

Payroll Fraud Monitoring

Payroll Fraud

One constant across all businesses is Payroll. As one of the primary expenditures in many organizations, payroll is often the subject of error, fraud and theft. Variables such as complex tax regulations, time tracking, attendance, incentive based pay and changes in contractual salary agreements, added to the high volume and frequency of transactions, make payroll an intricate task to process.

According to the Association of Certified Fraud Examiners (ACFE), companies lose 7% of their annual revenues to occupational fraud.

Occupational fraud and abuse schemes are numerous and varied. For example:

- Adding fictitious (ghost) employees to the payroll.
- Submitting dubious overtime claims.
- Claiming for unauthorized personal expenses.
- Making unauthorized changes to employee records, earnings, rates, etc.

Payroll Monitoring Solution

The focus of the SymSure Payroll Fraud Monitoring solution is to define and automate tests for the controls within the organization's payroll processes.

As outlined in Figure 1, the organization is allowed to define the control environment from employee records creation to final payments to employees. Once completed, SymSure's monitoring framework examines all master data and transaction records to detect control breaches and alert the relevant persons automatically.

SymSure Monitor is compatible with any source of data, including ERP and bespoke applications. By continuously monitoring the systems and applying a comprehensive resolution workflow, the audit and compliance process becomes independent and auditable.

This solution is deployed to all the relevant stakeholders; assigning them fraud mitigation tasks and ensuring that they are addressed in a timely manner. Financial and business process managers can focus on optimizing business performance and maximizing profits while mitigating the risk of fraud.

Preventative Controls

A key feature of payroll controls monitoring in SymSure is the ability to detect erroneous, suspicious and fraudulent activities before payments are made. This provides organization with valuable window of time to investigate exceptions to prevent losses due to error or fraud.

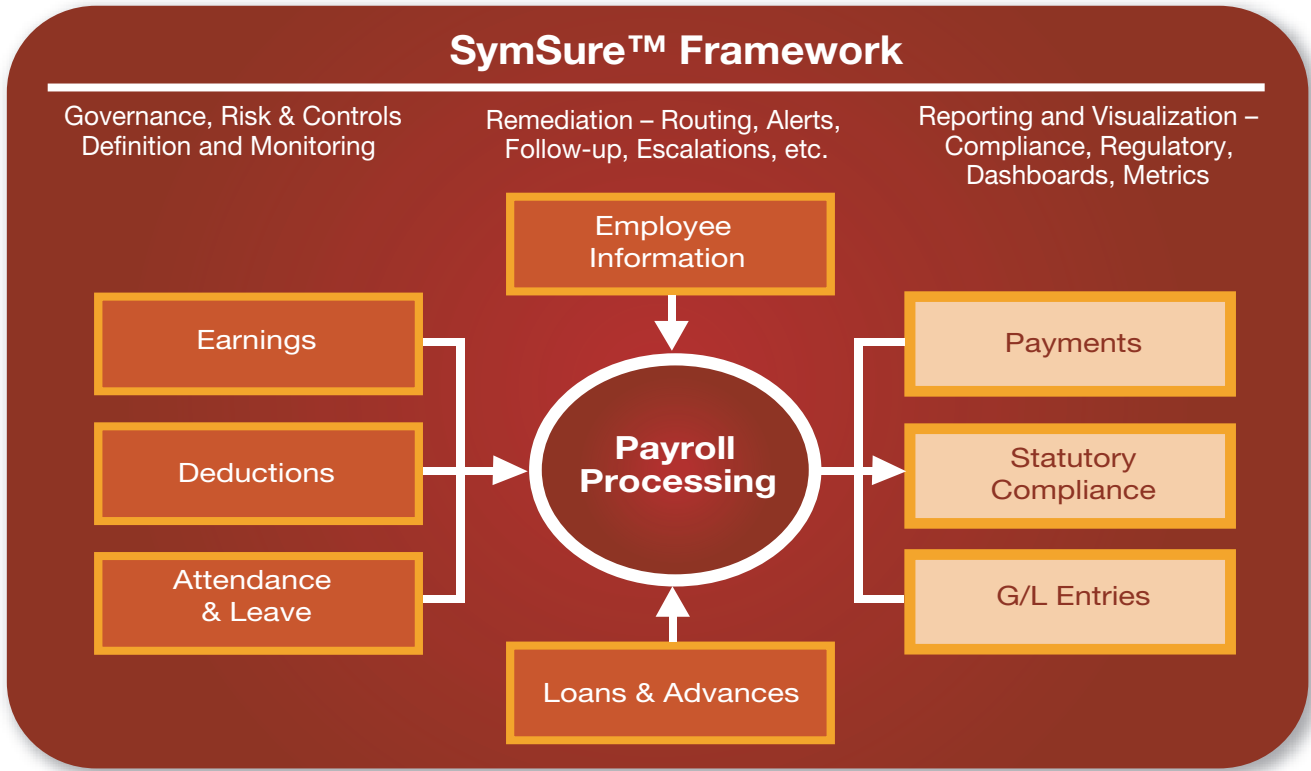


Figure 1 – SymSure Monitoring Business Process

SymSure Workflow and Reporting

When a breach occurs relevant alerts are triggered and a stringent remediation process is followed to ensure that high risk activities are addressed as stipulated by the business process owners.

