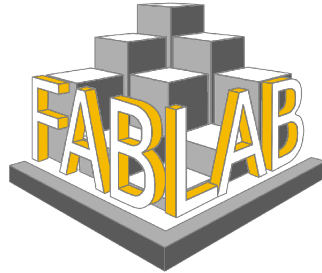


# Security Compliance and Audit Report

## Security Compliance and Audit Report at Company Fablab Jababeka

Fabrication Laboratory (Fablab) Jababeka



Leader: Abimanyu Eka Prasetya (001202200005)

Member:

Afsa Mifzal Zararghirfar (001202200150)

Carlos G. R. Pires Guterres (001202200178)

Diva Emanda Ghaitsha (001202200099)

Egan Maheshwara (001202200079)

Elgino Tanto Jaya (001202200143)

Farrel Fadhilah Rayadi (001201800087)

Ghifari Prayuga Gunawan (001202000050)




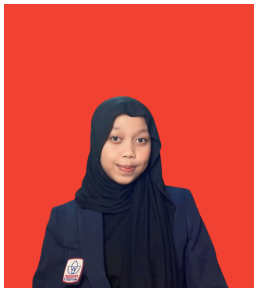
Jonathan Rocky P. Monteiro (001202200049)

Phuja Sharma Ratu Khirana (001202200094)

Septia Wahyu (001202000134)

Informatics Study Program

**Auditor Profile**

No	Student Picture	Student Short Bio
1.		Abimanyu has been an active and undergraduate student in President University since August 2022, majoring in Informatics and focusing on Cyber Security. And he is currently a second-year short semester.
2.		Elgino, an undergraduate student at President University since August 2022, is majoring in Informatics with a concentration in Cybersecurity. He is currently in his second-year short semester and is enrolled in a Cyber Security Audit & Compliance class.
3.		Carlos joined President University in August 2022 and is currently in his second year of study, pursuing a Bachelor's degree in Informatics with a specialization in Cyber Security. His academic interests lie in Digital Forensics and Incident Response, aiming to contribute to enhancing digital security measures.
4.		Diva Emanda, Second-year student majoring in Informatics with a concentration in Cyber Security at President University, North Cikarang, Indonesia.

5.		Jonathan is a 6th-semester undergraduate student at President University, majoring in Informatics with a concentration in Cyber Security. Since August 2022, he has been actively engaged in his studies at President University, exploring various aspects of cybersecurity to broaden his knowledge and skills in the field.
6.		Afsa is an active student studying at President University. Currently, he's in his second year majoring in Informatics, focusing on Cyber Security.
7.		Egan is a 6th-semester Information Technology student at President University, specializing in Cybersecurity. His academic focus includes Security Compliance and Audit, which aligns with his concentration.
8.		Ghifari is an active student at President University, having joined in August 2022. He is currently in his second year, majoring in Informatics with a concentration in Cyber Security.

9.		Phuja is an active student at President University since August 2022, majoring in Informatics with a concentration in Cyber security and include Security Compliance and Audit for elective enrollment.
10.		Septia is an active student at President University since August 2020, majoring in Informatics and taking Security Compliance and Audit.
11.		Farrel is an active student at President University since August 2018, majoring in Informatics. He is currently enrolled in a Cyber Security Audit & Compliance class.

### **Company Profile**

Fabrication Laboratory (Fablab) Jababeka, located at Jababeka Industrial Estate in Cikarang, Bekasi, West Java, Indonesia, is a center for technology and industrial solutions. The laboratory serves as a hub for startup development, academic programmes, and community engagement. In addition, Fablab is one of the Indonesian Centre for Digital Industry (PIDI) in Indonesia initiated by the Ministry of Industry of the Republic of Indonesia as a platform for stakeholders such as industry tenants, students, communities, government, and media to collaborate with each other in realizing industry 4.0 in Indonesia.

Fablab Jababeka focuses on Industry 4.0, Society 5.0, and Net Zero Emissions. It is designed for anyone who wants to learn and create, with an organization profile that focuses on the purpose to create, innovate, and collaborate. Fablab Jababeka's vision is to grow innovation and creativity through hands-on learning and experimentation. To achieve this, its mission includes offering workshops and training programmes to help individuals learn new skills, providing a platform for people with similar interests to discuss and collaborate, and encouraging tinkering with existing items and technologies to create new inventions. By offering resources and a collaborative environment, Fablab Jababeka supports the realization of Industry 4.0 in Indonesia through technological advancement and creative development.

Fablab Jababeka offers a range of products and services, including the loan of mechanical machine tools such as 3D printers, 3-in-1 3D printers (combining 3D printing, CNC milling, and laser cutting), robotic arms, Arduino kits, and basic equipment such as cutting tools and grinders. These tools are available for use by individuals who have the necessary certifications. Fablab Jababeka also provides consumable products such as 3D printer filament (PLA). Apart from offering products, Fablab Jababeka also provides seminar events, tool training and workshops related to the machines they offer.

## 1. GOVERN (GV)

**GOVERN (GV):** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored expectations, and policy.

### 1.1 Overview

Fablab Jababeka aligns cyber risk management with its mission to become a Silicon Valley-like innovation hub, by establishing consistent data flows and SOPs. Regular communication with internal and external stakeholders ensures their needs are met according to safety standards. Legal and regulatory requirements for access control are managed through documented SOPs. Internal resources are managed by the IT and Knowledge departments, while risk policies are created and communicated by the IT department. Cyber systems are updated through security patches, and threats are managed with firewalls and collaboration with ethical hackers. HR processes involve cybersecurity considerations, and suppliers are evaluated based on security and effectiveness criteria. Overall, Fablab Jababeka applies a structured approach to cyber governance, although some areas require improvement such as consistent policy updates and involving critical suppliers in incident planning.

### How many YESES does the company fulfill in the governance category?

The company fulfills 17 YESES in the Govern subcategory based on the interview analysis from 31 subcategories.

### 1.2 SWOT Analysis of Govern

Strength	Weakness	Opportunity	Threats
Clear alignment of cybersecurity risk management with the organizational mission.	Inconsistent updates and reviews of cybersecurity policies. (GV.OC-01)	Implementing more consistent and regular policy updates and reviews.	Rapidly evolving cybersecurity threats that require constant vigilance and updates.

