Web Server vs Application Server - Difference Between Technology Servers - AWS [online] (2025) *Amazon Web Services, Inc.*, available: https://aws.amazon.com/compare/the-difference-between-web-server-and-application-server/ [accessed 17 Feb 2025].
What Is a Database? [online] (2025) available: https://www.oracle.com/ie/database/what-is-database/ [accessed 17 Feb 2025].
What Is OAuth? | Microsoft Security [online] (2025) available: https://www.microsoft.com/en-us/security/business/security-101/what-is-oauth [accessed 17 Feb 2025].
What Is OT Security? | IBM [online] (2024) available: https://www.ibm.com/think/topics/ot-security [accessed 22 Feb 2025].
What Is OWASP? What Is the OWASP Top 10? [online] (2025a) available: https://www.cloudflare.com/learning/security/threats/owasp-top-10/ [accessed 27 Mar 2025].
What Is OWASP? What Is the OWASP Top 10? [online] (2025b) available: https://www.cloudflare.com/learning/security/threats/owasp-top-10/ [accessed 28 Mar 2025].
What Is Penetration Testing? | What Is Pen Testing? [online] (2025) available: https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/ [accessed 22 Feb 2025].
What Is Personally Identifiable Information (PII)? | IBM [online] (2022) available: https://www.ibm.com/think/topics/pii [accessed 23 Feb 2025].
What Is PRINCE2? The Definition, History & Benefits | UK [online] (2025) available: https://www.prince2.com/uk/what-is-prince2 [accessed 23 Feb 2025].
What Is Privilege Escalation? | CrowdStrike [online] (2025) *CrowdStrike.com*, available: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/privilege-escalation/ [accessed 21 Feb 2025].
What Is the CIA Triad and Why Is It Important? [online] (2025) *Fortinet*, available: https://www.fortinet.com/resources/cyberglossary/cia-triad [accessed 17 Feb 2025].