Continuous Monitoring for Infor/Lawson Software
Continuous Monitoring
for Infor/Lawson Software

Agenda

About Us
Definition
Benefits to Your Organization
How It Works
Audit
Access Alerts
Security Tuning
Risk Analysis
Demo
Complimentary Solutions
Services
Founded in 1983, Kinsey has provided software sales, implementation, support and development for 34 years.

Lawson reseller and implementation partner since 1997.

Lawson certified systems integrator partner.

Lawson complementary software partner.

Lawson’s “Go to” implementation partner for public sector.

Provide complementary Lawson software products.
Continuous auditing is a tool for *internal auditors* mainly and to some extent *external auditors* to continually gather audit evidence to support auditing objectives and activities. This means collecting data on processes, transactions and accounts to establish compliance with regulation, procedures and policies.
Objective:
To collect information regarding user activity that can be used for auditing, security validation and procedural risk analysis.
How It Works

User Initiated Transaction

Kinsey filter sends a copy of transaction to WebSphere JMS Queue for processing

Lawson IOS WebSphere Application

JMS Queue holds the transactions to be processed

Core IBM WebSphere Application

Transactions are held in the queue

Kinsey WebSphere Application

Kinsey application waits for WebSphere to send message

Kinsey Server

Take the Kinsey server off-line

Lawson Processing

Kinsey

Continuous Monitoring for Infor/Lawson Software
Objective:
To collect information regarding user activity that can be used to determine the user responsible for the transaction, the date and time of activity, the action taken and the record processed.
Login Activity

Filter by:
- User
- Date Range
- Transaction Source

Drill to:
- Form Summary
- Record Detail

Audit
Current Login Activity

[Image of a screenshot showing an activity monitor with details such as server ID, IP address, login ID, names, dates, and counts of transactions.]
Audit
Last Login Recorded

Filter by:
- User
- Form
- Action
- Date/Time
- Record Accessed

Drill to:
- User Security

Drill to:
- User Security
Capture every Portal or MS Add-in transaction processed by a Lawson user and filter by:

- User
- Form
- Function Code
- Date
- Record Key
- IP Address

---

### Audit

**Historical Activity**

![User-Form Detail](image)

Server: LSF_PROD | Profile: APS

<table>
<thead>
<tr>
<th>Full Name</th>
<th>Form</th>
<th>Form Description</th>
<th>Function</th>
<th>Date/Time</th>
<th>Key 1</th>
<th>Key 2</th>
<th>Key 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawson, Lawson</td>
<td>AR10.1</td>
<td>Customer</td>
<td>N</td>
<td>3/23/2016 10:46 AM</td>
<td>1</td>
<td>111</td>
<td></td>
</tr>
<tr>
<td>Lawson, Lawson</td>
<td>AR10.1</td>
<td>Customer</td>
<td>N</td>
<td>3/23/2016 10:46 AM</td>
<td>1</td>
<td>112</td>
<td></td>
</tr>
<tr>
<td>Lawson, Lawson</td>
<td>HR11.1</td>
<td>Employee</td>
<td>N</td>
<td>3/23/2016 10:46 AM</td>
<td>1</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Lawson, Lawson</td>
<td>HR11.1</td>
<td>Employee</td>
<td>N</td>
<td>3/23/2016 10:46 AM</td>
<td>1</td>
<td>101</td>
<td></td>
</tr>
<tr>
<td>Lawson, Lawson</td>
<td>HR11.1</td>
<td>Employee</td>
<td>N</td>
<td>3/23/2016 10:46 AM</td>
<td>1</td>
<td>102</td>
<td></td>
</tr>
<tr>
<td>Lawson, Lawson</td>
<td>PO20.1</td>
<td>Purchase Order Entry</td>
<td>N</td>
<td>4/12/2016 8:45 AM</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lawson, Lawson</td>
<td>PO20.3</td>
<td>PO Line Options</td>
<td>I</td>
<td>4/12/2016 8:45 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lawson, Lawson</td>
<td>PO20.3</td>
<td>PO Line Options</td>
<td>C</td>
<td>4/12/2016 8:46 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lawson, Lawson</td>
<td>PO20.3</td>
<td>PO Line Options</td>
<td>I</td>
<td>4/12/2016 8:47 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lawson, Lawson</td>
<td>AP10.1</td>
<td>Vendor</td>
<td>N</td>
<td>5/4/2016 9:26 AM</td>
<td>1</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

Copyright (c) 2017

---

**Continuous Monitoring for Infor/Lawson Software**
Metrics

- By System Code
- By Date
Objective:
To identify when unauthorized access to a form has been breached.