(GV.OC-01)		(GV.OC-01)	(GV.OC-01)
Regular communication with internal and external stakeholders ensures alignment with their expectations. (GV.OC-02)	Lack of involvement of critical suppliers in incident planning, response, and recovery activities. (GV.OC-02)	Engaging critical suppliers in incident planning and response activities. (GV.OC-02)	Potential for data breaches or security incidents due to gaps in policy updates and supplier involvement. (GV.OC-02)
Well-documented SOPs and access control policies for managing data security. (GV.OC-03)	Absence of a formal risk appetite and risk tolerance statement. (GV.OC-03)	Enhancing regular outreach and training programs on cybersecurity awareness and best practices. (GV.OC-03)	Dependency on third-party ethical hackers, which may pose risks if not properly managed. (GV.OC-03)
Strong internal resource management by dedicated IT and Knowledge departments. (GV.OC-04)	Infrequent and irregular cybersecurity outreach and awareness programs. (GV.OC-04)		Increasing regulatory requirements and standards that must be continuously met and integrated. (GV.OC-04)
Regular updates and management of cybersecurity threats through collaboration with ethical hackers and use of firewall protection. (GV.OC-05)			
Involvement of cybersecurity considerations in HR processes. (GV.RM-01)			
The absence of a risk appetite statement may indicate flexibility in risk management. (GV.RM-02)	Lack of a risk appetite statement suggests no clear guidelines for measuring and managing risk, potentially leading to inconsistent decision-making. (GV.RM-02)	Developing a risk appetite statement could clarify expectations and boundaries for risk management. (GV.RM-02)	The lack of a risk appetite statement may increase exposure to poorly managed risks, potentially harming the organization. (GV.RM-02)
The presence of a firewall and management by the IT department indicates	Absence of a formal strategy for managing third-party information		Without a clear strategy, risks from third-party information

an initial layer of protection against cyber threats. (GV.RM-04)	could create security gaps. (GV.RM-04)		might be overlooked. (GV.RM-04)
Individual reporting of bugs suggests that issues can be addressed directly. (GV.RM-05)	Communication channels used might not be optimal for handling security crises, potentially causing delays. (GV.RM-05)	Strengthening communication about cybersecurity risks through training and awareness for all team members. (GV.RM-05)	Lack of leadership from senior executives could diminish awareness and prioritization of cybersecurity. (GV.RM-05)
Standard methods for documenting and categorizing risks can aid in monitoring and reporting. (GV.RM-06)	Absence of a clear standardized method for calculating and prioritizing risks may lead to inconsistency. (GV.RM-06)	Implementing standardized methods could improve consistency and efficiency in cybersecurity risk management. (GV.RM-06)	
Engages ethical hackers and third parties for insights and improvements. (GV.RR-01)	Limited regular internal communication about cybersecurity among employees. (GV.RR-01)		
The presence of a structured flow and Standard Operating Procedures (SOPs) indicates a well-organized approach to managing cybersecurity risks. (GV.PO-01)		Exploring additional methods for communicating the policy, such as detailed documentation or interactive training, can enhance understanding and implementation. (GV.PO-01)	

### 1.2.1 Strength

- 1. GV.OC-01: The organizational mission:** For digitalization, data should be standardized first, and the flow should be aligned and not contradictory.
- 2. GV.OC-02: Communication with internal and external stakeholders:** Important regular communication with internal and external stakeholders refers to safety standard



3. **GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity:** Access data there are Standard Operating Procedure and access control for managing data security
4. **GV.OC-04: Critical Objectives capabilities:** Identify what the organization does well in terms of capabilities and services, stakeholders rely on or expect, such as reliability, efficiency, or innovation.
5. **GV.OC-05: Outcome capabilities:** Identify successful outcomes that the organization consistently achieves. For example, high customer satisfaction, on-time project delivery, or strong market presence.
6. **GV.RM-01: Risk management with stakeholder:** Effective communication and engagement processes with stakeholders that ensure their input is considered and objectives are well-supported.
7. **GV.RM-02: Risk Appetite and Risk Tolerance Statements:** The organization benefits from flexibility in risk management due to the absence of rigid risk appetite statements. This adaptability can be advantageous in rapidly changing environments.
8. **GV.RM-04: Strategic Direction for Risk Response:** The organization has established effective initial defenses such as firewalls and proactive threat management by the IT department, providing a solid foundation for mitigating immediate threats.
9. **GV.RM-05: Communication of Cybersecurity Risks:** Structured communication channels through Microsoft Teams and direct bug reporting facilitate effective coordination and prompt issue resolution, supporting proactive cybersecurity risk management.
10. **GV.RM-06: Standardized Method for Cybersecurity Risk:** Utilization of Microsoft Teams for coordination and existing practices for documenting and categorizing risks support effective monitoring and reporting of cybersecurity risks.

- 11. GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk:** The organization effectively collaborates with ethical hackers and third parties to address cybersecurity risks and updates its SOPs accordingly.
- 12. GV.PO-01: Policy for managing cybersecurity risks:** The company has established a comprehensive set of Standard Operating Procedures (SOPs) for cybersecurity risk management. This structured approach ensures that risk management activities are well-organized, consistent, and aligned with organizational priorities.

#### 1.2.2 Weakness

- 1. GV.OC-01: The organizational mission:** There is a need for better clarity and consistency in data flow across departments. This can be achieved by creating and implementing a clear SOP to ensure that data flow is standardized and not contradictory.
- 2. GV.OC-02: Communication with internal and external stakeholders:** Stakeholder engagement, although regular, can be improved to ensure that expectations regarding cybersecurity risk management are fully understood and met.
- 3. GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity:** Access to documentation processes for regulating information control is currently restrictive. While this ensures security, it may hinder staff efficiency and understanding. Developing a more accessible yet secure way for staff to access these processes can improve overall governance.
- 4. GV.OC-04: Critical Objectives capabilities:** Recognize any gaps between what stakeholders expect and what the organization currently delivers, such as slower response times or inconsistent quality.
- 5. GV.RM-02: Risk Appetite and Risk Tolerance Statements:** The absence of a formal risk appetite statement creates ambiguity in managing and measuring risk, potentially leading to inconsistent risk-related decisions.

6. **GV.RM-04: Strategic Direction for Risk Response:** The lack of a dedicated strategy for managing third-party information and reliance on external infrastructure may introduce potential security gaps and vulnerabilities.
7. **GV.RM-05: Communication of Cybersecurity Risks:** The absence of senior executive involvement in cybersecurity might reduce the effectiveness of leadership in addressing and prioritizing security issues.
8. **GV.RM-06: Standardized Method for Cybersecurity Risk:** The absence of a standardized method for calculating and prioritizing risks may lead to inconsistent risk management practices and hinder effective risk assessment.

#### 1.2.3 Opportunity

1. **GV.OC-01: The organizational mission:** Standardizing data flow presents an opportunity to improve the overall efficiency and security of data management. Implementing clear and consistent data standards will benefit the organization's digitization efforts.
2. **GV.OC-02: Communication with internal and external stakeholders:** Enhancing stakeholder communication and feedback mechanisms can lead to better alignment of cybersecurity strategies with stakeholder expectations. This proactive approach can strengthen stakeholder trust and support.
3. **GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity:** Strengthening access control processes and making them more accessible to staff can improve the organization's ability to protect individual, user, and customer information while maintaining efficiency.

