

CHAPTER 2 - LITERATURE REVIEW

2.1. Media Industry.

Industrial media refers to the economic sector involved in the production, distribution, and consumption of media content, be it in the form of text, audio, video, or other digital forms. According to (Curran and Hesmondhalgh, 2021), the media industry includes various fields such as films, television, music, publishing, and digital platforms. This industry does not only focus on the creation of content, but also in the distribution mechanism that ensures that the content can be accessed by the broad audience. Hesmondhalgh stressed that industrial media is an integral part of the creative economy, where economic value is produced through creativity and innovation in producing cultural products. However, this industry also faces challenges such as the concentration of ownership by large corporations, which can reduce the diversity of content and healthy competition.

One of the main challenges of industrial media is the adaptation of rapid technological changes. (Mosco, 2019) explains that the emergence of digital platforms and social media has shifted traditional business models, demanding media companies to innovate in terms of distribution and monetization of content. Other challenges are strict regulations related to copyright, data privacy, and dissemination of false information. In addition, Mosco highlights the inequality of access to digital infrastructure, which can widen the gap between developed and developing countries. These challenges not only affect industrial sustainability, but also have an impact on the quality and diversity of content produced.

The influence of industrial media on human life is very broad and complex. (Doyle, 2016) explains that the media not only functions as a source of information and entertainment, but also forms the way we think, interact, and understand the world. However, Doyle also warns that the dominance of algorithms in digital platforms can affect the type of content consumed, so that it has the potential to create a "bubble filter" that limits exposure to different perspectives. In addition, profit oriented media industries often sacrifice public interests, such as by spreading sensational content or

manipulating user emotions to increase involvement. Therefore, it is important to realize the impact of industrial media and take steps to consume it critically and responsibly. Cybersecurity risk resilience is the ability of an organization to prevent, survive, and recover from cybersecurity incidents. (Weil and Murugesan, 2020). This concept is applied in IT infrastructure by integrating proactive and reactive strategies to protect digital assets, ensure operational continuity, and minimize the impact of potential cyber threats. The basic principles of cybersecurity are often summarized in the CIA Triad, which includes Confidentiality, which is Ensuring that information can only be accessed by authorized parties. Integrity, which is Ensuring that data and systems remain accurate and are not subject to unauthorized changes. And Availability, which is Ensuring that information and system resources are available to authorized users when needed. (MI Khalid, 2025).

Cybersecurity risk management focuses on the process of identifying, assessing, and controlling threats to an organization's digital information and information technology systems. The goal is to protect data, networks, and devices from unauthorized access, damage, or attacks that could disrupt business operations. On the other hand, cyber resilience emphasizes an organization's ability to withstand and recover from a cyber incident, ensuring that business operations can continue despite an attack. In the context of the media industry, this distinction is important because risk management focuses on preventing and mitigating threats, while cyber resilience ensures the continuity of information delivery to the public despite cyber disruptions.

The media industry has become increasingly reliant on information technology (IT) infrastructure to support its operations, from content creation and distribution to audience engagement. However, this dependence on digital technologies has also exposed the industry to a range of cybersecurity threats and vulnerabilities (Alshboul *et al.*, 2021). The media industry's sensitive data, such as intellectual property, customer information, and financial records, make it a prime target for cybercriminals (Goel and Jain, 2018). Additionally, the industry's high profile nature and the potential impact of successful attacks on public perception and trust further underscore the importance of robust cybersecurity strategies.

According to a report by the World Economic Forum, the media industry ranked among the top three sectors most affected by cyberattacks in 2021, with an estimated global cost of \$23 billion. The rise in remote work and cloudbased services during the COVID-19 pandemic has also expanded the attack surface for media organizations, making them more vulnerable to threats such as phishing, ransomware, and data breaches (Shaukat *et al.*, 2024).

The media industry's reliance on complex IT infrastructure, including content management systems, digital asset management platforms, and cloud-based collaboration tools, has increased the potential for vulnerabilities and the need for comprehensive cybersecurity strategies (Goel and Jain, 2018). Outdated software, inadequate access controls, and lack of employee cybersecurity awareness can all contribute to the industry's susceptibility to cyberattacks (Alshboul *et al.*, 2021). Recognizing the critical importance of cybersecurity, many media organizations have started to invest in advanced security measures, such as network monitoring, threat intelligence, and incident response planning (Shaukat *et al.*, 2024). However, the rapidly evolving nature of cyber threats and the increasing sophistication of attackers require a more proactive and comprehensive approach to cybersecurity in the media industry (Goel and Jain, 2018).

PT Media Televisi Indonesia, known as MetroTV, is one of Indonesia's most prominent television networks, recognized for its strong focus on news and current affairs. Established in 2000, MetroTV has built a reputation as a reliable and credible source of information, catering to a wide audience that includes urban professionals, policymakers, and the general public. Its programming is centered around delivering real-time news, in-depth analysis, and investigative journalism, making it a go-to channel for breaking news and political coverage. Beyond news, MetroTV also offers a variety of educational programs, documentaries, and talk shows that address important societal issues, aligning with its motto, "Knowledge to Elevate the Nation." This commitment to education and public awareness has helped MetroTV establish a strong brand identity, characterized by professionalism, high production quality, and a focus on social responsibility.

From a business perspective, MetroTV as one of media industry operates as a commercial entity with multiple revenue streams. Its primary source of income comes from advertising, including commercials, sponsored content, and product placements. The channel also generates revenue through partnerships and collaborations with government agencies, private companies, and international media organizations. These collaborations often involve joint projects, content sharing, and the production of special events such as debates, award shows, and live coverage of major national events. Additionally, MetroTV has expanded its reach into the digital space, offering live streaming, on-demand content, and news updates through its website and mobile apps. This digital expansion allows MetroTV to engage with younger, tech-savvy audiences and adapt to the changing media consumption habits of viewers.

MetroTV's market position is strong, particularly in the news and current affairs segment, where it competes with other major networks like TVRI, Kompas TV, and CNN Indonesia. Its ability to provide comprehensive and timely news coverage has solidified its status as one of Indonesia's top news channels. Furthermore, MetroTV is actively involved in corporate social responsibility (CSR) initiatives, such as educational programs, disaster relief efforts, and environmental campaigns. These initiatives not only enhance its reputation but also strengthen its connection with the community. Despite facing challenges such as intense competition from other media platforms and the fragmentation of audiences due to the rise of social media, MetroTV continues to innovate and adapt. By investing in advanced broadcasting technology and diversifying its content offerings, MetroTV remains a trusted and influential player in Indonesia's media landscape.

2.2. Media Technology

In the digital era, the media industry has adopted various advanced technologies to increase production, distribution and consumption of content. Television media have adopted various advanced technologies to improve the quality of production and distribution of content. One of the main technologies is High-Definition (HD) and Ultra High-Definition (UHD or 4K), which provides a much sharper and detailed image resolution compared to traditional analog television. According to (Lotz and Lunardi, 2025), this technology not only enhances the viewing experience for the audience but

also allows content manufacturers to create more immersive visuals. In addition, High Dynamic Range (HDR) technology is used to improve color quality and contrast, making images look more lively and realistic. This technology has become the standard in the production of television shows, film and sports broadcasts.

In addition to visual technology, television media also uses internet protocol television (IPTV) and over-the-top (OTT) to distribute content. By (Johnson, 2019) explains that IPTV allows television broadcasts to be channeled through the internet network, so that the audience can access content on-demand and cross platforms. Meanwhile, OTT platforms such as Netflix, Upstream, and Disney+ have changed the way the audience to consume television content, by offering flexibility to watch anytime and anywhere. Traditional television stations also adopt the OTT model by launching their own streaming applications, such as BBC iplayer or NBC Peacock, to maintain relevance in the digital age.

High-Performance Computing (HPC) technology has also revolutionized content production, especially in the film and animated industry. According to (Lotz and Lunardi, 2025), HPC allows 3D graphics rendering and complex visual effects to be much shorter than the previous technology. For example, animated studios like Pixar use HPC to process scenes that require high details, so that they can meet the production time deadline without sacrificing quality. This technology is very important in industries that require high speed and precision.

The role of technology in the speed of content production is also seen in the use of real-time rendering and live streaming tools. (Gillespie, 2019) explains that this technology allows direct content production, such as news broadcasts or sports events, with quality equivalent to post production. For example, sophisticated cameras and real-time rendering software can produce direct visual effects during broadcasts, reduce the need for additional editing. This allows content to be broadcast faster and more responsive to the latest developments.

Although technology has increased the speed of content production, challenges remain. (Zuboff, 2022) warns that dependence on technology can reduce the quality of content

if it is not balanced with human creativity and control. In addition, the cost of implementing advanced technology such as AI and HPC can be a barrier for small content manufacturers. Therefore, it is important for the media industry to find a balance between utilizing technology for efficiency and maintaining the integrity and quality of the content produced.

The development of information technology today has reached a point where the nature of conventional technology which is massive and the nature of computer technology which is interactive can be combined. This is called convergence. Current media convergence allows mass media actors to deliver news while presenting information and entertainment on various media platforms. Therefore, media workers must be more creative in providing content for the audience. This condition is a great opportunity for creative and media industry players. Media, telecommunications, and technology companies work together and form strategic alliances to develop new business models that allow them to profit from consumers of on-demand media content. The same opportunity, according to Indrati, 2018, can also be seized by creative content developers who convert into digital formats that meet broadcasting industry standards using computers and mobile devices.

Media convergence has changed the way the television industry operates, by integrating digital technology to expand reach and interactivity. One of the main technologies used is Internet Protocol Television (IPTV). According to (Lotz and Lunardi, 2025), IPTV allows television broadcasts to be channeled through the internet network, so that the audience can access content on-demand and cross-platforms. This technology allows television stations to offer more flexible services, such as re-broadcasts, live streaming, and exclusive content that can be accessed through smart TV, computers, or mobile devices. IPTV also opens new opportunities for television to compete with streaming platforms such as Netflix and Youtube.

Cloud computing technology also plays a key role in television media convergence. (Dwyer *et al.*, 2021) states that cloud computing allows television stations to store and

manage large -scale content, and distribute them efficiently to various platforms. By using Cloud, television content manufacturers can reduce infrastructure costs and increase production speed. In addition, cloud computing allows better collaboration between the production team scattered in various locations, thus speeding up the process of making content such as direct events, serials, or documentary.

Interactivity is another aspect that is improved through technology in the convergence of television media. (Burgess, Marwick and Poell, 2018) explains that television now integrates interactive features such as the Second Screen Experience, where the audience can interact with content through other devices such as smartphones or tablets. For example, sports events or reality shows often provide companion applications that allow the audience to vote, access statistics, or participate in direct discussions. This technology not only increases the involvement of the audience but also opens new opportunities for monetization through interactive advertising and sponsors. ®

Although media convergence technology brings many benefits, the television industry also faces challenges. First, competition with digital platforms that are more flexible and cheaper, such as YouTube or Tiktok, demanding television stations to continue to innovate. Second, the challenges of regulations and copyright often hamper the distribution of cross platform content. (Zuboff, 2022) also reminded that dependence on user data for content personalization can cause privacy and ethical problems. Therefore, the television industry needs to find a balance between utilizing technology and maintaining the trust and satisfaction of the audience.

The work mechanism of the converged newsroom at PT.XYZ that has three multiplatform media consists of three main priorities. PT.XYZ has prepared a super desk newsroom to integrate media internal processes. The integration of three multiplatform media is intended to improve cost efficiency and prepare human resources to multitask to answer the challenges for the mass media industry in the digital era through convergence business model. The work methods of convergence journalists through a continuous process are supported by robust super desk, which will handle those left out

by the journalists. With regard to the convergence system having been applied as an effort to develop its business management, PT.XYZ has implemented a work mechanism with the integration concept Newsroom 3.0, which is presented in Figure 2.1.

