Assessment Report for «PhM», Pharmaceutical Manufacturing Company

Anastasiia Belousova (Student ID: 2088387)
June 10, 2023

Abstract

The report is carried out based on the NIST CSF 1.1 [1]. The organisation under consideration is pharmaceutical manufacturing company «PhM». In Section 1, a brief description of the company is provided; in Section 2, the risk analysis is performed.

1 Company Description

Pharmaceutical manufacturing company «PhM» is engaged in the development and production of vital medicines. Some raw materials may often be supplied from different countries, the same way as the finished products are distributed all over the world.

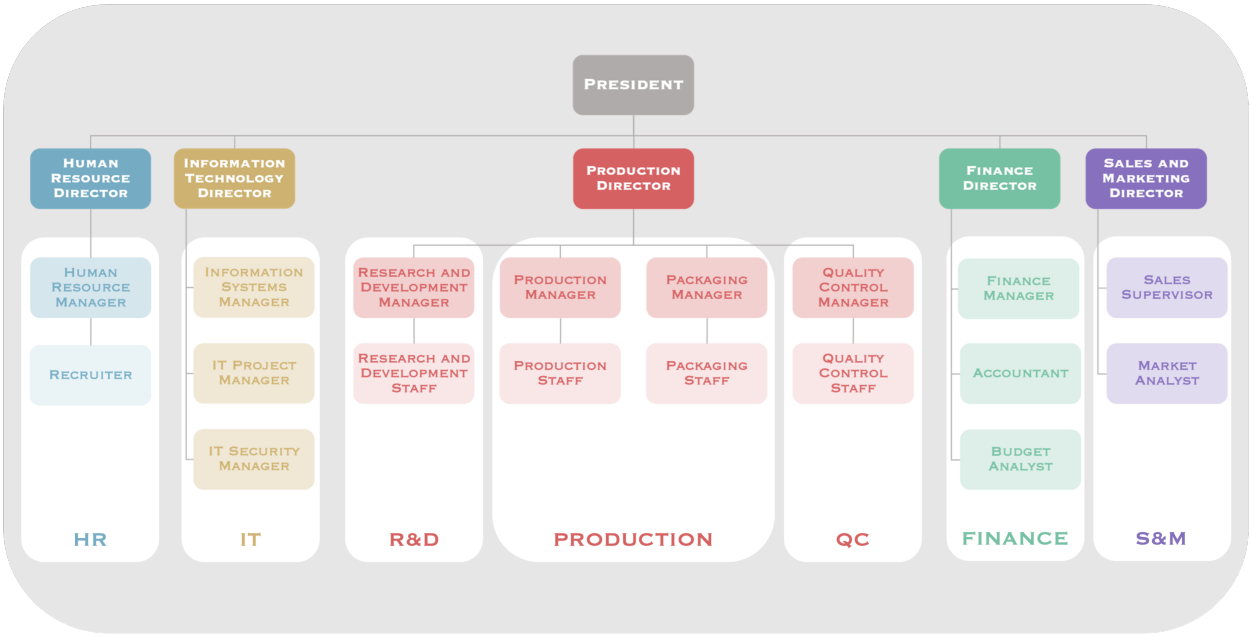

Figure 1: Company organisational chart

The company under consideration consists of the following 7 departments (Fig. 1):

1. **Research and Development** (R&D) department is where staff are engaged in identifying possible new production technologies and applications, and making improvements and modifications to existing production processes;
2. **Production** department deals with all stages of pharmaceutical product manufacture – from producing active ingredients to completion of finished products and packaging. These production processes are all carried out in strict adherence to both internal and external protocols;
3. **Quality Control** (QC) department is the functional area that monitors and documents activities, processes and products of manufacturing to ensure they meet strict standards and predefined expectations. Ultimately, this team ensures the safety of the drugs that go out for distribution [2];
4. **Sales and Marketing** (S&M) is responsible for finding out the need of the customer and fulfilling the need with the products and services of the organisation. This involves market research, setting prices, finding distribution channels, advertisements etc.;

5. **Finance** department acquires funds, manages and re-distributes the funds based on the budget planned for the financial year [3];
6. **Human Resource** (HR) department is charged with finding, recruiting, screening, and training job applicants [4];
7. **Information Technology** (IT) department ensures the continuous functioning of the manufacturing plant and its equipment.

Main processes are considered to be carried out in the first three departments – Production, R&D, and QC – therefore, the following assessment is conducted in relation to these subunits.

2 Risk Analysis

2.1 Business Environment (ID.BE)

«PhM» does not have an extensive understanding of its place in the supply chain of essential medicines. Considering the fact that the company deals with suppliers and distributors from multiple countries, security incidents during the product transportation to/from the plant can lead to severe consequences, including compromised product quality and patient safety.

Furthermore, the company has a comprehensive policy of maintaining the manufacturing process under normal conditions, but it lacks thorough procedures regarding the state when it is during/after an attack. Not having a clear insight of necessary actions threatens not only already mentioned patient safety, but also the manufacturing continuity.