4. **GV.RM-02: Risk Appetite and Risk Tolerance Statements:** The organization developing and implementing a clear risk appetite statement can provide direction, enhance strategic planning, and improve risk management practices across the organization.
5. **GV.RM-04: Strategic Direction for Risk Response:** Developing a comprehensive strategy for third-party information protection and aligning policies with best practices could further strengthen the organization's overall security posture.
6. **GV.RM-05: Communication of Cybersecurity Risks:** Enhancing communication strategies and involving senior executives in cybersecurity efforts can improve overall management and response to security risks, fostering a stronger security culture.
7. **GV.RM-06: Standardized Method for Cybersecurity Risk:** Implementing a standardized method for risk assessment and improving documentation practices could enhance consistency, efficiency, and overall effectiveness in managing cybersecurity risks.
8. **GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk:** The organization can enhance its cybersecurity posture by implementing more frequent awareness programs and proactively addressing emerging threats.
9. **GV.PO-01: Policy for managing cybersecurity risks:** The organization has the opportunity to enhance policy communication through additional methods such as detailed documentation, interactive training sessions, or periodic briefings. These methods can help ensure that all stakeholders fully understand and can effectively apply the policy.

#### 1.2.4 Threats

1. **GV.OC-01: The organizational mission:** The risks associated with digitalization, such as potential security breaches, need to be continually monitored and mitigated. Ensuring robust cybersecurity measures are in place is crucial to protect against these threats.

2. **GV.OC-02: Communication with internal and external stakeholders:** Stakeholder expectations regarding cybersecurity risk management may pose a challenge if not adequately met.  
Continuous engagement and transparent communication can help manage these expectations effectively.
3. **GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity:** Regulatory compliance and adherence to legal, regulatory, and contractual requirements regarding cybersecurity need constant attention. Failing to comply can result in legal and financial repercussions.
4. **GV.OC-04: Critical Objectives capabilities:** Assess how these threats might affect stakeholder expectations or reliance on the organization's services and capabilities.
5. **GV.RM-02: Risk Appetite and Risk Tolerance Statements:** Without a defined risk appetite, the organization may face increased exposure to unmanaged risks, potentially leading to significant vulnerabilities and unanticipated threats.
6. **GV.RM-04: Strategic Direction for Risk Response:** Potential security gaps due to the absence of a formal strategy for third-party information management and dependency on external infrastructure could expose the organization to increased risk.
7. **GV.RM-05: Communication of Cybersecurity Risks:** Lack of senior executive focus on cybersecurity may lead to slower response times and reduced effectiveness in handling critical security issues.
8. **GV.RM-06: Standardized Method for Cybersecurity Risk:** Inconsistent risk management due to the lack of standardized methods may result in overlooked or inadequately managed risks, potentially impacting the organization's security posture.

## 2. IDENTIFY (ID)

**IDENTIFY (ID): The organization's current cybersecurity risk is understood.**

### 2.1 Overview

The company uses various methods to identify and mitigate incoming threats and monitor these threats.

The IT department is largely responsible for this problem and the company has good mitigation methods and the only drawback is that it doesn't have the tools or tools used for monitoring.

The company fulfills 9 YESSES in the Govern subcategory based on the interview analysis from 21 subcategories.

### 2.2 SWOT Analysis of Identify

Strength	Weakness	Opportunity	Threats
The hardware is stored in a secure location that is not disclosed by the organization. The benefit of this approach is that the organization does not need to rent a place to store the hardware. (ID.AM-01)	Since inventory management is held by the Jababeka Center, this can be a weakness because Jababeka can see or audit what goods an organization owns, and leaks could occur. (ID.AM-01).	Provide rules or regulations for the management of Jababeka and provide more security for inventory (ID.AM-01).	Threats can arise both externally and internally because the organization does not directly manage the inventory. Theft can occur at any time, whether from outside sources or within the organization (ID.AM-01).
Inventories of software, services, and systems managed by the organization are maintained (ID.AM-02).	The one who maintained the software is not from the IT team. IT team is for networks and devices (ID.AM-02).	-	-
The company has baselines of communication and data flows through wired and wireless networks. The company will document network ports, protocols, and	-	The company should do documentation regularly (ID.AM-03).	-

services, which are updated every time there is a change (ID.AM-03).			
The company already has suppliers that provide IaaS, PaaS, and SaaS services. The IT team is responsible for maintaining and updating the services that are already provided by the suppliers (ID.AM-04).	-	The IT team that is responsible for maintaining the services and the suppliers that provide the services should keep in touch to avoid unwanted things happening (ID.AM-04).	This can happen if the IT team is not responsible for their job and suppliers commit fraud (ID.AM-04).
The company periodically conducts monitoring to track asset priorities and update the assets (ID.AM-05).	Not sure how often the company tracks and updates its assets (ID.AM-05).	-	-
The company checks every month to ensure the accuracy and completeness of records for each type of data, and there is a procedure when there are changes or updates to data types (ID.AM-07).	-	-	-
-	-	-	-
The company updates regularly to review processes and procedures for mitigating risk (ID.RA-01).	There is no time specified for the updates. The company doesn't have or use any technology or tools to monitor the vulnerabilities (ID.RA-01).	The company should use any tools and technology to monitor the vulnerabilities (ID.RA-01).	Threats can happen if the company doesn't have or uses any tools or technology for monitoring the vulnerabilities (ID.RA-01).
The company reviewed monthly so that it would be accurate, complete, and other	The company does not have criteria or basis for assessing or evaluating cyber perpetrators	The company should evaluate its tactics, techniques, and procedures (TTP) and implement policy	Lead to data leakage or unauthorized access, information could be obtained by the other personnel, and data

records assessed by the company. (ID.RA-02).	and currently, their tactics, techniques, and procedures (TTP) are still not implemented. (ID.RA-02)	criteria for cybercriminals (ID.RA-02)	breach could happen anytime. (ID.RA-02)
-	Because the company does not handle things like this, it can be concluded that there are weaknesses in security that are inadequate in dealing with threats from outside and inside (ID.RA-03)	Convene or create a credible security team division to deal with threats or matters related to cyber security (ID.RA-03)	Threats can occur both from outside and inside due to the lack of security arrangements (ID.RA-03)
-	-	-	-
-	-	-	-
The company has a plan to mitigate risks and updates regularly (ID.RA-06).	There is no time specified to do the update (ID.RA-06).	-	-
-	-	-	-
The company conducts vulnerability information with the stakeholders regularly. The company established and maintained the hardware for potential vulnerabilities (ID.RA-08).	Not sure how the company maintained the software (ID.RA-08).	-	-
The company has a process to assess the authenticity of hardware and verify the integrity of software before it is used (ID.RA-09).	Not sure if the company has a process to assess the authenticity of hardware and verify the integrity of software after being used (ID.RA-09).	-	-
-	-	-	-
-	-	-	-
-	-	-	-
The company has a meeting periodically with suppliers and has	-	-	-



a learning session with them (ID.IM-03).			
-	-	-	-

Highlight company Strength in **Identify**.