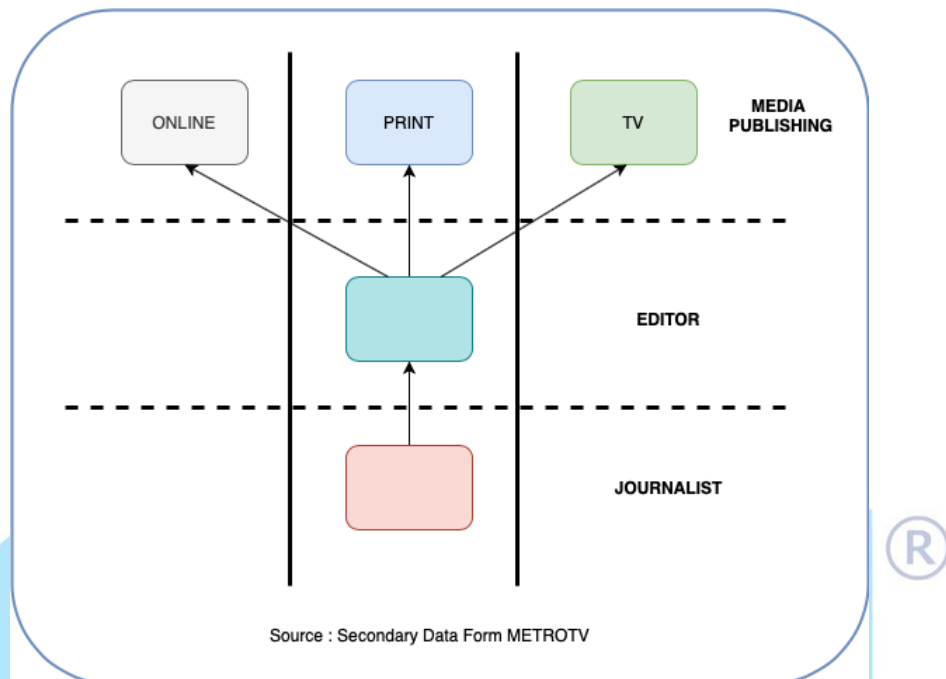


Figure 2.1. Newsroom 3.0 Model (Indrati,2018).

In the Newsroom 3.0 convergence model, journalists are required to present their work in multiple formats, including audio, visual, and written narratives, to the producer or editor. The producer or editor then takes responsibility for distributing these news materials across various platforms, selecting the appropriate format to suit the specific needs of each platform, such as television, online media, or print publications.

For the implementation using super desk newsroom model, PT.XYZ has provided the following:

1. Integrated editing room.
2. Content for various channels by integrating complete news flow for both print and digital versions since the planning stage to the production stage.
3. No particular person in charge of channels in the coordinating mechanism.
4. Responsibility for newsgathering for print and digital media that is borne by the head of section.

In Indrati research, preparation should also be carried out for the technological system, human resources, management system, work pattern, and key performance indicators to measure the journalists' development in terms of skills, knowledge, and behaviours. This will definitely require support from different parties involved, including:

1. IT and support department,
2. Research and data department of PT.XYZ,
3. Journalists,
4. Editing department,
5. Program/content department,
6. News portals, and
7. Training centre (human resource capital).

In supporting media convergence, PT.XYZ are implementing several technology transfers such as the use of digital broadcast television systems and from a newsroom perspective using the latest newsroom system that is integrated with various platforms. therefore, the implementation of a content management system (CMS) application for a news data collection center in the field from journalists is very important for the sustainability of the company's fast and integrated business.

2.3. Content Management System.

Content Management System (CMS) is a software that allows users to create, manage, and publish digital content without the need for in depth technical knowledge about programming. According to (Chaffey and Ellis-Chadwick, 2019), CMS is widely used in various industries, including the media, e-commerce, education, and government, to manage websites, blogs and other digital platforms. The main function of CMS is to simplify the process of manufacturing and update content, allowing the team to collaborate efficiently, and ensure consistency in the design and structure of content. With CMS, users can focus on the content itself, while the system handles technical aspects such as hosting, security, and optimization.

The CMS function is not limited to content management, but also includes media management, such as images, videos, and documents. According to (Pham and Nguyen, 2023), CMS provides a user-friendly interface to upload, manage, and integrate media

into content. In addition, CMS is often equipped with tools to optimize content to be friendly to search engines (search engine optimization or SEO), which helps increase the visibility of the website in search results. Other common features are found in CMS including user management, where administrators can manage access rights and roles for each team member, as well as the ability to schedule content publications.

The way CMS works is based on architecture that separates content from design and functionality. According to (Martinez-Caro *et al.*, 2018), CMS uses a database to store content, while templates and plugins set the appearance and features of the website. When the user creates or edits content through the CMS interface, the change is stored in the database. When visitors access the website, CMS takes content from the database and displays it according to the specified template. This approach allows fast and consistent content updates without the need to change the basic code of the website.

The technology used in CMS varies depending on the platform, but some general components including programming languages such as PHP, Python, or Javascript, as well as databases such as MySQL or PostgreSQL. According to Richardson and Ruby (2020), popular CMS such as WordPress, Joomla, and Drupal were built using open-source technology, which allows developers to adjust and expand functionality as needed. In addition, Modern CMS often integrates the Application Programming Interface (API) technology to connect websites with external services, such as social media, analytical devices, or payment systems.

Although CMS offers many benefits, there are also challenges that need to be considered. According to (Contu *et al.*, 2016), security is one of the main problems, because the popular CMS is often the target of cyber attacks. Therefore, it is important to ensure that CMS is always updated with the latest security patches and is equipped with safety features such as encryption and two -factors authentication. In addition, CMS performance can be affected if there are too many plugins or content that is not well optimized. By understanding the functions, ways of working, and the technology used in CMS, users can maximize their potential while overcoming challenges that might arise.

2.3.1.Design CMS Overview.

Content Management System (CMS) Special television media is designed to manage, organize, and distribute audiovisual content efficiently. According to (Lotz and Lunardi, 2025), CMS in the television context functions as a control center for production, storage and distribution of content, ranging from live events, record programs, to on-demand content. Its main functions include metadata management (such as the title, description, and tag), broadcast scheduling, and integration with distribution platforms such as Television, OTT, news website and social media. CMS also allows television stations to manage copyright and content licenses, ensuring compliance with industrial regulations. With CMS, the production process and distribution of content becomes more structured and can be accessed by various departments in media organizations.

The way CMS specifically television media involves the integration between content databases, storage systems, and user-friendly user interfaces. According to (Martinez-Caro *et al.*, 2018), CMS takes raw content (such as video, audio, and graphics) of the production system, storing it in centralized databases, and managing them through structured metadata. When the content is ready to be broadcast, CMS sends it to various distribution platforms, such as live broadcasts, streaming applications, or websites. The technology used in CMS includes storage and scale, artificial intelligence (AI) for content and recommendations analysis, as well as fire for integration with external systems such as analytical devices and ad platforms. With this technology, CMS allows television media to adapt to the demands of the digital era and improve operational efficiency.

2.3.2. System Design CMS.

Content Management System (CMS) Design Special Television Media is designed to meet the needs of the broadcasting industry complex, which involves large scale production, management, and distribution of audiovisual content. According to (Lotz and Lunardi, 2025), this system usually consists of several main modules, including media asset management (media asset management or MAM), broadcast scheduling, and integration with distribution platforms such as television system, website news and OTT. This CMS design emphasizes scalability and flexibility, allowing television stations to manage thousands of hours of coverage, which will be sidelined. In addition,

this CMS is designed to support collaboration between teams, such as producers, editors, and journalists, with intuitive interfaces and the ability to track change in real-time.

On figure 2.2, showing the technology that underlies the design of television media CMS includes server infrastructure for data storage and processing, as well as features for task automation such as tagging metadata, content builder story, journalist assignments, data from other sources and program recommendations. According to (Martinez-Caro *et al.*, 2018), CMS also integrates a fire to connect the internal system with an external platform. Data security is a priority in the CMS design, with features such as encryption, multi-factor authentication, and strict access rights management. With a comprehensive design, CMS allows television media to operate efficiently, reduce production costs, and improve end user experience through faster and better personalization distribution.

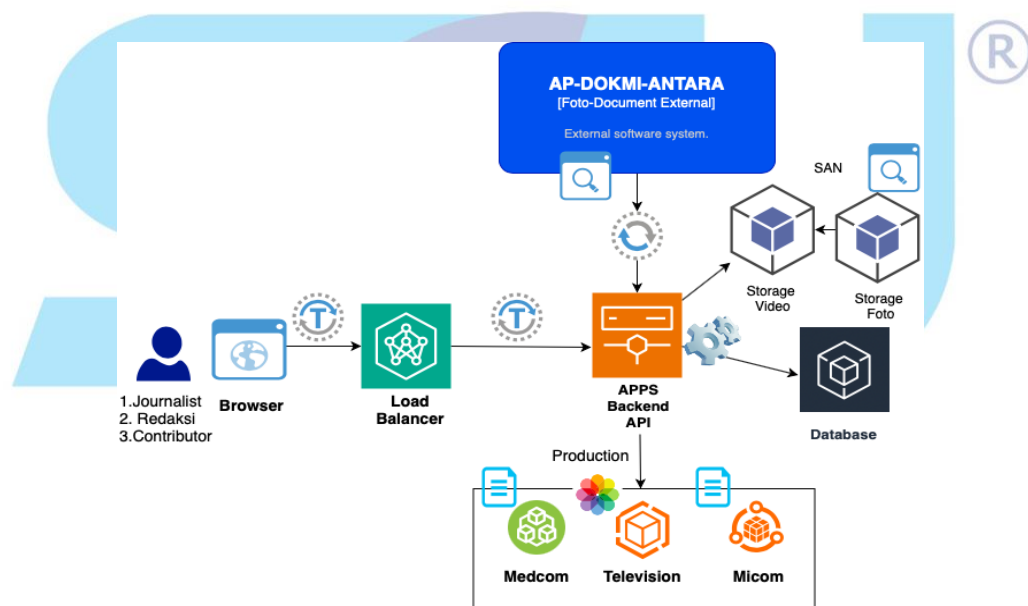


Figure 2.2. System Architecture CMS Newsbox

2.3.3. The Role of Infrastructure in CMS Operations.

IT infrastructure operations in the Content Management System (CMS) in television companies involve the management and maintenance of physical and digital components that support the production, storage and distribution of content. Based on figure 2.2. system architecture CMS, the infrastructure includes servers, networks, data storage systems, and software needed to run CMS. The IT team is responsible for

ensuring that all of these components function optimally, including carrying out routine maintenance, software updates, and monitoring system performance. Reliable infrastructure is very important to ensure operational smoothness, especially in a television production environment that requires high speed and reliability.

One key aspect of IT infrastructure operations is the availability of data storage management. The television companies must store and manage enormous volumes of data, including high quality videos, audio, metadata, and other digital assets from the coverage of journalists. The storage infrastructure used often involves the Network Attached Storage (NAS) or Storage Area Network (SAN) system, which provides large capacity and fast access to data. The IT team must ensure that this storage system can be discharged and has adequate backups to prevent data loss and ensure rapid recovery in the event of system failure.

IT infrastructure security is also a top priority in CMS operations in television companies. According to (Zuboff, 2022), unsafe IT infrastructure can be the target of cyber attacks, which can cause broadcast disorders, and financial losses due to CMS services off. The IT team must implement strong security measures, such as firewalls, intrusion detection systems (Intrusion Detection Systems or IDS), and data encryption. In addition, real time security monitoring and routine updates to security patches are very important to protect infrastructure from growing cyber threats.

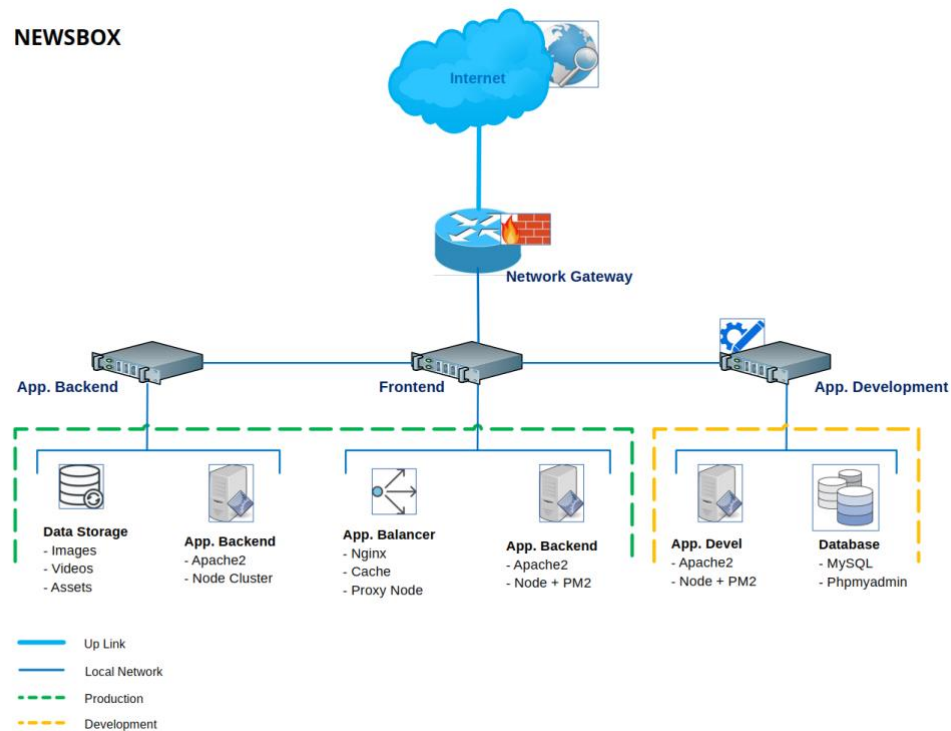


Figure 2.2. Network Architecture CMS Newsbox.

