| Identified risks | Potential Failure Mode | Potential Failure Effect | Severity (S) | Justification for Severity | Potential Causes | # | Occurrence (O) | Detectability (D) | Justification for Detectability | RPN (S * O * D) |
|---|---|---|---|---|---|---|---|---|---|---|
| Product Quality Loss | Reduced customer satisfaction, increased returns | Product quality degradation | 7 | The impact is high because product quality is a crucial element of customer satisfaction and could lead to repeated losses if left unchecked. | Delivery delays, inadequate storage conditions | | 6 | 6 | Quality control helps detect some losses, but delays add uncertainty to detection. | 252 |
| Automated System Failures and Online Command Failures | Delays in order processing | Customer dissatisfaction, revenue loss | 8 | The impact is high, but not catastrophic, as a backup solution could be put in place in the short term. However, the costs and disruptions are significant. | Technical failure, cyber attacks, outdated infrastructure | | 4 | 5 | These failures can be difficult to anticipate without real-time monitoring but can be detected quickly through system alerts. | 160 |
| Elevation of Privilege | Unauthorized modifications to critical systems, data loss | Sabotage or unauthorized system modifications | 6 | The impact is moderate, as while system manipulation is serious, it can be contained with disaster recovery solutions. | Weak access controls, insufficient user monitoring | | 5 | 5 | Privilege elevation can be detected with audit and monitoring systems, though they may not always alert immediately. | 150 |
| Denial of Service (DoS) | Website functionality loss, revenue loss | Website inaccessible, disruption of sales | 4 | The impact is low to moderate, as while it may result in lost revenue, DoS attacks can be mitigated or blocked quickly. | External attacks, system vulnerabilities | | 6 | 6 | DoS attacks are easy to detect once they start but difficult to anticipate. | 144 |
| Repudiation (Non-recognition of actions) | Disputes, financial penalties, operational inefficiency | Conflicts over responsibility for actions | 5 | The score is moderate, as logging systems help limit disputes, but it may take time to resolve these issues. | Poor action logging, lack of traceability | | 4 | 7 | Action traceability may fail, justifying a high detectability score. | 140 |

| Identified risks | Potential Failure Mode | Potential Failure Effect | Severity (S) | Justification for Severity | Potential Causes | # | Occurrence (O) | Detectability (D) | Justification for Detectability | RPN (S * O * D) |
|---|---|---|---|---|---|---|---|---|---|---|
| Tampering and Data Alteration | Financial loss, operational disruption | Incorrect modification of stock or data | 5 | The score is moderate, as these errors can be corrected with additional controls, but they would affect operational management and finances. | Insider threat, weak data integrity controls | | 5 | 5 | It's possible to detect these alterations, but it's not guaranteed, hence a medium score. | 125 |
| Supply Chain Delays | Delivery delays, product shortages | Customer dissatisfaction, financial loss | 7 | The impact is significant, especially if customers are affected on a large scale. | Customs delays, supplier issues, poor inventory management | | 4 | 4 | Many delays are predictable, but sudden disruptions, such as customs delays, are harder to forecast. | 112 |
| Spoofing and Unauthorized Access | Unauthorized access to customer data, manipulation of orders or stock | Alteration of customer data | 6 | The impact is moderate, as unauthorized access to data could be discovered quickly, but initial damages could be significant. | Weak authentication methods, phishing attacks | | 4 | 4 | Access surveillance helps, but it's insufficient for detecting all attempts. | 96 |
| Data Breach and Information Disclosure | Legal penalties (GDPR), reputation damage, customer trust loss | Loss of customer information | 9 | The score is high due to legal consequences and reputational impacts, which are critical aspects for any company handling sensitive customer data. | Weak data encryption, phishing attacks | | 3 | 3 | Detecting a data breach is often reactive, which justifies a low detectability score. | 81 |