#### 2.2.1 Strength

1. **Inventories of hardware (ID.AM-01):** The organization's hardware is well stored locally and maintained by the organization itself, they are not choosing third-party storage to store their hardware.
2. **Inventories of software (ID.AM-02):** The organization is good at managing its software because its software, systems, and services are managed by themselves, and this is a good thing for responding to threats from outside parties.
3. **Representation organization's authorized network (ID.AM-03):** These organizations have good network security because they control the basic lines of communication and data flow over wired and wireless networks, and they document network ports, protocols, and services that are updated whenever there are changes. This can be a good step in finding out what problems or threats will be faced in the future.
4. **Inventories of services (ID.AM-04):** The organization or company is good at service and already has suppliers that provide IaaS, PaaS, and SaaS services. and the IT team is responsible for maintaining and updating the services provided by the supplier.
5. **Inventories of services (ID.AM-05):** The company carries out asset monitoring periodically to check the asset priority scale and to update the assessment.
6. **Inventories of data and corresponding metadata (ID.AM-07):** The company checks every month to ensure that there are no data inconsistencies, in this case data records and several data, and

there are procedures that must be carried out if changes or updates occur according to the type of data.

7. **Vulnerabilities in assets (ID.RA-01):** The company always updates and reviews the processes and procedures carried out to mitigate risk.
8. **Cyber threat intelligence (ID.RA-02):** The company always checks every month to ensure the accuracy of the data assessed by the company.
9. **Risk responses (ID.RA-06):** The company always has a plan to mitigate risks and always updates it regularly.
10. **Processes for receiving, analyzing, and responding (ID.RA-08):** The company carries out vulnerability information with stakeholders on a regular basis, and the company always maintains its hardware that has potential vulnerabilities.
11. **The authenticity and integrity (ID.RA-09):** The company carries out a process to assess and check the originality of their hardware and verify the integrity of their software before use and what has already been used.
12. **Improvements are identified (ID.IM-03):** The company holds regular meetings with suppliers and has learning sessions.

Highlight company weakness in **Identify**.

#### 2.2.2 Weakness

1. **Inventories of hardware (ID.AM-01):** This company has a weakness because their inventory management comes from the Jababeka Center. This could be a problem for management if parties from outside the company see the company's inventory and data leaks could occur.
2. **Inventories of software (ID.AM-02):** The one who handles maintenance problems is not from the IT team.

3. **Inventories of services (ID.AM-05):** Not being sure how often a company tracks and updates its assets can create future weaknesses for the company.
4. **Vulnerabilities in assets (ID.RA-01):** The company not implementing time for updates and the company not using tools or monitoring the vulnerabilities which can cause serious problems in the future.
5. **Cyber threat intelligence (ID.RA-02):** The company does not have criteria or a basis for assessing or evaluating cyber perpetrators. This could be a serious problem. Punishment sanctions are not implemented and their TTP is still not implemented.
6. **Improvements are identified (ID.RA-03):** The company not handling something like this can be categorized as a weakness due to inadequate security in the face of external and internal threats.
7. **Risk responses (ID.RA-06):** There is no specified time for the company to update.
8. **Processes for receiving, analyzing, and responding (ID.RA-08):** Uncertainty in how companies maintain their software.
9. **The authenticity and integrity (ID.RA-09):** Unsure whether the company has a process for assessing the authenticity of the hardware and verifying the integrity of the software after use. This uncertainty can reduce the integrity of the company.

Highlight company opportunities in **Identify**.

#### 2.2.3 Opportunity

1. **Inventories of hardware (ID.AM-01):** Provides rules and regulations for the management of Jababeka centers and provides additional security for an organization's inventory.
2. **Representation organization's authorized network (ID.AM-03):** The company must update the documentation periodically.

3. **Inventories of services (ID.AM-04):** The company IT team must be more responsible in maintaining service and suppliers must provide service and must stay in touch to avoid anything undesirable
4. **Vulnerabilities in assets (ID.RA-01):** The company must use tools to monitor vulnerabilities and monitoring regularly.
5. **Cyber threat intelligence (ID.RA-02):** Companies must evaluate tactics, techniques, and procedures (TTP) and implement policy criteria against cybercriminals to prevent future threats
6. **Improvements are identified (ID.RA-03):** Convene or form a credible security team division to handle threats or matters related to cyber security to prevent future threats

Highlight company threats in **Identify**.

#### 2.2.4 Threats

1. **Inventories of hardware (ID.AM-01):** Threats can occur from outside or inside because organizations do not directly manage their inventory, theft and data leaks can occur from inside or outside
2. **Inventories of services (ID.AM-04):** This can happen because the IT team is not responsible in their work and suppliers can also commit fraud, here the actors can occur outside or within the organization
3. **Vulnerabilities in assets (ID.RA-01):** Threats can occur at any time and the company does not use tools or technology to monitor the vulnerabilities and could become a very big problem if this problem is not resolved in the near or long term
4. **Cyber threat intelligence (ID.RA-02):** Looking at data leaks or inappropriate access or information that can be obtained from other employees within the organization and data breaches or data leaks can happen at any time

5. **Internal and external threats (ID.RA-03):** Threats can occur from outside or inside, due to a lack of security arrangements and this can happen due to a lack of security

### 3. PROTECT (PR):

**PROTECT (PR):** Safeguards to manage the organization's cybersecurity risk are used

#### 3.1 Overview

The company demonstrates a strong commitment to safeguarding its cybersecurity infrastructure by implementing a variety of strategies and tools. These include using a request portal and a dedicated group for access control, employing encryption techniques like SHA-256 and MD5 for data security, and ensuring authenticity with official hardware and licensed software. The company also emphasizes physical security with CCTV and restricted server room access, while cloud-based and mirrored backup solutions support data integrity and availability.

How many YESES does the company fulfill in the **Protect** category?

The company fulfills 19 YESES in the **Protect** subcategory based on the interview analysis from 22 subcategories.