On Figure 2.2 there are several services found in CMS system, namely load balancer, App backend API, data storage, external source third party and database system. This CMS system is divided into two systems, namely the frontend application (load balancer) and the backend application (API). In addition there is also a server development that is used for the development of the system. This application is built with vmware virtualization technology with 2 vm hosts with IP public NAT to ip private. Domain system is <https://newsbox.mediagrounetwork.com>

2.3.4.Challenge CMS.

One of the main challenges of the Content Management System (CMS) specifically for television media is to manage a very large data volume. According to (Lotz and Potter, 2022), television stations must store and manage thousands of hours of content, including video, audio, metadata, and other related assets. This requires strong and scalable storage infrastructure, such as cloud computing, but high costs and technical complexity are often obstacles. In addition, managing metadata consistently and accurately to facilitate the search and collection of content is a challenge, especially when content comes from various sources and formats.

Integration with other systems and platforms is also a significant challenge for television media CMS. The television stations need to connect their CMS with various distribution platforms, such as IPTV, OTT, and social media, as well as analytic tools and advertising systems. This integration process is often complicated because of differences in technological standards and communication protocols. In addition, CMS must be able to adapt to the development of new technology.

Data security is another challenge that should not be ignored. According to (Barker, 2016), CMS Television media holds large amounts of sensitive data, including content entitled, user information, and operational data. Cyber threats, such as hacking and data leakage, can cause financial losses and significant reputation. Therefore, CMS must be equipped with strong security features, such as data encryption, multi-factor authentication, and real-time security monitoring. However, the implementation of these security measures often requires large investments and high technical expertise.

The last challenge is to ensure CMS can support dynamic and complex operational needs. The television stations often have to produce and distribute content in a short time, especially for live broadcasts or special events. CMS must be able to handle this pressure by providing a user-friendly interface and features that allow team collaboration efficiently. In addition, CMS must be able to accommodate various content and device formats, while ensuring the quality and consistency of the content produced. This challenge requires a flexible CMS design and continues to be updated to meet the demands of the growing media industry.

Based on figure 1.2, the media platform (CMS) faces a high risk of cyberattacks and potential data breaches, stemming from several key vulnerabilities in its design, implementation, and ongoing management. These issues collectively make it easily attackable and place valuable company assets at significant risk.

There are the key and detailed problems concerning the cyber vulnerability of the media platform (CMS) PT XYZ :

1. Inherent Design and Development Flaws.

The application was built in-house without adhering to established security standards. This fundamental lack of secure development practices makes the entire system inherently prone to cyberattacks from its foundation.

2. Outdated Systems and Lack of Auditing.

There is a deficit in system audits. Without regular security checks, vulnerabilities can persist undetected. The platform relies on old, unupdated technology and systems. This critical weakness makes the system easily attackable, as outdated software often contains known security flaws that have not been patched.

3. Broad Accessibility and Exposure of Assets.

The application is accessible to both internal journalists and the general public. This wide accessibility significantly broadens its potential attack surface, increasing the opportunities for malicious actors to attempt breaches.

The platform contains important company assets, including news content, video, and photos. These valuable assets are specifically highlighted as being vulnerable to theft.

4. Vulnerabilities from External Third-Party Integrations.

The platform includes integrations with external third-party systems such as Associate Pers, DOKMI, and storage. These integrations introduce additional points of vulnerability, meaning that data can be stolen through these external connections.

5. Susceptibility to Specific Attack Types.

The platform is specifically susceptible to various common cyberattacks. These include:

- a. SQL injection, which can allow attackers to manipulate or steal data from databases.
- b. Cross-site scripting (XSS), which can enable attackers to inject malicious scripts into web pages viewed by other users.
- c. The uploading of malicious content, which could allow attackers to execute harmful code or spread malware through the platform.
- d. DDoS, can cause broadcast service disruptions by overwhelming network infrastructure and cause operational stop.

6. Risk of User Credential Compromise.

User credentials are at significant risk of being stolen or leaked. The compromise of credentials could grant unauthorized access to sensitive parts of the platform or to user accounts, leading to further breaches or data theft.

Based on CMS problems above, effective risk management is essential to protect media platforms from cyber threats and prevent potentially damaging data breaches. Without a structured approach to identifying, assessing, and mitigating risk, platforms remain highly vulnerable to attacks that can compromise sensitive company assets, disrupt operations, and damage reputations. Cybercriminals are increasingly targeting weak systems, and outdated platform technology, lack of security audits, and insecure third-party integrations make them attractive targets. Risk management ensures that vulnerabilities are proactively addressed, security controls are strengthened, and incident response plans are in place to minimize damage in the event of a breach.

Furthermore, risk management helps prioritize security investments, ensuring resources are allocated to the most critical threats first. Given the platform's exposure to SQL injection, XSS attacks, and credential theft, a risk-based approach will enforce secure coding practices, regular patch updates, and multi-layered authentication. Compliance with industry security standards can also be achieved through systematic risk assessment. Without risk management, organizations are operating blindly, leaving loopholes that attackers can exploit, potentially resulting in financial losses, legal ramifications, and loss of user trust. Implementing a robust risk management framework is not just a precautionary measure; it is a necessity to maintain platform integrity and ensure long term operational resilience.

2.4.Risk Management.

Risk management on television media involves identification, assessment, and risk mitigation that can affect operational, reputation, and finance of television stations. According to (Santos and de Oliveira, 2019), one of the main risks is technical failures, such as broadcast disorders or damage to production equipment, which can result in downtime and loss of advertising income. To overcome this, television stations need to implement a backup system and disaster recovery plan (disaster recovery plan). In

addition, routine maintenance and technical staff training are also important to minimize the risk of operational failure.

Cyber security is another challenge that requires careful risk management. The television stations store large amounts of sensitive data, including content entitled, user information, and operational data. Cyber threats, such as hacking and data leakage, can cause financial losses and significant reputation. To overcome this, television stations need to implement strong security measures, such as data encryption, multi-factor authentication, and real-time security monitoring. In addition, cyber security awareness training for staff is also important to reduce the risk of cyber attacks.

Risk of reputation is also an important aspect in television media risk management. (Chalaby, 2018) explains that incompatible or controversial content can trigger negative reactions from the public and damage the reputation of television stations. To manage this risk, television stations need to have a strict protocol to review and approve content before being broadcast. In addition, having an effective crisis communication plan can help television stations respond quickly and precisely to the problems that arise, thereby minimizing the negative impact on reputation. With a proactive approach in risk management, television stations can protect their operations and maintain public confidence.

2.4.1.Risk Management Framework.

Cybersecurity risk management framework (cyber security risk management) is a structured approach to identify, assess, and reduce risks associated with cyber threats. According to (NIST, 2018) (National Institute of Standards and Technology) in its publication for improvement of critical infrastructure cybersecurity, this framework consists of five core functions: identification, protection, detection, response, and recovery. The identification function involves an understanding of the assets, systems, data, and organizational ability to manage cyber risk. This step is important to determine priority and focus on cyber security efforts, because not all assets have the same level of risk.

Protection Function within the Siber Risk Management Framework aims to implement steps that can reduce the possibility or impact of cyber attacks. According to ISO/IEC 27001 (2013), these steps include data encryption, access management, security awareness training for employees, and maintenance of security systems such as firewalls and antivirus. Protection also involves the development of clear security policies and procedures to ensure that all members of the organization understand their role in maintaining cyber security. With these steps, the organization can build strong defense against cyber threats.

The detection function within the cyber risk management framework focuses on identifying threats and security incidents quickly. According to the (Bhole, Sauter and Kastner, 2025), early detection is very important to minimize the impact of cyber attacks. Technology such as the Intrusion Detection Systems (IDS), network monitoring in real-time, and log analysis can help identify suspicious activity before developing into a large incident. In addition, the organization needs to have a Security Operations Center (SOC) team that is ready to monitor and respond to the 24/7 cyber threat. Effective detection allows the organization to take quick action before damage occurs.

Response and recovery function within the Siber risk management framework aims to deal with security incidents and restore operations as quickly as possible. According to (Nelson *et al.*, 2025) in the NIST Special Publication 800-61, the response involves steps such as the isolation of infected systems, forensic analysis, and communication with related parties. Meanwhile, recovery includes data recovery, system improvement, and post-incident evaluation to prevent the recurrence of similar events. With a structured response and recovery plan, the organization can reduce downtime and financial losses caused by cyber attacks. The comprehensive cyber risk management framework ensures that the organization is ready to face the growing cyber threat.

2.4.2.Risk Assessment.

NIST Special Publication (SP) 800-30 Revision 1 provides a risk assessment of comprehensive cyber security. According to (Nelson *et al.*, 2025), this framework is designed to help the organization identify, analyze, and evaluate risks associated with operational information systems and digital assets. The risk assessment process begins

with the identification of critical assets, potential threats, and vulnerability that may be exploited. After that, the organization assesses the impact and possibility of the risk, which is then used to determine the level of risk. This approach allows the organization to prioritize risks based on the severity and allocate resources effectively for mitigation.

The NIST SP 800-30 Rev1 framework consists of six key steps: (1) preparing for the risk assessment, (2) conducting the risk assessment, (3) communicating the risk assessment results, (4) maintaining the risk assessment, (5) responding to risk, and (6) monitoring risk over time (NIST, 2012). By following this framework, media organizations can gain a comprehensive understanding of their cybersecurity posture, prioritize risk mitigation efforts, and implement effective security controls to protect their information technology (IT).

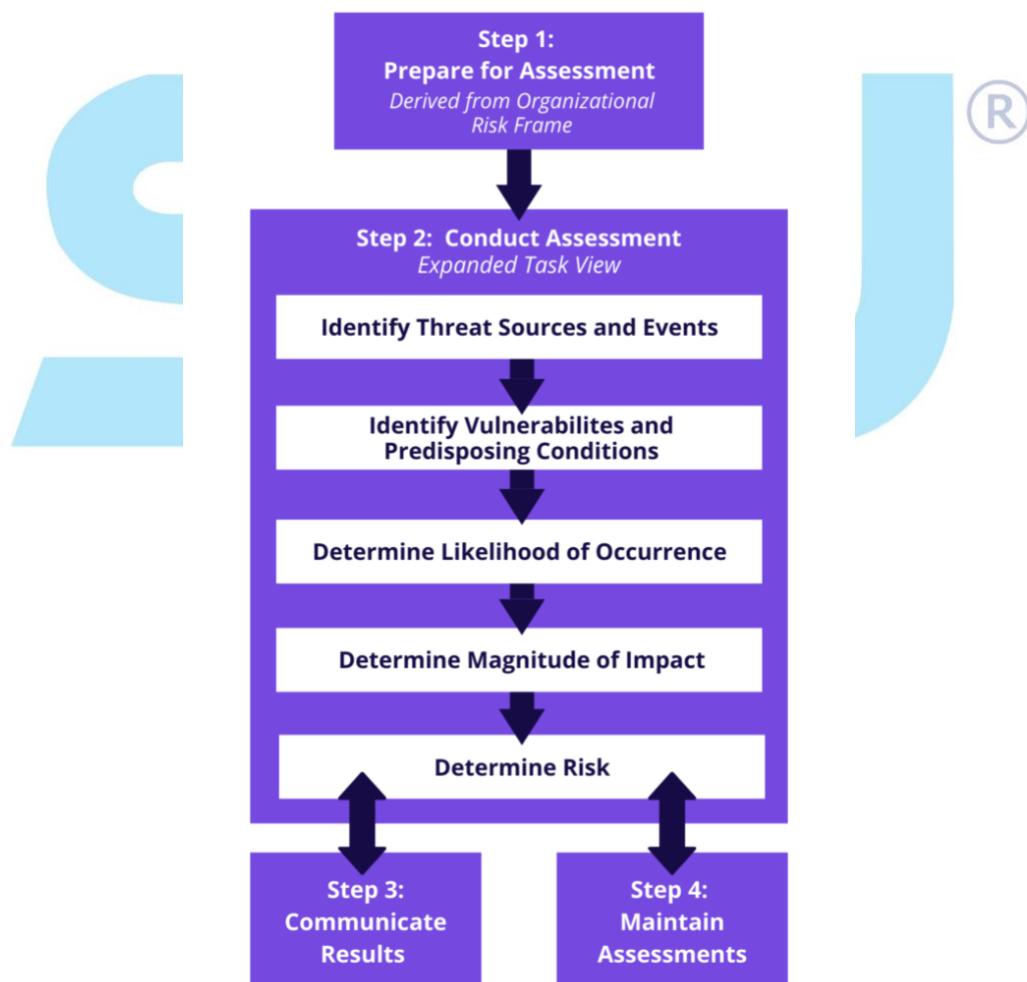


Figure 2.3. NIST SP 800-30 Rev1 Framework.(NIST,2018)

Base on figure 2.3., The NIST SP 800-30 Rev1 framework also emphasizes the importance of communication and documentation in the risk assessment process. According to (NIST, 2012), the results of the risk assessment must be communicated to the main stakeholders, including senior management, to ensure that mitigation decisions are organizational supported. In addition, detailed documentation of the assessment process, findings and mitigation recommendations is very important to ensure transparency and accountability. This framework is iterative, meaning that the risk assessment must be carried out regularly to accommodate changes in the environment of the threat, technology, and operations of the organization. By following this framework, the organization can build a proactive and structured approach in managing cyber security risks.