Method:
• Define alternative form privileges for a user
• Validate against user security
• Validate against user activity
BUILDING A RULE

BY USER
- fnelson
- bthomas
- smiller

• Form=GL40.1  Rule= ALL ACCESS
• Form=GL45.1  Rule=ALL ACCESS
• Form=GL190  Rule=ALL ACCESS

Full access is allowed for just these 3 users.

Unauthorized Access Alerts
Security Access by User

Role GLjournal
Role GLadm
Role APclrk

GLprocess
GLreports
GLmaint
APprocess

GL40.1
GL45.1
GL190
Unauthorized Access Alerts
Security Access by Role

BUILDING A RULE

BY ROLE
• GLjournal
• GLadm

• Form=GL40.1  Rule= ALL ACCESS
• Form=GL45.1  Rule=ALL ACCESS
• Form=GL190  Rule=ALL ACCESS

Full access is only allowed for users assigned one of these 2 Roles.
Building a Rule

By Role

- GLjournal
- GLadm

- Form=GL40.1  Rule= ALL ACCESS
- Form=GL45.1  Rule=ALL ACCESS
- Form=GL190  Rule=ALL ACCESS

Full access is only allowed for users assigned one of these 2 Roles.
Objective:
Provide information that can be used to improve security by limiting access based on actual user activity.
By combining Kinsey’s User Security Report... with the User Activity Report...
...we can determine the forms a user has access rights to but may or may not be using.

Filter by:
- User
- Role
- Security Class
- Form
- Date Range
Segregation of Duties (SOD) reporting validates that you have the proper checks and balances in place to prevent fraudulent activity.

**Objective:**
To determine which users and policies present the highest degree of risk.
By comparing your security settings...

to our SOD policies....

SOD Risk Analysis
Violation Report

Continuous Monitoring for Infor/Lawson Software
...we can create an SOD violation report by User.

Example: Payables (153); Investigate Discrepancies or Expenditure issues conflicts with Initiate Checks for Expenditure.
The Risk Analysis Grid combines the SOD Violation report with actual user activity to highlight the policies with the highest degree of risk.

Example: Payables (153); Investigate Discrepancies or Expenditure issues conflicts with Initiate Checks for Expenditure.
By drilling on a specific violation you can view the User’s security settings and a policy access grid.

Drill to Security Reporting

SOD Risk Analysis
Policy Access Grid
Product Demo
Complimentary Solutions

Activity Monitor
- Audit
- Security Tuning
- Unauthorized Access

Security Reporting
- User
- Role
- Security Class
- Usage Comparison

SOD Reporting
- 200+ Prebuilt Policies
- Violation Reports
- Email Notifications

Security Auditing
- Audit all object changes
- Email Notifications

Transaction Auditing
- Selectively audit over 6500 Lawson Forms

SOD Remediation
- Risk Analysis Grid
- Security Modeling

Security Modeling
- Build What-if scenarios for Users, Roles, Forms

Landmark Reporting
- Actor
- Role
- Security Class
- Lawson LPL Detail
Services

Installation
Remote installation services take between 1 and 3 days depending on the product selected. After testing most customers are fully operational within 2 weeks.

Training
Training is also done remotely using Kinsey certified Lawson consultants. Training takes anywhere from 1 to 3 days depending on the applications selected.

Security Consulting
Our team of security consultants have assisted over 60 Lawson clients build and maintain Lawson Security.
Contact Us

✉️ g.henson@kinsey.com
📞 call 757-621-8236
🌐 www.kinsey.com

Thank you for attending!
We hope you found it helpful!