#### 3.2 SWOT Analysis to Protect

Strength	Weakness	Opportunity	Threats
The company uses a request portal to manage data access before access is granted (PR.AA-01).	The labeling is only done for Jababeka's existing inventory on site (PR.AA-01).		
The company has documentation procedures and does regular reviews every			

week through weekly reports (PR.AA-02).			
The company uses official and authentic hardware (PR.AA-03).	Not sure what the company does to authenticate users and services (PR.AA-03).	The company should do authentication for users and services (PR.AA-03).	
-	-	-	-
The company has a group that manages access control to ensure that separation of duties is maintained (PR.AA-05).			
The company has CCTV to protect every asset that is monitored every hour, and there is a server room that cannot be visited by third parties (PR.AA-06).		The server room should be protected (PR.AA-06).	
There is cyber security training for the employees (PR.AT-01).		The company should test the employees about cyber security regularly (PR.AT-01).	
The internals at Fablab are the ones who provide training for employees (PR.AT-02).		The internals should train employees from the entire division of a particular division (PR.AT-02).	
The company uses third-party software for the database. To protect data integrity, they implement data encryption using SHA-256 and MD5 to protect data. (PR.DS-01)			
The company uses Microsoft Teams and third-party digital signatures with specific requirements, has automatic encryption and uses internal	the company doesn't block emails from external communications, only categorize them, which could be seen as a		

emails from FebLab within their organization. (PR.DS-02)	potential security risk.(PR.DS-02)		
The company protects the CIA of data with support from Jababeka and also has specific internal communication procedures for accessing the data (PR.DS-10).			
The company uses cloud backup with mirror backup. They also monitor internet connectivity and check data integrity(PR.DS-11)	The company rarely backs up critical data which is monthly and other data every six months. (PR.DS-11)		
The company implements limiting data access to devices registered in the system and assigns role-based privileges to control information access. The company also uses paid licenses to ensure all software is registered (PR.PS-01)			
		Other employee should be introduced about how software is maintained, replaced, and removed(PR.PS-02)	
The company regularly checks data containing the serial numbers of each hardware to determine if it is outdated and selects hardware according to each user's tasks to ensure routine maintenance can be			

performed without interrupting their work.(PR.PS-03)			
The company maintains logs of all activities and reports, including tests to check for unauthorized access attempts, which are also recorded in the logs.(PR.PS-04)			
All the applications that company use are official and are carried out in the IT department to verify integrity.(PR.PS-05)			
The company examines the OSI layer based on the software and the end-to-end flow as well.(PR.PS-06)			
The company categorizes or segments the network into internal and external networks.(PR.IR-01)			
The company use cloud databases which allows easy recovery(PR.IR-02)			If the cloud database is faced by environmental threats, the data can't be backed up and recovered. (PR.IR-02)
The company performs backups that can be immediately redirected and checks for system failures from the logs. (PR.IR-03)			
The company monitors the bandwidth and storage regularly(PR.IR-04)		The lack of current forecasting presents an opportunity to implement this practice to better plan for future resource needs and growth.(PR.IR-04)	The company doesn't have backup for power supply(PR.IR-04)



### 3.2.1 Strength

1. **Authentic Hardware and Software(PR.AA-03 & PR.PS-01):** By utilizing official and registered tools, the company reduces the risk of vulnerabilities associated with counterfeit or unlicensed products.
2. **Physical Security Measures(PR.AA-06):** The use of CCTV and restricted access to server rooms add an additional layer of protection for critical assets.
3. **Employee Cybersecurity Training(PR.AT-01):** Cybersecurity training is provided to employees, improving awareness and preparedness against cyber threats.
4. **Strong Data Encryption Practices(PR.DS-01):** The use of SHA-256 and MD5 for data encryption demonstrates a commitment to protecting data integrity and confidentiality.
5. **Cloud and Mirror Backup Solutions(PR.DS-11):** Cloud-based and mirrored backups ensure data integrity and availability, providing robust recovery options.
6. **Comprehensive Activity Logging(PR.PS-04):** Activity logs and tests for unauthorized access attempts are maintained, enhancing monitoring and security.
7. **Segmentation and Monitoring(PR.IR-01):** Network segmentation and regular monitoring of bandwidth and storage contribute to enhanced cybersecurity and operational efficiency.

### 3.2.2 Weakness

1. **Incomplete Inventory Labeling(PR.AA-01):** Labeling is limited to Jababeka's existing inventory on-site, which may result in oversight and mismanagement of assets not covered under current procedures.

2. **Inadequate Email Security Measures(PR.DS-02):** The company does not block external emails, only categorizes them, which poses a potential security risk and increases vulnerability to phishing and malware attacks.
3. **Infrequent Data Backups(PR.DS-11):** Critical data is backed up only monthly, and other data every six months, which could lead to significant data loss in case of a system failure or cyber incident.

### 3.2.3 Opportunity

1. **Improve Server Room Security(PR.AA-06):** Strengthening physical security measures for the server room will better protect critical infrastructure from unauthorized access and potential threats.
2. **Regular Employee Cybersecurity Testing(PR.AT-01):** Conducting regular cybersecurity assessments for employees will help ensure they are prepared to handle threats and follow security protocols effectively.
3. **Software Maintenance Training(PR.PS-02):** Educating employees on software maintenance, replacement, and removal procedures will improve software management and reduce vulnerabilities.
4. **Implement Forecasting Practices(PR.IR-04):** Developing forecasting capabilities can improve planning for future resource needs and growth, enhancing the company's ability to adapt and scale efficiently.

### 3.2.4 Threats

1. **Environmental Vulnerabilities to Cloud Databases(PR.IR-02):** The company risks significant data loss and operational disruptions if environmental threats impact cloud databases, as backup and recovery processes may be compromised.

2. **Lack of Redundant Power Supply (PR.IR-04):** Without backup power solutions, the company is vulnerable to operational disruptions and data loss during power outages.

#### 4. DETECT (DE)

DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed

##### 4.1 Overview

The Company uses a variety of methods and strategies to spot possible intrusions and attacks on cybersecurity. Important tasks include reviewing credential records, monitoring unusual access patterns, and keeping an eye out for anomalies in networks and physical environments. The IT department is primarily in charge of these tasks, which include monitoring and detection. They ensure that the network and service traffic are thoroughly inspected for any potential negative events. Automated logging and notification systems are in place to alert the relevant personnel to potential threats.

In the **Detect** category, We found out that there are 9 YESSES out of 11 subcategories.

##### 4.2 SWOT Analysis to Protect

Strength	Weakness	Opportunity	Threats
Fablab continually keeps monitoring services and network activities to find any potential threats (DE.CM-01).			
The organization has automated logging for a credential reader logs, and alerts are sent for potentially harmful activities (DE.CM-02)			

Consistently keeping a check on user or staff activity logs. <b>(DE.CM-03)</b>			Serious security breaches can result from inadequate tools to detect internal threats and inadequate monitoring of internal activity. <b>(DE.CM-03)</b>
The organization here will use internal services, which will minimize the impact on external providers. <b>(DE.CM-06)</b>	Due to the lack of control over external service providers, it can be dangerous if an individual or department uses that provider. <b>(DE.CM-06)</b>	The risks connected to using third-party services can be reduced by creating monitoring strategies for external service providers. <b>(DE.CM-06)</b>	External providers could cause vulnerabilities if not periodically monitoring. <b>(DE.CM-06)</b>
	The methods and tools that Fablab uses within the company to identify phishing, malware, data leaks, and exfiltration have not been properly validated and tested. <b>(DE.CM-09)</b>	Using these advanced tools can improve the ability to perform a detection, especially for malware, phishing, and data theft. <b>(DE.CM-09)</b>	The ever-evolving cyber threat landscape, including sophisticated phishing attacks, advanced malware, and data exfiltration techniques, presents ongoing challenges. <b>(DE.CM-09)</b>
IT departments use tools like SIEM to continuously monitor logs and also identify malicious activities that could occur to the company. <b>(DE.AE-02)</b>		Improve the overall security posture in the Fablab and can improve the accuracy of threat detection by incorporating the latest cyber threat intelligence into log analysis tools. <b>(DE.AE-02)</b>	
Fablabs collects data from multiple sources. <b>(DE.AE-03)</b>	Although log analysis is performed using tools such as SIEM, Fablab does not consistently use these tools to integrate threat intelligence. <b>(DE.AE-03)</b>	Fablab detection and reaction to security incidents can be significantly improved simply by integrating threat intelligence and using SIEM tools consistently across the organization. <b>(DE.AE-03)</b>	Inadequate resources for IT and security teams can make it difficult to implement and maintain sophisticated monitoring and detection systems, which can result in security vulnerabilities. <b>(DE.AE-03)</b>
	There is no formal ticketing system to	Implementing a structured ticketing	