2.4.3. Threat.

Threats in cyber security refer to potential hazards that can exploit vulnerability in information systems or networks, causing damage, disruption, or loss. According to NIST (National Institute of Standards and Technology) in SP 800-30 Rev1 (2012), threats can come from various sources, including hackers, malware, phishing attacks, and even human errors. This threat can be external, such as attacks from evil actors outside the organization, or internal, such as employees who are accidentally or intentionally endanger the system. Cyber threats continue to develop along with technological advances, making it more difficult to detect and overcome.

One of the most common cyber threats is malware, dangerous software designed to damage, interfere, or get invalid access to a computer system. According to Symantec (2021), malware includes viruses, worms, trojans, ransomware, and spyware, which can spread via email, downloads, or infected websites. Ransomware, for example, encrypts victims of data and requests a ransom to restore access, causing significant financial and operational losses. This threat is increasingly sophisticated with the use of obfuscation and encryption techniques, making it more difficult to detect by traditional antivirus software.

Cyber threats also include distributed denial of service (DDOS) attacks, which aim to disrupt services by flooding servers or networks with fake traffic. According to

(NSFOCUS, 2024), DDOS attacks can paralyze websites, applications, or online services, causing expensive downtime and damage the reputation of the organization. In addition, cyber threats can also come from within the organization, such as employees who are dissatisfied or careless who can leak sensitive information or deliberately damage the system. To overcome this threat, the organization needs to adopt a holistic cyber security approach, including training in security awareness, sophisticated threat detection technology, and an effective incident response plan.

In the context of threat modeling, threats are defined as potential hazards or attacks that can exploit vulnerability in a system, causing damage, disruption, or loss. According to (Shostack, 2014) in his book *Threat Modeling: Designing for Security*, threats are key elements in the threat modeling process because it helps identify and understand how attackers can target the system. Threats can come from various sources, including evil actors such as hackers, insider threat (threats from within the organization), or even natural disasters. The main purpose of identifying threats is to predict and mitigate risk before they can be exploited.

Threats in the modeling threat are not static; They continue to develop along with changes in technology and attacker tactics. According to (Eckhart *et al.*, 2019) in *The Security Development Lifecycle*, new threats continue to emerge, such as zero-day attacks that exploit unknown vulnerability. Therefore, threat modeling must be a sustainable and iterative process, where new threats are identified and assessed regularly. By understanding and anticipating threats, organizations can build a safer and tougher system to cyber attacks.

2.4.4.Vulnerability.

Vulnerability in the context of cyber security refers to weaknesses or defects in systems, networks, or applications that can be exploited by threats to cause damage or disturbance. According to NIST (National Institute of Standards and Technology) in SP 800-30 Rev1 (2012), vulnerability can emerge from various sources, including configuration errors, software bugs, or unsafe system design. This vulnerability can be found in various layers of technology, ranging from hardware, operating systems,

applications, to network protocols. Identification and vulnerability mitigation is an important step in reducing cyber security risks.

Vulnerability is often classified by type and impact. According to the Common Vulnerability and Exposures (CVE) database, vulnerability can include buffer overflows, SQL injection, Cross-Site Scripting (XSS), and Misconfigurations. For example, SQL Injection is a vulnerability that allows the attacker to insert a dangerous SQL code into the database query, so that it can access or manipulate sensitive data. Vulnerability like this can have a significant impact, including data violations, information theft, and service disruption. Therefore, it is important to routinely scan vulnerability scanning to identify and improve this weakness.

The vulnerability management process involves identification, assessment, and vulnerability mitigation. According to ISO/IEC 27001 (2013), the organization must implement a vulnerability management program that includes regular scanning, risk assessment, and the application of patch or security renewal. Tools such as nessus, QUALYS, and OPENVAS are often used to scan vulnerability and produce detailed reports about the weaknesses found. In addition, the organization must have a clear process to prioritize and improve vulnerability based on the severity and potential impact.

Vulnerability is not only limited to technical aspects, but can also involve human factors. Human errors such as the use of a weak password, click on the phishing link, or failure to follow the security protocol can create vulnerability exploited by the attacker. Therefore, cyber security awareness training for employees is an important component in reducing vulnerability. With a holistic approach that includes technical and human aspects, organizations can effectively reduce risks associated with vulnerability and increase their cyber security posture.

2.4.5. Security Gap Analysis.

In the context of threat model risk management research on Content Management System (CMS) applications, security gap analysis plays a very important role as a bridge between the actual security conditions of the system and the security conditions that

should be implemented. Security gap refers to the gap between existing security controls and controls recommended by industry standards, such as OWASP Top 10 or CIS Controls. Identifying these gaps allows researchers to systematically reveal vulnerabilities in the CMS architecture that have not been adequately protected. For example, a CMS may have a basic login system, but is not equipped with brute force protection or multi-factor authentication, thus posing a significant risk of credential exploitation.(Tudela *et al.*, 2020)

Security gap analysis serves not only as a diagnostic tool but also as a strategic basis for risk mitigation planning. By comparing real systems with ideal security frameworks, researchers can determine the most urgent security control priorities to be implemented (Shostack, 2014). It also helps in evaluating residual risk, which is the risk that remains even though some controls have been implemented, and provides technical and managerial justification in choosing a mitigation strategy or risk acceptance (ISO/IEC 27005:2018). In addition, security gap analysis supports the threat modeling process to be more contextual and factual, because the threat model is based on actual vulnerability maps and not just design assumptions (Ucedavélez and Morana, 2015). The output of this analysis is also very useful in communicating risks to non-technical stakeholders, because it can be presented in a visual or tabular format that shows the relationship between threats, existing controls, detected gaps, and recommendations for improvement.

Thus, security gap analysis is a crucial stage in the risk-centric threat modeling approach, especially in CMS systems that are often exposed to various cyber attack vectors. The existence of security gaps that are not systematically identified can cause organizations to have a false perception of the security of their systems, making them vulnerable to incidents that are detrimental operationally and reputationally.

2.5.Risk.

Risk in the context of cybersecurity refers to the potential loss or negative impact that can occur due to the exploitation of vulnerabilities by threats. According to NIST (National Institute of Standards and Technology) in SP 800-30 Rev1 (2012), risk results from a combination of the possibility of a threat occurring and the impact it causes if

the threat successfully exploits the vulnerability. This risk can affect an organization's assets, including data, systems, reputation, and operations. Therefore, risk management is an important process for identifying, assessing, and reducing risk to an acceptable level.

Threats are one of the key components in the risk equation. According to Shostack (2014) in his book *Threat Modeling: Designing for Security*, a threat is an entity or event that has the potential to cause damage to a system or asset. Threats can come from various sources, such as hackers, malware, natural disasters, or even human error. These threats can be external, such as cyber attacks from outside the organization, or internal, such as careless or disgruntled employees. Threats are the factors that trigger risk, but without vulnerabilities, threats cannot cause harm.

Vulnerabilities are another important component of the risk equation. According to ISO/IEC 27001 (2013), a vulnerability is a weakness or flaw in a system, network, or application that can be exploited by a threat. Vulnerabilities can arise from a variety of sources, including misconfigurations, software bugs, or insecure system designs. Examples of vulnerabilities include buffer overflows, SQL injection, and misconfigurations. Vulnerabilities are the entry points for threats to cause harm, and without vulnerabilities, there is no risk.

The relationship between risk, threats, and vulnerabilities can be described by a simple risk equation: $\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$. According to (NIST, 2012), risk increases if there is a threat that has the ability to exploit the vulnerability, and if the impact of that exploitation is significant. For example, if a system has vulnerabilities that can be exploited by threats such as malware, and the impact is a severe data breach, then the resulting risk will be high. Therefore, reducing risk can be done by mitigating threats, fixing vulnerabilities, or reducing potential impacts.

Risk management involves steps to identify, assess, and mitigate risks. According to (Cichonski *et al.*, 2012) in NIST SP 800-61, the first step is to identify assets, threats, and vulnerabilities. After that, the risk is assessed based on the likelihood of occurrence and the impact it causes. The final step is to implement security controls to mitigate the

risk, such as fixing vulnerabilities, increasing security awareness, or adopting threat detection technology. This approach ensures that risks are managed proactively and continuously.

According to the Verizon Data Breach Investigations Report (2021), cyber threats continue to become more sophisticated, while new vulnerabilities continue to be discovered as technology advances. Therefore, risk management must be an ongoing and iterative process, where new threats and vulnerabilities are identified and assessed periodically. By understanding the relationship between risks, threats, and vulnerabilities, organizations can develop effective security strategies to protect their assets and minimize potential impacts.

2.5.1. Risk Mitigation

The ISO/IEC 27001:2013 framework is an international standard that provides a structured approach to information security risk management. According to (Malatji, 2023) in *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*, this framework aims to identify, assess, and mitigate risks associated with an organization's information assets. ISO 27001:2022 emphasizes the importance of a risk-based approach, where organizations must proactively identify threats and vulnerabilities that can affect the confidentiality, integrity, and availability of information. This process begins with determining the scope of the information security management system (ISMS) and identifying critical assets that need to be protected.

Once assets are identified, the next step is to conduct a risk assessment. According to (Malatji, 2023) in *Information Security Risk Analysis*, ISO 27001:2022 guides organizations to evaluate the likelihood and impact of each identified risk. This assessment involves analyzing threats, vulnerabilities, and potential impacts on the organization's operations. Based on the assessment results, risks are then prioritized, and mitigation measures are designed to reduce the risks to an acceptable level. Security controls recommended by ISO 27001:2022 include technical, physical, and administrative measures, such as data encryption, access management, and security awareness training for employees.

Implementation of security controls and risk mitigation is at the heart of the ISO 27001:2022 framework. According to (Humphreys, 2007) in *Implementing the ISO/IEC 27001 Information Security Management System Standard*, organizations must ensure that the selected controls are effective in reducing risks and are in line with business needs. In addition, ISO 27001:2022 emphasizes the importance of periodic monitoring and review of the ISMS to ensure that controls remain relevant and effective in the face of changing threat environments. By adopting this framework, organizations can build a sustainable risk management system, ensure the protection of information assets, and support operational continuity.

In (Fonseca, Vieira and Madeira, 2014) with title *Web Security Vulnerability Analysis*, OWASP TOP 10 is a standard published by the OWASP community that contains a top ten list of vulnerabilities that can compromise web security . As for the list of 10 vulnerabilities based on the OWASP Top 10 2021 guide shown in figure 2.4 below :



Figure. 2.4. OWASP Top 10 List 2021.(Tudela *et al.*, 2020)

Mitigation against the OWASP Top 10 2021 is a crucial step in reducing the level of risk and minimizing vulnerability exposure in Content Management Systems (CMS), considering that CMS is often the target of attacks due to its open, modular, and widely used nature. Vulnerabilities such as Broken Access Control, Cryptographic Failures, and Injection listed in the OWASP Top 10 2021 have been proven to be frequently exploited to gain unauthorized access, steal data, or take over CMS systems (OWASP, 2021). Implementing OWASP Top 10 based security controls can help organizations identify mitigation priorities that have a significant impact on reducing cyber risk.

