ZTOWN

Internal Audit Report

Payments System Application Review

Report Rating	Needs Improvement

Observations Summary		
High	Medium	Low
-	2	1

Executive Summary

BACKGROUND

The audit of the organization's Payments System was conducted to assess the effectiveness and efficiency of the system's controls and processes. The Payments System plays a critical role in facilitating financial transactions, managing payment information, and ensuring the accuracy and integrity of payment processes.

The purpose of this audit was to provide management with an independent assessment of the Payments System's controls, highlighting areas of strength and areas that require improvement. The findings and recommendations outlined in this report aim to assist management in strengthening the system's controls, enhancing security measures, and improving overall operational efficiency and effectiveness.

SCOPE AND APPROACH

The scope of this audit will include the examination of the application controls within the Payments System of ZTOWN. It will encompass the entire payment processing lifecycle, starting from the initiation of transactions through to their final authorization and recording.

Scope Area	Relevant Matters
Governance	1. Business users sign-offs are obtained and documented
Data Input	1. Data input authorization and access management 2. Format and required field checks; standardized input screens
Data Processing	1. Error reports and audit trails are maintained and reviewed 2. Data backups are marinated, complete, and occur in a timely manner
Data Output	1. Output controls are designed and operating effectively to ensure that all transaction outputs are complete and accurate.

To achieve the audit objectives, the following approach was adopted:

1. Gain an understanding of the Payments System's architecture, configuration, and relevant policies and procedures.
2. Evaluate the design of the application controls, including access controls, authentication mechanisms, transaction processing rules, and segregation of duties.
3. Perform walkthroughs and testing of key controls to assess their operational effectiveness and adherence to established procedures.
4. Identify any control weaknesses or deviations and assess their impact on the reliability and security of the Payments System.

CONCLUSION

The audit of the organization's Payments System identified several key observations that require management's attention and action. These observations highlight weaknesses in input field validation, data backup practices, and access management controls, which, if left unaddressed, could expose the organization to various risks and vulnerabilities.
Further details regarding the audit findings and their management action plans will be presented in the subsequent sections of this report.

MANAGEMENT RESPONSE

Management has agreed to all observations raised in this report and actions plans to remediate risks have been developed with agreed target dates.

Detailed Observations

Opportunities to enhance the existing processes and improve the control environment are summarized below. The next section contains further details of these observations.

No.	Title	Summary	Rating
1	Input Validation Checks	The system lacks adequate validation and verification mechanisms for input fields, which increases the risk of inaccurate or fraudulent payment data being processed.	**Medium**
2	Payments System Backups	The organization only performs data backups once a year, which poses a significant risk to the availability, integrity, and recoverability of critical data.	**Medium**
3	Access Management	Review of user access records and permissions revealed a few instances where inactive or terminated employees still had active user accounts in the Payments System.	**Low**

Detailed Observations

1.	Input Validation Checks	Medium

Observation

During the audit of the organization's Payments System, a weakness was identified in the input field checks control. The system lacks adequate validation and verification mechanisms for input fields, which increases the risk of inaccurate or fraudulent payment data being processed.

During sample testing of payment data entry, it was observed that the system does not enforce mandatory fields or perform comprehensive data validations, allowing incomplete or invalid data to be accepted without appropriate error handling.

Impact

The absence of robust input field checks poses significant risks to the integrity and accuracy of payment data within the Payments System. Without proper validation and verification controls, erroneous or unauthorized information may be entered, leading to processing errors, payment discrepancies, and potential financial losses. Moreover, the lack of input field checks increases the organization's vulnerability to fraudulent activities, such as data manipulation or injection attacks.

Agreed Management Action(s)

IT will:

1. Implement comprehensive data validation and verification mechanisms for all input fields within the Payments System, including mandatory field enforcement, format checks, length restrictions, and input range validation.

Detailed Observations

2.	Payments System Backups	Medium

Observation

During the audit of the organization's data management practices, a weakness was identified in the data backup procedures. It was observed that the organization only performs data backups once a year, which poses a significant risk to the availability, integrity, and recoverability of critical data. Examination of backup logs and documentation revealed that data backups are performed only once a year, contrary to industry best practices and data protection standards. The extended time intervals between backups leave the organization vulnerable to data loss and limit the ability to recover systems and data in a timely manner.

Impact

The organization's reliance on an annual data backup practice significantly compromises data availability and recovery capabilities. Insufficient backup frequency exposes the organization to substantial risks, including prolonged system downtime, permanent data loss, business disruption, and compromised continuity. In the absence of regular and frequent backups, the organization faces an elevated threat of unrecoverable data, financial losses, regulatory non-compliance, and reputational damage.

Agreed Management Action(s)

IT will:

1. Review and update the data backup policy to establish a more frequent and robust backup schedule.
2. Implement automated backup solutions that ensure regular and reliable backups of critical data, systems, and configurations.

Detailed Observations

2.	Access Management	Low

Observation

During the audit of the organization's Payments System, some minor weaknesses were identified in the access management practices. While the access controls generally align with industry standards, there are a few areas where improvements can be made to enhance the overall security posture.
Review of user access records and permissions revealed a few instances where inactive or terminated employees still had active user accounts in the Payments System. Although the number of such accounts is limited, implementing a more efficient deprovisioning process will minimize the risk of unauthorized access.

Impact

Insufficient access controls increase the risk of unauthorized individuals gaining access to sensitive systems, applications, or data. This can result in data breaches, unauthorized modifications, or misuse of information, leading to potential financial losses, reputational damage, and regulatory non-compliance.

Agreed Management Action(s)

IT will:

1. Establish a streamlined deprovisioning process to promptly remove access rights for inactive or terminated employees, reducing the risk of unauthorized access.

Appendices

Rating Definitions

Audit Observation Rating Definition – Below is a summary of Observation Rating definitions.

High	A weakness that can significantly compromise internal control and/or its operational effectiveness. The agreed management action plan must be implemented with prioritisation and focus.
Medium	A weakness that can undermine the system of internal control and/or its operational effectiveness. The agreed management action plan is to be implemented.
Low	A weakness which does not seriously detract from the system of internal control and/or its operational effectiveness, but nevertheless should be addressed by management in accordance with the agreed action plan.

Audit Report Rating Definition – Control Based Opinion - Rated at the scope-level, considering the risk to the objectives of the relevant area or process under review.

Unsatisfactory	There are multiple high rated observations that in likely scenarios could in aggregate expose the business to critical levels of risk which may result in a material financial, reputation, operational, market or compliance impact.
Needs Significant Improvement	There are high or multiple medium rated observations that in likely scenarios could in aggregate expose the business to high levels of risk which may result in a significant financial, reputation, operational, market or compliance impact.
Needs Improvement	There are medium or multiple low rated observations that in likely scenarios could in aggregate expose the business to moderate levels of risk which may result in a moderate financial, reputation, operational, market or compliance impact.
Satisfactory	There are no observations or few low rated observations that in likely scenarios only expose the business to low levels of risk and are more in the nature of a procedural improvement than of a control weakness that would have a financial, reputation, operational, market or compliance impact.