	document and track incidents as they occur, nor are there any tools or software specifically designed to alert on threats. <b>(DE.AE-06)</b>	system and tools for alerting, reporting, tracking, and managing incidents will be easier. This will result in faster resolution and better follow-up. <b>(DE.AE-06)</b>	
			Fablabs may be under greater pressure to constantly update and improve their monitoring and detection capabilities due to increasing regulatory requirements for cybersecurity and data protection at all times. <b>(DE.AE-08)</b>

#### 4.2.1 Strength

1. **Continuous Monitoring (DE.CM-01):** The Organization continuously monitors network activity and services to detect potential threats that can be affected at any time.
2. **Automated Logging and Alerts (DE.CM-02):** The Response times will be improved with the automated systems that could log credential reader activity and it will issue alerts to the potentially malicious external or internal activity that can cause a threat.
3. **Personnel Activity Monitoring (DE.CM-03):** User and staff activity logs are continuously checked, contributing to internal security.
4. **Internal Monitoring Capabilities (DE.CM-06):** The organization primarily uses internal services, minimizing reliance on potentially less secure external providers.
5. **Log Analysis Tools (DE.AE-02):** Tools like SIEM are used by the IT department to monitor logs and identify malicious activities, aiding in comprehensive threat detection.

6. **Multi-Source Information Correlation (DE.AE-03):** Data is collected from multiple sources, improving the ability to detect and analyze potential threats.

#### 4.2.2 Weakness

1. **Inadequate Tools for Internal Threats (DE.CM-03):** There is a lack of adequate tools to detect internal threats, which can lead to serious security breaches.
2. **Limited Monitoring of External Providers (DE.CM-06):** Insufficient monitoring of external service providers can be risky if these providers are used without proper oversight.
3. **Inadequate Phishing and Malware Detection (DE.CM-09):** Current methods and tools for detecting phishing, malware, and data leaks have not been properly validated and tested.
4. **Inconsistent Use of SIEM Tools (DE.AE-03):** While log analysis is performed using SIEM tools, these tools are not consistently used to integrate threat intelligence.
5. **No Comprehensive Reporting Tools (DE.AE-06):** The absence of a formal ticketing system to document and track incidents and lack of specific tools for alerting on threats can hinder effective incident management.

#### 4.2.3 Opportunity

1. **Adoption of Advanced Monitoring Tools (DE.CM-09):** Using advanced tools for detecting malware, phishing, and data theft can improve detection capabilities.
2. **Enhanced External Provider Monitoring (DE.CM-06):** Developing strategies for monitoring external service providers can mitigate risks associated with third-party services.
3. **Utilize Cyber Threat Intelligence (DE.AE-02):** Incorporating the latest cyber threat intelligence into log analysis tools can improve threat detection accuracy and overall security posture.

4. **Standardization in SIEM Usage (DE.AE-03):** Consistently using SIEM tools and integrating threat intelligence can significantly enhance the organization's detection and reaction to security incidents.
5. **Improve Reporting and Documentation Systems (DE.AE-06):** Implementing a structured ticketing system and tools for alerting, reporting, tracking, and managing incidents can lead to faster resolution and better follow-up.

#### 4.2.4 Threats

1. **Emerging Cyber Threats (DE.CM-09):** The evolving cyber threat landscape, including sophisticated phishing attacks, advanced malware, and data exfiltration techniques, presents ongoing challenges.
2. **Third-Party Risks (DE.CM-06):** External service providers could introduce vulnerabilities if not adequately monitored.
3. **Inadequate Resource Allocation (DE.AE-03):** Potential security risks may arise from lack of funding IT and security teams' ability to deploy and maintain complex monitoring and detection systems.
4. **Compliance and Regulatory Pressure (DE.AE-08):** The organization may face increasing regulatory requirements for cybersecurity and data protection, necessitating constant updates and improvements to monitoring and detection capabilities.

## 5. RESPOND (RS)

**RESPOND (RS):** Actions regarding a detected cybersecurity incident are taken.

### 5.1 Overview

The company has an organized and structured response to incidents. When an attack occurs, the company prioritizes understanding the attack before focusing on recovery and reporting. Attacks are categorized according to their threat level, and the most serious attacks are immediately escalated to senior management for action. In addition to its response strategy, the company has implemented structured communication protocols to ensure efficient incident handling. The IT team has a policy of regularly reviewing logs to conduct in-depth incident analysis, which helps to identify patterns and mitigate future threats. The company also takes great care to maintain detailed records during the investigation process. Access to these records is strictly controlled and requires a formal request from within the organization. This policy ensures that unauthorized external parties cannot easily retrieve sensitive incident information, thus maintaining the integrity of the investigation and the confidentiality of the data.

How many YESES does the company fulfill in the **Respond** category?

The company fulfills 11 YESES in the Respond subcategory based on the interview analysis from 13 subcategories.

### 5.2 SWOT Analysis to Respond

Strength	Weakness	Opportunity	Threats
All reports will be made after the incident is first identified and mitigated (RS.MA-01)	Delay in incident reports due to analyzed and mitigated process (RS.MA-01)	-	The risk associated with delayed reporting is that it may lead to an increased impact before the incident is formally reported (RS.MA-01)



Reports of high-level attacks are immediately relayed to upper management (RS.MA-02)	Regular attack reports are only at the IT department level allowing for an insufficient attention (RS.MA-02)	-	-
Categorisation of incidents by asset such as, software and hardware enables a structured approach (RS.MA-03)	-	Developing more comprehensive incident categories, organizations (RS.MA-03)	-
Monthly reports from the cloud by IT team help ensure that incident status is tracked consistently and accurately (RS.MA-04)	Reliance on the IT team for incident status tracking can result in delays (RS.MA-04)	-	-
Having a clear IT policy to initiate the recovery process from scanning logs can direct the right actions (RS.MA-05)	-	-	-
The IT department is at the forefront of incident responses since they are skilled at responding to and mitigating incidents (RS.AN-03)	There are anomalies that cannot be indicated potentially as a gap. (RS.AN-03)	Ensuring each anomaly can be tracked down. (RS.AN-03)	-
The company makes sure that only authorized personnel can access records. (RS.AN-06)	-	-	Attackers from the outside could target record-keeping systems in an effort to change or remove investigation records. (RS.AN-06)
Data integrity is protected by the organization's policy of not disclosing internal data to anyone outside of the relevant parties. (RS.AN-07)	Might be dangerous if there are problems with network connectivity or the NTP server. (RS.AN-07)	-	Any NTP setup error or misconfiguration (RS.AN-07)