2.6. Combine Risk Management and Threat Modeling Framework.

Risk Management Framework (RMF) and Threat Modeling Framework are two complementary approaches to cybersecurity management. RMF, as described in NIST SP800-37 Rev. 2, provides a systematic framework for categorizing information systems, selecting and implementing security controls, conducting risk assessments, obtaining authorizations, and conducting ongoing monitoring based on the organization's risk level (NIST, 2012) Meanwhile, Threat Modeling with the popular STRIDE method focuses on mapping system components and data flows to identify and prioritize threat scenarios (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege) along with specific mitigation recommendations (Shostack, 2014).

The integration of these two frameworks is seen when the output of Threat Modeling (a detailed list of threat scenarios and estimates of their likelihood and impact) is used as the main input in the RMF Risk Assessment phase, so that risk probability and impact analysis can be carried out more accurately and measurably. Thus, Threat Modeling not only enriches the risk identification and analysis process in RMF, but also ensures that the designed controls focus on the highest threats throughout the information system life cycle.

This is a comparative table mapping key phases of a generic Risk Management Framework (e.g., ISO27005 / NIST SP 800-30) to corresponding activities in a Threat Modeling Framework STRIDE/DREAD :

Table. 2.1. Comparative mapping RMF to Threat Model.

Risk Management Framework	Threat Modeling Activity.	Relationship
1. Establish Context	Define system scope & boundaries.	Threat modeling uses these boundaries to draw data-flow diagrams and identify assets.
2. Risk Identification	Enumerate assets & trust boundaries. Identify potential threat agents & goals.	Threat models produce concrete threat scenarios.
3. Risk Analysis	Analyze threat paths & attacker techniques.	Likelihood & impact estimates are informed by attack method and exploitation feasibility.
4. Risk Evaluation	Prioritize threats by severity & exploitability.	Threat priority mapping (e.g., STRIDE severity, DREAD risk score) feeds back into risk ranking.
5. Risk Treatment	Propose and design mitigations (controls)	Mitigation actions (e.g., input validation, auth checks) directly address modeled threats.
6. Monitoring & Review	Update threat model with changes & new findings	Ongoing threat-model updates ensure risk register stays current as the system evolves.

With the relationship between risk management and threat models in accordance with table 2.1, this research conducted risk management with a threat model approach so that the analysis of the probability and magnitude of the risk impact in this research can be carried out more accurately and measurably.

2.7. Threat Modeling.

Threat modeling is a systematic process for identifying, categorizing, and prioritizing threats to a system or application. According to (Shostack, 2014) in his book *Threat Modeling: Designing for Security*, the main purpose of threat modeling is to understand how threats can affect a system and develop strategies to reduce the associated risks. This process involves an in-depth analysis of the system architecture, data flow, and interactions between system components. By conducting threat modeling, organizations can identify potential vulnerabilities before they are exploited by attackers.

The main purpose of threat modeling is to identify and understand potential threats to a system or application, so that organizations can develop effective mitigation strategies. According to (Shostack, 2014) in his book *Threat Modeling: Designing for Security*, this process helps security teams map how threats can exploit vulnerabilities in the system, as well as assess the potential impact that can be caused. By understanding threats early on, organizations can design more secure systems and reduce cybersecurity risks before the system is implemented or used.

In addition, threat modeling aims to prioritize threats based on their severity and likelihood of occurrence, so that security resources can be allocated efficiently. According to (Casola *et al.*, 2024) in *The Security Development Lifecycle*, threat modeling allows organizations to focus on the most critical threats and develop appropriate security controls, such as strong authentication, data encryption, or intrusion detection systems. Thus, threat modeling not only improves system security but also helps organizations comply with security regulations and standards, and protect their assets and reputations from cyber attacks.



Figure 2.5. Threat Model Process.(Shostack, 2014)

On figure 2.5 ,the threat model has several steps, namely

1. Identify Assets
2. Architecture Review.
3. Decompose the application or infrastructure.
4. Determine the threats.
5. Determine countermeasures and mitigations.
6. Rank the threats.

The threat modeling process is a foundational technique in cybersecurity risk management, especially in systems such as Content Management Systems (CMS) that handle critical data and user interactions. The methodology commonly comprises six essential steps that guide analysts in identifying and mitigating security threats in a structured manner. The first step, *Identify Assets*, focuses on enumerating all valuable components within the system, including sensitive data, system modules, and operational workflows. This helps establish what needs to be protected and the potential impact if an asset is compromised (Shostack, 2014).

The second step, *Architecture Review*, involves analyzing the system's structural blueprint, including its components, data flows, and trust boundaries. This architectural insight is critical in understanding how information traverses the system and where potential vulnerabilities might exist (Myagmar, Lee and Yurcik, 2005). The next phase, *Decompose the Application or Infrastructure*, breaks the system into discrete modules such as web servers, databases, and external APIs. This granular decomposition identifies entry and exit points, which are vital for mapping out attack surfaces and vectors.

In the fourth step, *Determine the Threats*, threat modeling techniques such as STRIDE or attack trees are employed to identify security threats that may exploit weaknesses in the system. Each threat is mapped to system components, ensuring comprehensive threat coverage. Following this, the *Determine Countermeasures and Mitigations* phase proposes appropriate security controls for each identified threat. These may include input validation, access control, encryption, or anomaly detection, aiming to either eliminate or reduce the impact and likelihood of exploitation (Shostack, 2014).

Finally, the sixth step, *Rank the Threats*, prioritizes identified threats using scoring methodologies such as DREAD or CVSS (Common Vulnerability Scoring System). This prioritization allows security teams to focus their resources on mitigating the most critical threats first, based on factors like exploitability, impact, and exposure within the operational environment.(Kim, Kim and Kim, 2022)

The stages above can be summarized in table 2.2, namely based on steps, focus and outcomes.

Table 2.2. Summary Threat Modeling Step.

Step	Focus	Outcome
1. Identify Assets	Determine what to protect	Asset inventory
2. Architecture Review	Understand system structure	High-level diagram
3. Decompose System	Detail how components interact	Entry points, data flows
4. Determine Threats	Find potential attack vectors	Threat list
5. Mitigations	Define how to reduce risks	Security controls
6. Rank Threats	Prioritize threats	Risk matrix or score

2.7.1.Data Flow Diagram.

Data Flow Diagram (DFD) is a visual representation that illustrates the flow of data in a system, including how data is processed, stored, and transferred between system components. According to (Shostack, 2014) in his book *Threat Modeling: Designing for Security*, DFD consists of several main elements, such as external entities (users or other systems), processes (activities that process data), data storage (databases or files), and data flows (data movement paths).

A Data Flow Diagram is a graphical representation that depicts the flow of data within a system and the processes that transform this data. It is a high-level architecture model that provides a visual understanding of how data moves between different components within a system (Sion *et al.*, 2018). Here list of components of a DFD :

1. Entities : External actors that interact with the system.

2. Processes : Operations that transform incoming data into outgoing data.
3. Data Stores : Repositories where data is stored.
4. Data Flows : Arrows indicating the direction of data movement.

Apart from having several components, Data Flow Diagrams (DFD) also come in various levels which show different levels of complexity in the diagrams created. These levels are categorized into Level 0, Level 1, Level 2, and Level 3. The following is a comparative analysis of each level can see on Table 2.3 for more detail.

Table 2.3. Level of Data Flow Diagram. (Shostack, 2014)

Level	Description	Use Case
Level 0 (Context layer)	Offers a high-level overview of the system, depicting it as a singular process along with its interactions with external components.	Initial stage of system analysis to provide a general overview.
Level 1 (Process layer)	Breaks down the single process in Level 0 into sub-processes.	Detailed analysis of system components and data flows.
Level 2 (Subprocess layer)	Further decomposes the processes in Level 1 into more detailed activities.	Complex systems requiring a granular understanding of data flows and transformations.
Level 3 (Lower-level layer)	Provides a meticulous process taxonomy, characteristically detailing task-level components and their operational relationships.	Complex architectures requiring granular decomposition to facilitate comprehensive comprehension and systematic examination.

In threat modeling, DFD functions as a tool to understand how data moves through the system and where potential threats can occur. According to (Howard and Lipner, 2006) in The Security Development Lifecycle, DFD helps security teams identify system components that interact with sensitive data, such as data entry points, processing processes, and data storage. By visualizing data flow, teams can more easily find vulnerabilities that might be exploited by threats, such as data leaks or man-in-the-middle attacks.

The main purpose of using DFD in threat modeling is to map and analyze security risks associated with data flows. According to (Ucedavélez and Morana, 2015) in Risk Centric Threat Modeling, DFD allows security teams to see holistically how data moves through the system and where critical points require additional protection. For example, if the DFD shows that sensitive data passes through an unencrypted network, the team can identify the risk and implement encryption to mitigate the threat.

DFD also helps in communicating security risks to non-technical stakeholders. According to Ross et al. (2012) in NIST SP 800-160, the visualization provided by DFD makes it easier to understand how threats can affect the system and why certain mitigation steps are needed. By using DFD, security teams can clearly explain to management or development teams about areas that require special attention, so that decisions about resource allocation and security priorities can be made more informed.

Therefore, DFD is a very important tool in threat modeling because it provides a clear picture of the data flow and interactions between system components. According to (Shostack, 2014), DFD not only helps identify threats and vulnerabilities but also ensures that security measures are implemented at the most critical points. By using DFD, organizations can build systems that are more secure and resilient to cyber attacks, while ensuring compliance with applicable security standards and regulations.

2.7.2. Threat Modeling Approach.

Threat modeling is a systematic approach used to identify, measure, and address security risks in an application or system. This method helps in analyzing potential

threats and evaluating their vulnerabilities, so that it can be used as a basis for planning an effective security strategy.

According to Shostack (2014), threat modeling acts as a guide for developers and security professionals to understand the various threats that may occur. With this approach, they can design appropriate mitigation steps to reduce risks and increase protection for the systems or applications being developed.

2.7.2.1.Asset Centric.

The Asset-Centric approach to threat modeling focuses on an organization's critical assets, such as sensitive data, systems, and infrastructure, as explained by Shostack (2014). This method aims to identify and prioritize threats and vulnerabilities that could impact these valuable assets. By understanding the associated risks, organizations can take more effective protective measures.

This approach is very useful for organizations that already have a clear understanding of their most important assets and want to ensure optimal protection. In threat modeling, the term asset is generally used in three main contexts: something that an attacker is targeting, something that an organization wants to protect, and the means by which either of these objectives can be achieved.

2.7.2.2.Attacker Centric.

The Attacker-Centric approach focuses on understanding the mindset, tactics, and potential goals of attackers. According to Shostack (2014), this method is very important because it allows organizations to anticipate and prepare for various attack strategies, thereby increasing their defense capabilities. By analyzing possible attack paths, techniques applied, and attacker goals, organizations can identify security gaps and weaknesses that are at risk of being exploited.

This approach involves simulating attack scenarios, analyzing attack vectors, and understanding the motivations and capabilities of attackers. These insights help in designing and implementing effective security measures to deal with potential threats.

Thus, organizations can be better prepared to protect their systems from breaches and intrusions that can compromise their data and infrastructure.

2.7.2.3. Software Centric.

The Software-Centric approach focuses on identifying and addressing threats that specifically target software and applications. According to Shostack (2014), because vulnerabilities in software are often the primary entry point for cyberattacks, this approach examines the design, architecture, and code of a program to find potential weaknesses.

This process includes a thorough code review, software architecture analysis, and the use of automated tools to detect security holes. By identifying and fixing software vulnerabilities early in development, organizations can prevent exploitation of these vulnerabilities, thereby increasing the security and reliability of the applications they develop.

2.7.2.4. Risk Centric.

The Risk-Centric approach focuses on mapping threats based on the level of risk they pose to the organization. According to (Ucedavélez and Morana, 2015), this approach is essential to ensure that security resources and efforts are focused on the most significant threats, thus providing optimal protection for the organization.

This method includes a comprehensive risk assessment, which involves identifying, analyzing, and prioritizing threats and vulnerabilities based on factors such as likelihood of occurrence and impact. By understanding the risk landscape, organizations can design more targeted and effective mitigation strategies. This ensures that high-risk vulnerabilities are addressed promptly, and that the security controls implemented are aligned with the organization's risk tolerance and business objectives.

2.7.3. Threat Modeling Framework.

Threat modeling frameworks provide a structured method for identifying, assessing, and mitigating security threats in software and systems. These frameworks help security analysts in carrying out a systematic process to evaluate the security posture of an application or system.

In the field of cybersecurity, there are various frameworks specifically designed for threat modeling. These frameworks serve as a methodological approach in detecting, analyzing, and handling security threats. As shown in Table 2.4, a comparison between these frameworks is presented to provide in-depth insight into the capabilities and limitations of each approach.