Other key aspects of the solution are the automation of reporting and visualization of the control environment. SymSure automates key reporting for stakeholders, including statutory and regulatory bodies.

Reports include:

- Key payroll metrics
- Payroll expense trending
- Bank Account and G/L reconciliations
- Best practice comparisons

Standard dashboards are included in the framework:

- Trending of results across dates
- Grouping by risk ranking
- Grouping by status (new, pending, overdue, etc.)
- Comparisons across processes and users

Sample of Tests

Master Data Amendments	
Changes in bank account numbers	Test to return all employees with changes in their bank account number.
Employees added	Check for employees that have been added to the payroll over a period.
Employees removed	Check for employees removed or made inactive from the payroll over a period.
Payroll codes added	Reports all payroll codes that have been added to payroll over a period.
Changes in taxation methods	Reports any differences in the method used to calculate payroll taxes.
Reactivation of payroll codes	Highlights all payroll codes that were not being used for a period and are now reactivated.
Master Data Exceptions	
Duplicate bank account details	Reports all cases of duplicated bank account details.
Missing bank account details	Reports all cases where bank account details are missing.
Potentially duplicated payroll codes	Return all cases where there are payroll codes appear to be duplicated based on description of usage.
Duplicate payments	Reports all cases where there is a suspected duplicate payment to an employee.
Duplicate Tax ID	Reports all cases where tax data appears to be conflicting and/or duplicated.
Tax ID Errors	Reports all instances where the Tax ID does not conform to the code composition.
Segregation of Duties (SoD)	
SoD conflicts	Reports all cases where there are potential SoD conflicts.
Overtime Exceptions	
Overtime abuse	Return employees who have submitted overtime hours that are considered excessive.
Overtime rate exceptions	Return exceptions in the hourly rate used to calculate overtime payments.
Suspicious Activities	
Active employees not paid	Returns all employees that are active and are not receiving a basic salary.
Payments after contract ends	Returns all employees being paid after their employment contract has ended.
Ghost employees	Reports payments being made to employees that are not reconciling to other independent employee data sources.
Irregular payments	Reports Employees with irregular payments. For example an employee being paid January to June and then August to December.
Changes in Basic Pay	Returns detail report of changes to employee's basic salaries and rates.
Inconsistent earnings or deductions	Earnings and deductions that do not conform to business rules. For example bonuses being paid more than x times per year or deductions entered with a negative amount (effectively an earning).

Benefits

Business Challenge	SymSure Solution
<p>STAKEHOLDERS' REQUIREMENTS Escalating risk and compliance requirements</p>	<ul style="list-style-type: none"> • Provide enterprise wide definition and monitoring of controls and assurances that they are effectively implemented across all business processes
<p>AUTOMATION Automating control breach detection and remediation</p>	<ul style="list-style-type: none"> • Detects breaches at the data source • Distributes results across the enterprise by customer-defined rules via dashboards, e-mail, SMS • Provides workflow for remediation including automatic detection of resolution of errors • Allows the user to define controls in multiple business processes with a consolidated view • Increases efficiency by making analytics repeatable with the ability to adjust tolerances • Business rules and parameters are customizable and new logic can be built by the organization • Monitoring can also be applied to business metrics • Issues are identified as soon as they occur
<p>INTEGRATION Seamlessly integrate into existing solutions</p>	<ul style="list-style-type: none"> • No changes required to underlying systems being monitored • Non-intrusive access to data and cannot amend source data • User and group security with LDAP support • Strong encryption
<p>PROCESS OPTIMIZATION Makes the process more efficient and less costly</p>	<ul style="list-style-type: none"> • Issues detected more timely • Lower recovery costs • Greater level of automation • Compliance and other reporting automatically generated • Knowledge and expertise captured in the control systems and made repeatable

Copyright © 2009 SymSure Limited.
All rights reserved. No part of this manual may be transmitted, in any form or by any means (photocopying, electronic, mechanical, recording or otherwise) or reproduced, stored in a retrieval system, without permission in writing from the publisher.
All trademarks are the property of their respective companies.



CONTACT US:
+ 1 416 530 4567
email: info@symsure.com