The Compliance & Information Security function is asked to survey the company's current state of affairs in terms of security of the supply chain and to improve the existing policies to meet the following controls:

- **ID.BE-1**: Identification of the company's role in the supply chain allows to understand security risks associated with its third-party stakeholders such as vendors, suppliers, and distributors. It makes it less likely to have any security breaches related to production delivery.
- **ID.BE-5**: Determining the resilience requirements for all operating states allows the company to better prepare, respond, and recover from incidents, thus minimising the risks of interruption and deterioration of production.

2.2 Identity Management, Authentication and Access Control (PR.AC)

«PhM» does not manage the physical access to the production equipment at the proper level. The admission of unauthorized persons to a direct manufacturing process creates the risk of introducing foreign substances or tampering with the equipment, which can lead to contamination and/or adulteration of the produced medicines.

Since the company is also engaged in research and development of new drugs, without ascertaining that only proofed identity individuals can access the related data and interact with it, it is possible to have a leak of intellectual property or a change of sensitive research data.

Therefore, the Compliance & Information Security function is asked to implement, in collaboration with the Production and R&D departments, better regulations regarding the authentication and access control in line with the following requirements:

- **PR.AC-2**: Managing physical access to production equipment ensures that only authorized individuals with appropriate clearances are allowed near the manufacturing process. It decreases the risk of the resulting medicines alteration and reduced quality.
- **PR.AC-6**: Ascertaining that all activities are carried out by people with identities, proofed and bound to credentials and asserted in interactions, allows sensitive information protection and robust framework establishment. It minimises the probability of unauthorized access to sensitive assets and data manipulation/theft.

2.3 Awareness and Training (PR.AT)

«PhM» does not carry out enough trainings devoted to the information security education. The staff's lack of comprehension of their roles and responsibilities can lead to intentional or unintentional misuse of the sensitive data. Misuse of privileged access can also result in considerable damage to the company's systems, reputation, and data confidentiality. Moreover, it becomes challenging to assign accountability for security incidents, policy violations, or unauthorized actions.

Furthermore, it is crucial to clarify the roles and responsibilities of third-party stakeholders as well. Vendors, suppliers, and distributors play critical roles in the company's operations. If the risks associated with these stakeholders are not properly addressed, it can lead to disruptions in the supply chain and delays in production delivery.

The Compliance & Information Security function, in cooperation with the HR department, should carry out appropriate training programs for both internal staff and third-party stakeholders in order to comply with the following controls:

- **PR.AT-2**: Privileged users awareness of their responsibilities allows to enhance the overall accountability and effectiveness. It becomes less likely for the personnel to deviate from the established policies and procedures.
- **PR.AT-3**: Third-party stakeholders awareness of their responsibilities allows the production robustness and continuity, and reputation maintenance. It minimises the risk of missed deadlines and non-compliance with industry related regulations.

2.4 Data Security (PR.DS)

«PhM» does not implement a proper number of measures (e. g. access control, data classification) in order to protect stored sensitive information and records. Such data is subject to tampering and theft, which can lead to the exposure of the confidential patient and business records, intellectual property, and research information.

There are also possible issues regarding the data that is being transmitted between systems. Such unprotected data is liable to eavesdropping which can result, for instance, in the company's R&D data being compromised and research findings, clinical trial data, drug formulas being stolen.

The Compliance & Information Security function is asked to implement the necessary measures concerning stored and transmitted information to meet the following requirements:

- **PR.DS-1**: Data-at-rest protection allows to maintain the confidentiality, integrity, and availability of sensitive information. It minimises the risks of financial losses, legal liabilities, damage to reputation, and loss of customer trust.
- **PR.DS-2**: Data-in-transit protection ensures data confidentiality which reduces the risk of unauthorised third party being able to intercept the communication inside the company and steal the sensitive information.

2.5 Information Protection Processes and Procedures (PR.IP)

«PhM» does not appear to have a sufficient number of procedures that maintain the protection of the company's information systems and assets. The company is engaged in the manufacture of essential medicines, and so, failing to backup the data, crucial for its production, leads to supply interruptions which can endanger patient health.

The company should improve already implemented policies regarding data destruction. Information that is not securely destroyed can be retrieved and accessed by unauthorised individuals, from or out of the company. This can lead to data breaches, compromising sensitive information, intellectual property, patient data, or confidential business data.

- **PR.IP-4**: Managing and maintaining backups of information allows, in case of need, to restore data to a known, trusted state, ensuring its integrity, accuracy, and reliability. It minimises the risks of information loss, production interruptions, and delays.
- **PR.IP-6**: Proper data destruction ensures the security of sensitive information, which minimises the possibility of its use for unauthorized purposes.

References

[1] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1

[2] The Structure and Departments in a Pharmaceutical Manufacturing Company

[3] Various Departments and their functions in a Manufacturing Industry

[4] Human Resources (HR) Meaning and Responsibilities