Tabel 2.4. Comparison Threat Model.(Shotack,2014)

No	TM	Characteristics	Type	Use Case	Limitations
1	STRIDE	Concentrates on six types of security threats.	Software Centric	Security threat modeling in software development and system architecture.	Be time-intensive and may generate false positives or negatives.
2	LINDDUN	Addresses seven categories of privacy concerns.	Software centric	Systems handling sensitive personal data.	Complexity and time-consuming.
3	PnG	Prioritizes security throughout the software development lifecycle.	Software centric	Software development environments.	Focus on the motivation and skill human attacker.
4	PASTA	Seven-stage process, risk-centric	Risk centric	Aligning security efforts with business risk	Resource-intensive and time-consuming.
5	DREAD	Five categories for risk assessment.	Risk centric	Assessing and prioritizing security threats.	Subjectivity leading inconsistent risk scoring.
6	CVSS	Standardized vulnerability scoring by NIST.	Risk centric	Vulnerability management programs	Limited to vulnerability scoring.

No	TM	Characteristics	Type	Use Case	Limitations
7	Security Cards	Tool for Identifying security and privacy risks.	Asset centric	Initial phases of software design and development.	Limited brainstorming and ideation
8	ATTACK TREES	Hierarchical visualization of attack paths.	Attacker centric	Network security and system security analysis.	Complexity and time cons
9	hTMM	Combination method SQUARE , Security Cards and PnG.	Attack Centric	Security assessment of software applications, networks, and systems.	Can be time consuming due to its hybrid nature.
10	Quantitative TMM	Hybrid Method consist of Attack trees, STRIDE, CVSS.	Risk Centric	Risk-based decision-making in cybersecurity and IT governance.	Predictions may not always reflect real-world scenarios due to changing threat landscapes.
11	VAST	Base on threat modeler, automated threat modelling platform.	Software Centric	Its scalability and usability in large organizations.	Complexity and time consuming.
12	OCTAVE	Risk Assessment and planning for cybersecurity.	Risk Centric	Focuses on assessing organization risks.	Not focus on technological risks.

2.7.3.1.STRIDE.

STRIDE is a threat modeling framework developed by Microsoft, which focuses on identifying six types of security threats, namely Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, as explained by (Shostack, 2014). For more details, please refer to Table 2.5. This framework is used to systematically categorize and handle security threats in a system, with an approach that is in line with the Software-Centric Approach. STRIDE is commonly applied in software development to ensure secure system design. This methodology requires the analysis of each system component based on six threat categories to identify potential vulnerabilities. Although it provides a structured approach to threat identification, this

framework may not cover all aspects of modern cybersecurity threats and requires in-depth understanding to be applied effectively.

Table 2.5. STRIDE Modeling.

Symbol	Threat	Property Violated	Threat Definition
S	Spoofing	Authentication	Pretending to be something or someone other than yourself
T	Tampering	Integrity	Modifying something on disk, memory or network.
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible, can be honest or false.
I	Information Disclosure	Confidentiality	Providing information to someone not authorized to access it.
D	Denial of Services	Availability	Exhausting resource needed to provide services.
E	Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do.

2.7.3.2. DREAD Model.

The DREAD threat model is a framework used to assess and prioritize security risks based on five criteria: Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability. According to (Kim, Kim and Kim, 2022) in The Security Development Lifecycle, DREAD helps security teams quantify risk by assigning a score to each criterion, so that risks can be prioritized based on their severity. This approach allows organizations to focus on the most critical threats and allocate security resources effectively.



Figure 2.6. DREAD Threat Modeling.(Nweke, Weldehawaryat and Wolthusen, 2021)

Each component in figure 2.6. DREAD plays an important role in assessing risk. Damage Potential measures how much damage a threat can cause, while Reproducibility assesses how easily a threat can be reproduced. Exploitability evaluates the ease of exploiting a vulnerability, and Affected Users identifies the number of users who may be affected. Discoverability assesses how easily a vulnerability can be discovered by an attacker. According to Shostack (2014) in his book *Threat Modeling: Designing for Security*, by assessing each criterion separately, the security team can get a more comprehensive picture of the level of risk associated with a particular threat.

Although DREAD is a useful tool for assessing risk, this approach also has several limitations. According to (Ucedavélez and Morana, 2015) in *Risk Centric Threat Modeling*, one criticism of DREAD is the subjectivity in assigning scores, which can vary depending on the perception and experience of the security team. In addition, DREAD does not always take into account the business context or the long-term impact of the threat. Therefore, DREAD is often used in conjunction with other frameworks, such as STRIDE or PASTA, to obtain a more holistic and accurate risk analysis. By combining various approaches, organizations can develop a more effective and resilient security strategy against cyber threats.

2.7.3.3. PASTA.

The PASTA (Process for Attack Simulation and Threat Analysis) threat model is a seven-step approach designed to integrate business risk analysis with threat modeling

techniques. According to (Ucedavélez and Morana, 2015) in the book Risk Centric Threat Modeling, PASTA aims to identify and analyze the most relevant threats to an organization by considering the business context and security objectives. This approach begins by defining the objectives and scope of the project, followed by identifying the technical and business assets that need to be protected. By combining business and technical perspectives, PASTA ensures that the identified threats have a significant impact on the organization's operations and objectives.

The steps in PASTA include an in-depth analysis of the application architecture, identification of potential threats, and attack simulations to understand how threats can be exploited. According to Shostack (2014) in Threat Modeling: Designing for Security, PASTA uses techniques such as attack trees and data flow diagrams (DFD) to visualize attack paths and points of vulnerability in the system. These steps help security teams prioritize threats based on their potential impact and likelihood of occurrence, so that resources can be allocated effectively to mitigate risks.

One of PASTA's strengths is its focus on business context and collaboration across teams. According to UcedaVelez and Morana (2015), PASTA involves stakeholders from various departments, including security, development, and business, to ensure that threat analysis is aligned with organizational goals. This approach is also iterative, meaning that the threat modeling process is carried out periodically to accommodate changes in the threat environment and business needs. Thus, PASTA not only improves system security but also ensures that the security measures taken support overall business goals.



Figure 2.7. PASTA Threat Model.(Ucedavélez and Morana, 2015)

According to UcedaVelez & Morana (2015) in the book Risk Centric Threat Modeling, according to figure 2.7. the first stage is Objective Definition, where the team determines the security objectives and scope of the project. The second stage is Technical Scope Definition, which involves identifying technical assets and system components that need to be protected. The third stage is Application Analysis, where the team maps the application architecture, data flow, and interactions between system components using tools such as Data Flow Diagrams (DFD). This stage helps identify points of vulnerability and areas that require additional protection.

The fourth stage is Threat Analysis, where the team identifies potential threats that can exploit vulnerabilities in the system. According to Shostack (2014) in Threat Modeling: Designing for Security, the fifth stage is Attack Simulation, where the team simulates an attack to understand how the threat can be exploited and the impact it might have.

The sixth stage is Vulnerability and Impact Analysis, where the team assesses the vulnerabilities and potential impact of the identified threats. The final stage is Risk Management, where the team develops and implements mitigation strategies to reduce risks. This approach ensures that the most relevant and high-impact threats are proactively addressed.

2.7.3.4. Attack Tree Model.

Threat model attack tree is an approach used to visualize and analyze potential attacks on a system with a hierarchical structure similar to a tree. According to Shostack (2014) in Attack Trees Modeling Security Threats, the first stage in building an attack tree is to identify the attack objective, which is usually placed as the root of the tree. This objective can be data theft, service disruption, or unauthorized access to the system. Once the objective is set, the next step is to identify the possible ways that the attacker can achieve that objective, which are represented as branches of the tree. Each branch can have sub-branches that represent more detailed steps or alternatives that the attacker can take. One example of the Attack Tree threat model is explained in figure 2.8. Root node is gain unauthorized access and sub domain is five aspect explain the below.

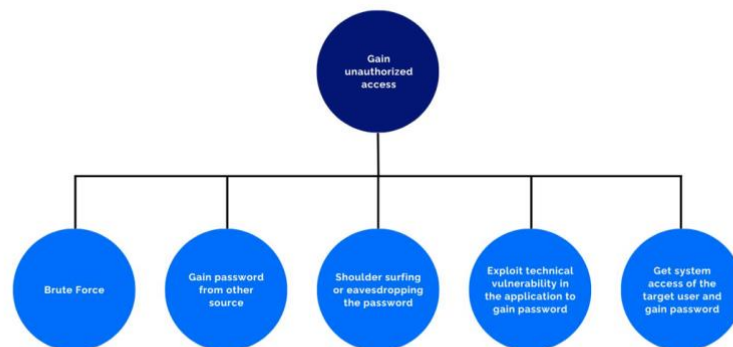


Figure 2.8. Attack Tree Threat Model example. (Buldas et al,2020)

The next stage is to assess the likelihood and impact of each attack. According to Shostack (2014) in Threat Modeling: Designing for Security, each node in the attack tree can be assigned a value that reflects the likelihood of the attack being successful, the costs involved, or the impact caused. This assessment helps the security team

prioritize threats and develop effective mitigation strategies. The final stage is to develop security controls to block or complicate the identified attacks. By using an attack tree, security teams can clearly understand how an attack might occur and take proactive steps to protect the system.

2.7.3.5. LINDDUN.

LINDDUN is a privacy-focused threat modeling framework developed to help identify and mitigate privacy threats in a system. The name LINDDUN stands for the six types of privacy threats it targets:

1. Linkability
2. Identifiability
3. Non-repudiation
4. Detectability
5. Disclosure of information
6. Unawareness
7. Non-compliance

Unlike security threat models such as STRIDE that focus on technical security, LINDDUN specifically addresses privacy risks, making it suitable for systems that process personal data such as health applications, e-commerce, or financial services.

While LINDDUN offers a comprehensive analysis of privacy threats and a structured methodology for assessment, it can be complex to apply and requires a solid understanding of privacy concepts. According to (Wuyts, Sion and Joosen, 2020) it systematically analyzes a system against seven categories of privacy concerns to uncover potential privacy risks and involves a six-stage process figure 2.9.

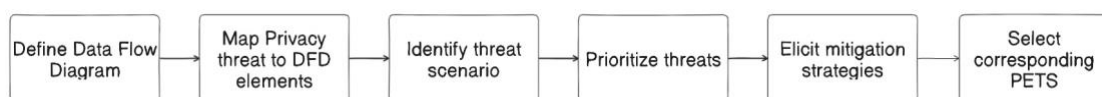


Figure 2.9. LINDDUN Steps. (Shotack,2014)

2.7.4. Cybersecurity and Privacy Risk Management.

The relationship between cybersecurity and privacy risk management is becoming increasingly close with the increasing digitalization of services and the complexity of cyber threats. In practice, cybersecurity focuses on protecting the confidentiality,

integrity, and availability of data, while privacy risk management emphasizes the protection of individual rights related to the collection, processing, and storage of personal data (NIST, 2020). The NIST Privacy Framework (2020) introduces a risk-based approach that enables organizations to identify, assess, and manage privacy risks in a manner that aligns with cybersecurity controls. By mapping privacy protection activities against cybersecurity controls, the framework helps organizations balance operational, security, and regulatory compliance needs.

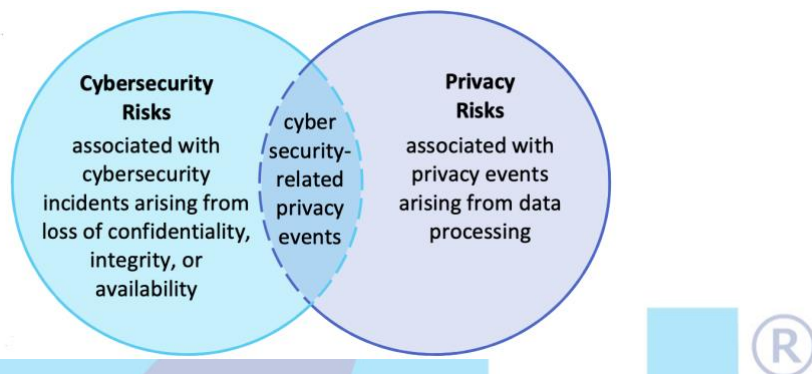


Figure 2.10. Cybersecurity and Privacy Risk Relationship. (NIST,2020)

In the NIST Privacy Framework (2020), figure 2.10 shows the relationship between cybersecurity and privacy risk as complementary but with different focuses. Cybersecurity risk management focuses on protecting organizational assets, including systems, networks, and data, from threats that could compromise the confidentiality, integrity, and availability of information. In contrast, privacy risk management focuses on protecting individuals from the potential impacts of personal data processing, such as privacy breaches, unauthorized data disclosure, or non-transparent profiling (NIST, 2020). While the two have distinct scopes, privacy risks often stem from cybersecurity weaknesses, for example, when system vulnerabilities allow unauthorized access to personal data. Therefore, NIST emphasizes the importance of integrating cybersecurity and privacy risk management to build a holistic approach. By linking technical security controls with privacy principles, organizations can simultaneously reduce risks to digital assets while minimizing negative impacts on individuals, thereby supporting the principle of privacy by design and increasing user trust in the system.