The IT department reviews other possible incident targets. reliance on the IT staff to employ automated technologies to look for persistence evidence and signs of compromise (RS.AN-08).	If the IT department is the only one handling these activities, bottlenecks may result. (RS.AN-08)	The incident management process as a whole can be improved by encouraging collaboration between IT and other departments. (RS.AN-08)	-
Attack logs are submitted along with an explanation of potential measures to internal senior management (RS.CO-02).	There is no specific explanation how the stakeholder being notified would be the weakness.(RS.CO-02)	Using automated system to notify stakeholders can ensure to sent notification consistently.(RS.CO-02)	Delay in notify to the stakeholders could make slower incident response.(RS.CO-02)
The approach is designed to provide a sense of security, which can help maintain internal morale and prevent external reputational damage.(RS.CO-03)	Transparency problems might result from the policy of not reporting incidents to external stakeholders. (RS.CO-03)	Developing an open reporting procedure that, where necessary, involves external stakeholders may increase compliance and trust.(RS.CO-03)	Limited internal reporting could lead to misinformation or misunderstandings. (RS.CO-03)
Company uses individual method depend for what incident make it more effective to respond any type of incident (RS.MI-01)	It may take a lot of time and resources to respond to each type of incident. (RS.MI-01)	Periodically training for employees to help become familiar to each type of incident. (RS.MI-01)	Increasing complexity of cyber attack, the organization may face challenges in adapting new types of incident. (RS.MI-01)
-	The lack of automated and manual eradication capabilities exposes the organization to long-term consequences resulting from incidents. (RS.MI-02)	Investing in safety measures that can be fully automated can improve the organization's capacity(RS.MI-02)	As cyber attacks get more complex and common, a lack of eradication tools may cause situations to worsen and last longer. (RS.MI-02)

### 5.2.1 Strength

1. **Incident Reporting (RS.MA-01):** The company waits to report incidents until their impact is known and mitigated, ensuring that reporting is more accurate and relevant. This reduces the risk of disseminating incorrect or incomplete information.
2. **Reporting Prioritization (RS.MA-02):** By delivering cybersecurity reports directly to higher-ups, organizations ensure that incidents receive higher attention and appropriate prioritization, expediting necessary actions.
3. **Categorization by Asset (RS.MA-03):** By categorizing incidents by assets such as hardware and software, organizations can group incidents in a structured way, making handling and response easier.
4. **Monthly Reports From The Cloud (RS.MA-04):** The use of monthly reports by the IT team from the cloud helps to ensure that the status of incidents is tracked consistently and accurately.
5. **Clear IT Policies (RS.MA-05):** Having a clear IT policy for starting the recovery process from scanning logs can direct the right actions.
6. **Incident Analysis (RS.AN-03):** The IT department is at the forefront of incident responses since they are skilled at responding to and mitigating incidents.
7. **Controlled Access to Records (RS.AN-06):** The company ensures that only authorized personnel can access records. This helps maintain the integrity and security of sensitive information.
8. **Data Integrity Protection (RS.AN-07):** Data integrity is protected by the organization's policy, this ensures that sensitive information remains secure.
9. **Incident Target Review and Automated Analysis (RS.AN-08):** The IT department reviews other possible incident targets this helps in identifying the potential threats before causing the damage.

10. **Incident Reporting to Senior Management (RS.CO-02):** Attack logs are submitted to internal senior management to ensure they are informed of incidents and can make decisions to mitigate the impact.
11. **Security and Morale (RS.CO-03):** The approach is designed to provide a sense of security, which can help maintain internal morale and prevent external reputational damage.
12. **Incident-Specific Response Methods (RS.MI-01):** The company uses individual methods depending on the type of incident, making it more effective to respond to any specific incident.

#### 5.2.2 Weakness

1. **Delayed Incident Reporting (RS.MA-01):** Delaying reporting an incident until its impact is confirmed and mitigated may cause delays in involving third parties or authorities.
2. **Reporting Limitations (RS.MA-02):** Reports unrelated to cybersecurity are only received by the IT department, which may not get adequate attention from upper management, causing a slow response to incidents.
3. **Reliance on the IT Team (RS.MA-04):** Reliance on the IT team for incident status tracking can result in delays or lack of transparency in incident status reports.
4. **Anomaly Detection Gaps (RS.AN-03):** There are anomalies that cannot be indicated, potentially gaps in the monitoring and detection systems.
5. **Network Connectivity and NTP Server Issues (RS.AN-07):** There might be dangers if there are problems with network connectivity or the NTP server.
6. **Potential Bottlenecks (RS.AN-08):** If the IT department is the only one handling these activities, bottlenecks may result. This could lead to delays in incident response.

7. **Lack of Specific Notification Procedures (RS.CO-02):** There is no specific explanation of how stakeholders are notified, which could lead to gaps in communication.
8. **Transparency Issues (RS.CO-03):** Transparency problems might result from the policy of not reporting incidents to external stakeholders.
9. **Resource-Intensive Response (RS.MI-01):** It may take a lot of time and resources to respond to each type of incident.
10. **Exposure to Long-Term Consequences (RS.MI-02):** The lack of automated and manual eradication capabilities exposes the organization to long-term consequences resulting from incidents.

#### 5.2.3 Opportunity

1. **Incident Category Development (RS.MA-03):** By developing more comprehensive incident categories, organizations can more effectively identify, address, and prevent different types of attacks.
2. **Enhanced Anomaly Tracking (RS.AN-03):** Ensuring each anomaly can be tracked down provides an opportunity to enhance the organization's monitoring.
3. **Cross-Departmental Collaboration (RS.AN-08):** The incident management process as a whole can be improved by encouraging collaboration between IT and other departments.
4. **Automated Notification Systems (RS.CO-02):** Using automated systems to notify stakeholders can ensure that notifications are sent consistently.
5. **Open Reporting Procedure (RS.CO-03):** Developing an open reporting procedure that, where necessary, involves external stakeholders may increase compliance and trust.
6. **Regular Employee Training (RS.MI-01):** Periodically training employees to help them become familiar with each type of incident.

7. **Investment in Automated Safety Measures (RS.MI-02):** Investing in safety measures that can be fully automated can improve the organization's capacity to respond to incidents.