2.7.5. Privacy Threat Modeling and UU PDP.

Privacy threat modeling is an approach designed to identify, analyze, and mitigate potential threats to personal data within an information system. In the context of content-based systems such as Content Management Systems (CMS), these threats can include user identity traceability through metadata, data misuse for profiling, and a lack of transparency regarding the use of user data. This modeling helps organizations understand privacy vulnerabilities within a system's architecture from the design stage, thus supporting the implementation of the principle of privacy by design (Wuyts, Sion and Joosen, 2020)

The results of privacy threat modeling must be integrated with an information risk management framework to determine the severity and likelihood of a threat occurring. This approach aligns with international standards-based risk management models that combine threat identification, impact assessment, and technical and organizational mitigation measures. In practice, privacy threat modeling serves as a critical input into the risk assessment process, which then forms the basis for formulating security control policies such as encryption, pseudonymization, access control, and regular audits. Thus, the relationship between privacy threat modeling and risk management is complementary: threat modeling provides a structured threat mapping, while risk management provides quantitative and qualitative approaches to assessing and responding to these threats (NIST, 2020)

In the context of national law, the integration of privacy threat modeling and privacy risk management has become highly relevant with the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) in Indonesia. This law requires data controllers to protect users' personal data through transparent, secure, and accountability-based mechanisms. Articles in the PDP Law regulate the rights of data subjects, the obligations of data controllers, and sanctions for data breaches. Thus, organizations that implement privacy threat modeling can more easily align their systems with applicable regulations while minimizing legal and reputational risks resulting from privacy breaches. This demonstrates that privacy threat modeling is not only technical but also strategic in ensuring regulatory compliance and building public trust in personal data management (Republic of Indonesia, 2022).

The following is a table of LINDDUN's Privacy Threat Mapping against the main articles of the UU PDP (Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi).(Kadek Reza Ayuning Pranindya, 2025)

Table 2.6. Privacy Threat and UU PDP 2022 Mapping.

Threat Category	Threat Description	Pasal UU PDP	Compliance Context
Linkability	Personal data may be linked between systems/activities without consent.	Pasal 4 (data subject rights), Pasal 20 (consent to data processing)	Protection of individual rights so that online activities are not easily linked without authorization.
Identifiability	Individual identity can be identified from the processed data.	Pasal 16 (data minimization), Pasal 58 (obligation to protect personal data)	Data controllers are required to reduce the risk of identification through anonymization.
Non-repudiation	Data activity can be used to deny or bind individuals without legal basis.	Pasal 5 (right to privacy and freedom from arbitrary use), Pasal 39 (right to object)	Protection against misuse of individual activity recordings that could be legally detrimental.
Detectability	The existence of personal data can be detected by third parties even if the contents are unknown.	Pasal 14 (data confidentiality), Pasal 46 (prohibition of unauthorized distribution)	Preventing the detection of metadata or access patterns that could open up privacy gaps.
Disclosure of Information	Personal data is exposed without authorization (data leak).	Pasal 39–41 (data breach notification), Pasal 57 (administrative sanctions)	Data controllers are required to provide notification if a privacy breach occurs.
Unawareness	Data subjects are not aware of the processing of their data.	Pasal 6 (right to information), Pasal 21 (transparency of processing purposes)	Transparency principle: data subjects must be informed of the purpose, duration and method of data processing.

Threat Category	Threat Description	Pasal UU PDP	Compliance Context
Non-compliance	Data processing does not comply with applicable laws/regulations.	Pasal 57–60 (criminal and administrative sanctions)	The PDP Law requires compliance with the law and establishes sanctions for violations.

Mapping LINDDUN privacy threat categories against key articles in the Personal Data Protection Law (UU PDP, 27 2022) demonstrates a strong link between the threat modeling framework and regulatory aspects in Indonesia. Linkability and Identifiability threats are mapped to articles on data subject rights, consent, and data minimization obligations, emphasizing the importance of preventing unauthorized linkage of digital activities and individual identification. Non-repudiation and Detectability threats relate to the protection of privacy rights, data confidentiality, and the data subject's right to object to unauthorized processing. Furthermore, Disclosure of Information threats correlate with articles governing data breach notification and administrative sanctions, emphasizing the role of data controllers in maintaining information security. Meanwhile, Unawareness is mapped to articles governing the right to information and disclosure of processing purposes, emphasizing the principle of transparency. Finally, Non-compliance is directly linked to articles on criminal and administrative sanctions, thus serving as a reminder of the importance of full compliance with national regulations.

Thus, this mapping demonstrates how the LINDDUN framework can serve as a bridge between technical approaches in privacy threat analysis and legal aspects and compliance with the PDP Law. This integration not only helps in the identification and mitigation of privacy risks but also ensures that the design of information systems, including Content Management Systems (CMS), is aligned with the national legal framework. This supports the implementation of the privacy by design principle, as aligns with academic literature (Wuyts, Sion and Joosen, 2020) while strengthening the protection of individual privacy rights in Indonesia.

2.7.6. Privacy Threat Modeling in CMS

Privacy threat modeling is a systematic approach to identifying, analyzing, and mitigating threats to personal data in an information system. It focuses not only on

security (confidentiality, integrity, and availability), but also on aspects of user privacy, such as: How data is collected, processed, stored, and shared. The risk of legal violations (e.g., PDP (Perlindungan Data Pribadi) in Indonesia, GDPR in Europe). The potential for misuse of user data, even when the system is technically secure.

The main components of privacy threat modeling are:

1. Identification of Privacy Assets, namely personal data, metadata, access history, and user preferences.
2. Actor Analysis, namely who can access/misuse data (internal and external).
3. Trust Boundaries, namely the limits on data flow between subsystems vulnerable to leaks.
4. Threat Classification, namely using a privacy-specific framework.
5. Mitigation & Control, namely data minimization, pseudonymization, encryption, access control, and consent management.

Privacy threat modeling is needed in Content Management System (CMS) to identify and reduce the risk of personal data leakage, because traditional approaches based on security threat modeling such as STRIDE are not able to handle privacy issues comprehensively, so that privacy frameworks such as LINDDUN are more appropriate to use in this context (Shostack, 2014). Comparison Table of Threat Modeling Models for Privacy in CMS :

Table 2.7. Comparison Table of Threat Modeling Models for Privacy in CMS

Framework	Focus	Strength	Weakness	References
STRIDE	Security threats (Spoofing, Tampering, Repudiation, Information Disclosure, DoS, Elevation of Privilege).	Structured, easy to use, often used for software.	Not specifically addressing privacy issues, more on technical security.	(Shostack, 2014)
LINDDUN	Privacy threats (Linkability, Identifiability, Non-repudiation,	Privacy-specific, supporting personal data mapping and regulatory analysis.	More complex, requires special skills.	(Wuyts, Sion and Joosen, 2020)

Framework	Focus	Strength	Weakness	References
	Detectability, Disclosure, Unawareness, Non-compliance).			
NIST Privacy Framework (2020).	Risk-based, compliance, governance.	Providing a strategic approach, supporting privacy by design.	Not technical details, more on organizational governance.	(Karie <i>et al.</i> , 2021)
ISO/IEC 29134 :2023	Privacy Impact Assessment (PIA), regulation & governance.	Supports regulatory risk analysis, PIA documentation.	Does not provide explicit threat categories.	(Ruiz <i>et al.</i> , 2023)

Threat modeling is a systematic approach used to identify, analyze, and mitigate security and privacy risks in an information system. In the context of a Content Management System (CMS), threats relate not only to technical security aspects such as spoofing, tampering, information disclosure, and denial of service, but also to privacy issues arising from the management of user data (Shostack, 2014). Traditional approaches such as STRIDE, developed by Microsoft, focus on pure security threats, making them inadequate in addressing more complex user privacy risks.

As a complement, (Wuyts, Scandariato and Joosen, 2014) introduced LINDDUN, a threat modeling framework specifically designed for privacy issues. LINDDUN classifies threats into seven categories: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance. These categories are relevant for CMSs that manage users' personal data, such as comment metadata, login history, or content that can be traced back to user identities.

The NIST Privacy Framework (2020) and ISO/IEC 29134, which emphasize risk evaluation and regulatory compliance, including the GDPR in Europe and the PDP Law in Indonesia. That threat modeling can be extended to encompass privacy threats in applications, which is analogously relevant for CMSs in managing content and user data.

Based on the literature comparison in Table 2.7, it can be concluded that a combination of various models is needed to produce a comprehensive approach to threat modeling in CMS. STRIDE remains relevant for identifying technical security threats, while LINDDUN is more effective in detecting privacy threats inherent in personal data management. Governance frameworks such as the NIST Privacy Framework or ISO/IEC 29134 provide an additional layer of regulatory compliance and organizational privacy policies. Therefore, the integration of this threat modeling approach can simultaneously address security and privacy challenges in modern CMS development.

2.8.Previous Study

This research discusses the importance of PT. XYZ's CMS as a crucial asset for a television company because it plays a central role in the process of collecting, producing, and distributing news content. However, dependence on information technology and digital systems makes the CMS vulnerable to cybersecurity threats, such as ransomware attacks, data leaks, or deliberate system disruptions. These risks can not only disrupt company operations but also damage reputation and public trust, which are invaluable intangible assets for television companies. Therefore, determining risks through **threat modeling, risk assessment, and threat mitigation** of this CMS application can help PT. XYZ ensure the continuity of media operations and compliance with privacy laws in reducing cybersecurity risks.

(Aven, 2016) emphasize that risk assessment is a core component of an organization's risk management process, aiming to identify, estimate, and prioritize risks to an organization's operations. They note that traditional quantitative analysis has focused solely on risk factors (such as threats and vulnerabilities) without formal definitions for assessment metrics. To address this, the study proposes a formal model and quantitative security metrics that can provide deeper insights into risk estimation. This model-based approach not only improves understanding of an organization's risk profile but also supports more effective security decision-making (e.g., through security budget allocation). With more measurable and structured risk information, the reliability and security of an organization's systems can also be enhanced through more effective threat identification and mitigation.

Threat modeling is very important to ensure the operational sustainability of the system, especially in a growing environment and full of cyber threats. Threat modeling is a systematic approach to identify, categorize, and prioritize threats to a system or

application. According to (Shostack, 2014) in Threat Modeling designing for Security. Various threat modeling methods such as STRIDE, DREAD, PASTA, LINDDUN and Attack Tree have been developed to help organizations understand and reduce security risks. Each of these methods has a different approach and focus, but all of them aim to improve system security and resilience.

DREAD is another model used to assess and prioritize security risks. According to (Kim, Kim and Kim, 2022), Dread evaluates threats based on five criteria: damage potential (potential damage), reproducibility (the ability to be reproduced), exploitability (ease of exploitation), affected users, and discoverability (ease of discovery). By giving a score to each criterion, the security team can prioritize threats based on their severity. Dread is very useful for allocating safety resources effectively and ensuring that the most critical threats are handled first.

LINDDUN (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure, Unawareness, Non-compliance) is a privacy threat modeling framework developed to systematically identify privacy risks in software systems (Deng *et al.*, 2023). This model is designed to meet regulatory demands such as GDPR and CCPA, especially in the context of personal data management (Sion *et al.*, 2025).

With the many threat models, (Bhole, Sauter and Kastner, 2025), explains the security related threat modeling framework for risk evaluation as in table 2.6 below.

Table 2.8. Security related threat modeling framework for risk evaluation

(Çankaya *et al.*, 2024)

Framework	Key Focus	Methodology Type	Primary Use Case
STRIDE	Threat Categorizations	Technical	Software design and Architecture Threat.
DREAD	Risk Assesment	Scoring Based	Risk Prioritazion of Threat
PASTA	Risk Base Attack Simulation	Process Driven	Real world attack simulation and risk assesment
VAST	Agile and scalable Modeling	Visual and scalable	Large scale enterprise and Agile
OCTAVE	Risk Based Assesment	Business Centric	Information security strategy and risk management
Trike	Risk and behavioral analysis	Role Based	System with role based access and action analysis

Table 2.8 above shows that each threat model has a different focus, depending on the methodology used. Therefore, this methodology can be implemented to identify risk-based threats in our organization.