#### 5.2.4 Threats

1. **The Risk of Delaying Reports (RS.MA-01):** The company faces the risk of late reporting. Delays in incident reporting may result in greater repercussions, such as reputational damage or more significant financial losses, before appropriate action can be taken.
2. **External Threats to Record-Keeping Systems (RS.AN-06):** Attackers from the outside could target record-keeping systems in an effort to change investigation records.
3. **NTP Setup Errors or Misconfigurations (RS.AN-07):** Any NTP setup error or misconfiguration could lead to inaccuracies in time-stamped data.
4. **Delayed Notifications (RS.CO-02):** Delays in notifying stakeholders could result in slower incident response times.
5. **Limited Internal Reporting (RS.CO-03):** Limited internal reporting could lead to misinformation or misunderstandings
6. **Complexity of New Cyber Attacks (RS.MI-01):** The organization may face challenges in adapting to new types of incidents.
7. **Lack of Eradication Tools (RS.MI-02):** A lack of eradication tools may cause situations to worsen and last longer

## 6. RECOVER (RC)

**RECOVER (RC):** Assets and operations affected by a cybersecurity incident are restored

### 6.1 Overview

Through port security, attack route analysis, and data quarantining, Fablab Jababeka handles recovery. In addition to using defenders, firewalls, and log analysis, they also use file hashing and inspections to confirm the integrity of backups. By handling recovery internally, cutting off external networks, and completing recovery according with predetermined guidelines and thorough documentation, they maintain control and security. Difficulties with manual verification, interruptions in operations, and insufficient external communication are among the challenges.

How many YESES does the company fulfill in the **Recover** category?

Fablab Jababeka fulfills 7 YESES from 8 questions during interview for the **Recover** category

### 6.2 SWOT Analysis to Recover

Strength	Weakness	Opportunity	Threats
Before starting recovery procedures, Fablab Jababeka verifies the safety of all ports, analyzes potential attack routes, and guarantees data quarantine. (RC.RP-01)	Initial checks may not be as effective as they could be because of the lack of knowledge about the methods of attack. (RC.RP-01)	Using advanced quarantine methods might improve response times and results. (RC.RP-01)	-
Solid recovery procedures are guaranteed by detailed log analysis and running firewalls and defenders. (RC.RP-02)	Plans for recovery are updated randomly meaning that new threats might not be recognized at the time. (RC.RP-02)	To improve resiliency, apply tools for predictive analysis and regular updates based on new threat intelligence. (RC.RP-02)	It's possible that new cyberthreats won't be immediately identified from previous logs. (RC.RP-02)

Fablab conducts detailed hardware inspections and uses file hashing to ensure that backups are intact and unaltered. (RC.RP-03)	Integrity checks that depend only on manual verification procedures may be difficult to detect. (RC.RP-03)	-	Hardware issues and ransomware attack could be the most problem to do recovery (RC.RP-03)
Control and security are maintained through internal recovery and disconnection from external networks. Cybersecurity risk management is integrated with internal policies and attack reporting. (RC.RP-04)	Communication and operations are disrupted when external connections are disconnected. (RC.RP-04)	-	-
Data integrity is ensured by automatic cloud mirror backups. (RC.RP-05)	-	Reliability can be improved by using several backup sources and thorough checks. (RC.RP-05)	-
Identifying the completion of recovery requires precise standards based on the damage scale. Accurate incident records are guaranteed by the IT team's thorough documentation. (RC.RP-06)	Subjective criteria could result in inconsistent results. The process of documentation can take a long time. (RC.RP-05)	-	-
By using Microsoft Teams, the organization efficiently updates internal stakeholders on recovery progress. (RC.CO-03)	Lack of communication with outside parties may result in problems with transparency. (RC.CO-03)	-	-



There is a process established for informing executives about incidents. (RC.CO-04)	There's no specific procedure for updating the public or steps to clarify recovery and prevent similar incidents in the future. (RC.CO-04)	-	-
---	--	---	---

### 6.2.1 Strength

1. **Pre-Recovery Safety Checks (RC.RP-01):** Before starting recovery procedures, verifies port security, examines potential attack routes, and makes sure data is quarantined.
2. **Solid Recovery Strategies (RC.RP-02):** Defenders, firewalls, and in-depth log analysis are used to support recovery efforts.
3. **Backup Integrity (RC.RP-03):** Ensure that backups are complete and unaltered by performing thorough hardware checks and using file hashing.
4. **Control and Security (RC.RP-04):** Combines cybersecurity risk management with internal policies, recovers internally, disconnects from external networks, and upholds control and security.
5. **Reliable Recovery Standards (RC.RP-06):** Maintains accurate incident records through comprehensive IT documentation and specifies recovery completion using standards based on damage scales.

### 6.2.2 Weakness

1. **Difficulties with Manual Verification (RC.RP-03):** Identifying problems could be difficult if integrity checks were to be performed completely manually.
2. **Disruption of Operations (RC.RP-04):** Disabling external connections may cause problems with operations and communication.

3. **Lack of Transparency (RC.CO-03):** Transparency problems can result from poor interaction with outside parties.

#### 6.2.3 Opportunity

1. **Advanced Quarantine Methods (RC.RP-01):** Improving response times using modern techniques for quarantine.
2. **Predictive Analysis and Threat Intelligence (RC.RP-02):** Resilience and preparation could be improved by using predictive analysis tools and routinely updating recovery plans
3. **Improved Backup Dependency (RC.RP-05):** Increasing dependability through various emergency plans and comprehensive reviews.

#### 6.2.4 Threats

1. **Unidentified Cyberthreats (RC.RP-02):** It may take some time to detect new cyberthreats from previous logs.
2. **Recovery Difficulties (RC.RP-03):** Major challenges to recovery attempts could come from ransomware attacks and hardware problems.

## Conclusion

In summary, the security compliance and audit report for Fablab Jababeka gives a detailed look at the current state of the organization's cybersecurity. The assessment shows several strong points, such as good pre-recovery safety checks, solid recovery strategies, reliable backups, and strong data encryption. These actions help make the organization more secure and resilient.

However, the report also finds some weaknesses, such as problems with manual verification, disruptions during external disconnections, and weak email security. Fixing these weaknesses is important to improve the organization's cybersecurity.

The opportunities section suggests possible improvements, like better quarantine methods, predictive analysis tools, regular employee cybersecurity tests, and improved server room security. By taking these opportunities, Fablab Jababeka can further strengthen its cybersecurity and efficiency.

The report also mentions several threats, like unknown cyberthreats, difficulties in recovering from ransomware attacks, and vulnerabilities in cloud databases. These threats highlight the need for continuous monitoring, regular updates, and strong risk management to protect the organization's assets and data.

Overall, while Fablab Jababeka has an adequate base in cybersecurity, ongoing efforts to fix weaknesses and use opportunities will be crucial to maintaining and improving its security in the face of evolving cyber threats. The organization's focus on cybersecurity training, regular policy updates, and working with stakeholders will be key to achieving long-term resilience and compliance with industry standards.