The operational sustainability of the system is very dependent on the ability to identify and reduce security risks. According to (Ross, McEvelley and Oren, 2018) in NIST SP 800-160 Developing Cyber Resilient System, Threat Modeling is a key component in cyber security risk management. By using methods such as stride, dread, pasta, and attack tree, organizations can identify potential threats, assess their impact, and develop effective security controls. This approach ensures that the system can operate safely and reliably, even in an environment full of threats.

According to (Tudela *et al.*, 2020), The OWASP Top Ten project brings together the most important vulnerability categories and mitigation control. Web applications in organizations and companies connected through the Internet and Intranets imply that they are used to develop any type of business, but at the same time they have become a valuable target of a great variety of attacks by exploiting the design, implementation or

operation vulnerabilities, included in the OWASP Top 10 project, to obtain some type of economic advantage, privileged information, denial, extortion, etc. This control includes aspects such as access management, data encryption, and security monitoring. By applying relevant control, the organization can reduce vulnerability and ensure that their system remains operating safely and reliably. In addition, ISO 27001: 2022 encourages a review and continuous improvement, ensuring that risk management remains relevant to the environmental changes in threats and business needs. Thus, this approach supports the operational sustainability of the system in the long run. In this research using the ISO 27001:2022 and OWASP Top 10 approach includes the mitigation of security controls that are tailored to the needs of the organization. Furthermore, the literature study above will be explained in the related work table 2.7 as follows :

Table 2.9. Summarizes the comparison of other related studies.

Criteria	(Eom <i>et al.</i> , 2019)	(Gakh <i>et al.</i> , 2024)	(Kim, Kim and Kim, 2022)	(Khalil <i>et al.</i> , 2023)	(Das <i>et al.</i> , 2024)	Our Research
Framework	TV-HARM	PRIAM - LINDDUN	STRIDE - DREAD	STRIDE	STRIDE-DREAD-SAHARA	STRIDE-LINDDUN-DREAD
Key Focus	Analyze the Threat of SDN.	Threat Model Privacy Analysis at E-Justice System Application	Threat Model and Risk Evaluation on Operational ICS	Identify Threat of Cyber Physiscal System	Analysis Threat and Risk for infotainment system.	Design Threat Model Driven Risk Management of Media CMS
Relevance with Our Research	SDN and CMS also require security posture modeling due to the complexity of integration with external services (cloud, API.)	LINDDUN step using identifying privacy risks in the login credential CMS.	Threat identification and mitigation methodology based on components.	Threat identification and mitigation methodology based on components.	Risk evaluation with the DREAD Model to identify risk priorities.	-

Criteria	(Eom <i>et al.</i> , 2019)	(Gakh <i>et al.</i> , 2024)	(Kim, Kim and Kim, 2022)	(Khalil <i>et al.</i> , 2023)	(Das <i>et al.</i> , 2024)	Our Research
Use Case	Enhancing the security of SDN while considering various threat vectors.	Identify Threat of System electronic judicial registry for claim proceedings.	Mitigate threat and risk of Distributed Control System.	Identify security requirements through threat modeling for microgrid.	List vulnerabilities in the infotainment system.	Enhancing Security posture Software of Media CMS
Sector	SDN Infrastructure	E-Justice platform (legal documents, PII)	Industrial Control System (ICS/DCS).	Microgrid energy systems.	In-Vehicle Infotainment System (IVIS).	Custom CMS News at Media Industry
Analysis Method	The paper proposes a novel framework named Threat Vector Hierarchical Attack Representation Model (TV-HARM) for evaluating SDN security threats. Three security metrics are defined: Network Centrality Measure, Vulnerability score, and attack impact metrics.	The authors propose practical guidelines for risk modeling steps in PRIAM, benefiting from LINDDUN's supporting materials.	The paper employs the STRIDE methodology for identifying security threats. DREAD methodology is utilized to prioritize identified risks and develop a remediation plan. Threat analysis using details from system architecture and decomposition. The analysis incorporates case studies of cybersecurity.	The study proposes methodology STRIDE. This methodology includes a systematic threat elicitation procedure based on an attack taxonomy created for the research. The methodology emphasizes identifying information and system assets, including control and measurement categories.	The study applied STRIDE model to assess security issues in infotainment systems. Risk assessment methodologies such as SAHARA and DREAD were utilized to evaluate potential security threats..	Determine Business Security Goals, this research identify threat with STRIDE, LINDDUN model. Implementation Vulnerabilities Analysis, Risk Evaluation using DREAD and mitigation control by ISO 27001 and OWASP Top 10. This research determines the risk by using a combination of threat models so that the results obtained are more comprehensive.

Criteria	(Eom <i>et al.</i> , 2019)	(Gakh <i>et al.</i> , 2024)	(Kim, Kim and Kim, 2022)	(Khalil <i>et al.</i> , 2023)	(Das <i>et al.</i> , 2024)	Our Research
Risk Evaluation	Quantitative scores.	Misuse case assess likelihood and impact, compute risk scores per module.	Scoring By DREAD, validation use case STUXNET, TRITON	Rank threats by (qualitative/semi-quantitative)	SAHARA and DREAD frameworks	DREAD Framework, Validation use expert interviews.
Strenght	The authors demonstrate the effectiveness of their proposed security assessment framework through experimental analysis. The framework is deemed effective for evaluating the security of SDN while considering various threat vectors.	The paper enhances the PRIAM method by integrating systematic threat elicitation steps from LINDDUN and LINDDUN+ into risk identification. A case study on an e-justice platform demonstrates the applicability of the proposed enhancements.	The study contributes to the understanding of cybersecurity risks in ICSs, which are increasingly connected to the internet. It emphasizes the importance of conducting thorough risk assessments and utilizing methodologies like STRIDE and DREAD to identify and prioritize threats effectively.	The study proposes a systematic methodology to apply STRIDE to cyber-physical systems (CPSs). The paper concludes that the proposed threat modeling methodology can effectively identify key security functions in complex systems like microgrids.	STRIDE's structured approach aids in thorough analysis of infotainment system components. The study identified 34 potential security threats, demonstrating STRIDE's effectiveness.	Risk Evaluation and threat identify more detail with more than one method. Risk Centric Control Mitigation risk recomendation for technical and Management perspective.
Limitations	The effectiveness of countermeasures is not	The proposed risk modeling method has non-exhaustive coverage of	The paper acknowledges that not all identified threats can be	The methodology's application faced challenges due to the lack of	FMVEA focuses on single causes, potentially overlooking	Focus on Custome CMS application of journalist. Input News Process and Strem

Criteria	(Eom <i>et al.</i> , 2019)	(Gakh <i>et al.</i> , 2024)	(Kim, Kim and Kim, 2022)	(Khalil <i>et al.</i> , 2023)	(Das <i>et al.</i> , 2024)	Our Research
	fully analyzed, limiting understanding of their impact on security posture.	feared events, limiting its applicability to GDPR requirements only.	eliminated due to the limited resources, which may hinder comprehensive threat mitigation efforts.	detailed system information, such as operating systems and network protocols.	multi-stage attacks, which is a significant limitation.	News to Production Process.

According to previous research discussed in Table 2.9 there are gap analysis in previous study, At (Eom *et al.*, 2019), the paper summarizes potential new threats in Software Defined Networking (SDN) and emphasizes the importance of threat modeling and security assessment to evaluate SDN security. It highlights the development and applicability of the Threat Vector Hierarchical Attack Representation Model (TV-HARM) for capturing various threat vectors in SDN. The authors demonstrate the effectiveness of their proposed security assessment framework through experimental analysis, utilizing three security metrics: Network Centrality Measures, Vulnerability Scores, and Attack Impact Metrics. The framework is deemed effective for evaluating the security of SDN while considering various threat vectors. The gap this paper acknowledges the existence of unknown vulnerabilities in SDN controllers, such as Floodlight and POX, which may not be applicable in all SDN settings for security evaluation. It highlights the limitation of not considering all possible attack paths in the security evaluation, focusing only on defined attacker and target paths. The research does not account for the functional differences among various SDN controllers, which could impact security assessments and countermeasure selections. Future work is suggested to investigate the effects of different SDN functionalities on security assessment.

At (Gakh *et al.*, 2024), The paper enhances the Privacy Risk Analysis Method (PRIAM) in e-justice system application, method by integrating LINDDUN and LINDDUN+ for systematic threat elicitation steps. It maps PRIAM's feared event categories to LINDDUN's privacy threat types. The improved PRIAM method was applied to the

Small Claim Net II e-justice application, demonstrating its practicality. The study identifies weaknesses in PRIAM and proposes practical guidelines for risk modeling. The ambiguity in PRIAM's terminology presents a significant research gap in understanding its application. There is a lack of descriptions regarding the risk modeling process in PRIAM. Insufficient common knowledge materials for modeling decisions hinders effective use of PRIAM. The validation of threat modeling and risk assessment results is challenging due to speculative nature.

At (Kim, Kim and Kim, 2022) The paper concludes that cybersecurity threats targeting Industrial Control Systems (ICSs) are increasingly sophisticated and frequent, necessitating a robust threat modeling approach. It emphasizes the importance of conducting thorough risk assessments and utilizing methodologies like STRIDE and DREAD to identify and prioritize threats effectively. The study highlights the need for tailored countermeasures to mitigate risks associated with Distributed Control Systems (DCSs) in oil refineries, given their critical role in safety and operational integrity. Overall, the research advocates for a structured methodology to enhance the security posture of ICSs against evolving cyber threats. There is insufficient documentation and understanding of the various threats that can compromise ICSs, which hampers effective threat modeling.

At (Khalil *et al.*, 2023), The paper concludes that the proposed threat modeling methodology can effectively identify key security functions in complex systems like microgrids, despite the challenges of missing information and expert reliance. It emphasizes the importance of incorporating an attack taxonomy to enhance the threat elicitation process and reduce dependence on expert knowledge. The authors acknowledge the need for systematic validation of the methodology's outcomes and suggest that their approach could be adapted to other cyber-physical systems, although scalability remains a concern. The research noted absence of detailed and repeatable threat modeling methodologies in existing literature, particularly concerning trust boundaries identification and threat elicitation processes. Additionally, scalability issues are identified for systems with numerous elements, complicating the application of the proposed STRIDE per-element approach.

At (Das *et al.*, 2024), The paper concludes that the increasing complexity of infotainment systems in modern vehicles poses significant cybersecurity risks, necessitating thorough threat modeling to identify potential vulnerabilities. It emphasizes the importance of applying the Microsoft STRIDE model alongside SAHARA and DREAD risk assessment methodologies to evaluate and prioritize security threats effectively. The study identifies 34 potential security threats, recommending specific mitigation strategies for each to enhance the overall security posture of automotive infotainment systems. The paper indicates a need for future work on threat modeling specifically targeting hardware components connected to road vehicles, suggesting a gap in the current focus on software aspects alone. It highlights that the STRIDE model is not suitable for the early design phase, indicating a gap in methodologies applicable during initial design stages. The research also points out the necessity for modeling misuse cases and misuse sequence diagrams, which are currently not addressed, representing another area for further exploration.

According to previous research gap analysis above, to effectively this thesis will adopt a risk based approach that focuses on modeling threats and security. By utilizing software centered methodology, this study aims to proactively identify and reduce the potential risk inherent in the CMS application. This approach will combine the PASTA Framework and Attack Tree to specifically deal with the system of operational sustainability of the system, given the CMS system acts as the backbone of the company in receiving news content from various field journalists. The LINDDUN framework is used to identify data privacy related threats in processes within the CMS.

The research will employ the STRIDE methodology for identifying security threats, inspired by its successful application in Industrial Control Systems highlighted by (Kim, Kim and Kim, 2022). This research will use step by step methodology to identify security threats, which as explained by (Kim, Kim and Kim, 2022) , (Khalil *et al.*, 2023) and (Eom *et al.*, 2019). Base on those papers, this research will combines using STRIDE, DREAD, and LINDDUN framework is designed to provide a comprehensive risk assessment, ensuring that the CMS system in the media industry is not only efficient in managing journalist data but is also tough in protecting the system to keep operating. This hybrid approach, combining STRIDE , LINDDUN, and DREAD is designed to

offer a comprehensive risk assessment. This strategy is very important in the media sector, where operational sustainability and business reputation are top priorities.

