

A key step involves understanding the process by which the business rules are identified, worked, tested and ultimately approved into production.

### Reserving

Insurers are required to record liabilities for unpaid claims. The insurer's accurate financial reporting and even solvency depend heavily on the adequacy of these recorded claims reserves. Actuarial specialists assess the adequacy of the claims reserve process. The actuaries study historical patterns of claims settlement and use this information to project the ultimate cost of incurred claims.

Claims reserves are recorded for unpaid claims, including claims that have been reported and claims that have yet to be reported. Unreported claims are referred to as incurred, but not reported (IBNR). Individual claims may be recorded based on the expected payment amount for each individual claim or on actuarially determined amounts for similar claims. Actuarial projections are also made for the IBNR claims based on actuarially determined patterns.

Public accounting firms devote extensive resources to test the adequacy of claims reserves. They test the underlying data, and will engage the assistance of a specialist or actuary. Internal auditors may consider testing the accuracy of the underlying data used for the actuarial projections and the controls relating to this data. The public accountants may consider using the work performed by internal audit in order to reduce their own testing.

### System testing

Testing the accuracy of claims is challenging because of the large volume of claims. However, routine samples may not provide adequate coverage of the population. You may need to consider advanced testing techniques to examine the controls built into the automated claims processing system. This can also help to reduce the substantive testing that is required.

When gaining your understanding of the system and identifying the control activities, ascertain which controls are performed manually and which are automated by the software application. Automated controls are also known as application controls.

The benefit of testing application controls is that you only need to test a sample of one. For example, if you are testing to ensure that only approved claims are paid, you can test substantively by selecting a sample of paid claims and

looking for the authorization for each sample. By testing the application control, you test to ensure that the system does not allow a claim to be paid unless it is approved.

There are two approaches for testing this application control; either one is considered sufficient by itself.

The first method is testing the configuration. Often there is a configuration screen or menu that will allow system administrators to select to enforce the control. A screen print of this configuration will suffice as evidence.

The second approach is used when the configuration screen is not readily accessible, or when the enforcement of the control is hard coded into the system. In such situations, you should ask a user to attempt to pay a claim that has not been approved. If properly configured, the system should display an error message saying a claim cannot be paid without approval (or similar meaning). A screen print of the error message is considered sufficient evidence for this test.

If a screen print is not feasible, observation of the error message and a memo to that effect is adequate.

Remember that placing reliance upon any application control is only possible if there are also strong IT general controls in place. IT general controls include things such as system development, change control, physical security, logical security, backup and recovery and operations.

For example, if there are weak change controls, you cannot place reliance upon the application control because it could be changed tomorrow, or could be different than it was yesterday. If there are weak logical access controls, an unauthorized individual may be able to override an application control.

### Conclusion

Claims processing presents a variety of risks and a complex array of processes. An excellent understanding of these areas is an important first step for internal auditors to develop. Insurers are heavily dependent on the utilization of automated systems and internal auditors must develop meaningful approaches to evaluate the embedded controls in these systems. **NP**



process, it may be necessary to review original documents received and confirm whether a supervisory, peer or independent quality review of the information entered into the system ensured its completeness and accuracy.

Auditors should assess whether the claim was reviewed timely and updated periodically according to the insurer’s claim processing procedures. The company’s claims manual should detail these procedures. When the company’s process is automated, which is becoming more the norm,

you will need to coordinate with information technology (IT) professionals to understand the data feeds into the claims process.

Providers or clearinghouses submitting claims information via the EDI process should follow the American National Standards Institute 837 format. A key audit step is the reconciliation of the claims count total, per the 837 files, to the claims count uploaded to the claims system. Also, you should do a similar reconciliation of the total dollar value.

**Key risks to consider**

The claims function represents one of the most significant of insurance company processes, financially and operationally. Key risks to be considered include:

Key Risk	Reasons
Invalid or fraudulent claims are processed and approved for payment	<ul style="list-style-type: none"> <li>• Inadequate coverage</li> <li>• Overriding of stale or declined claims</li> <li>• Fictitious claims</li> <li>• Duplicate claims</li> <li>• Claims processed on incorrect accounts</li> <li>• Collusion between insureds or providers and claim examiners</li> </ul>
Claims are not processed timely	<ul style="list-style-type: none"> <li>• Manual or automated backlogs</li> <li>• Incorrect routing of information</li> <li>• Lost claims or information</li> <li>• Pending claim information</li> </ul>
Claims data is corrupt or invalid	<ul style="list-style-type: none"> <li>• System data incorrect or outdated</li> <li>• Data corrupted</li> <li>• Data not adequately backed up</li> </ul>
Claims are processed incorrectly	<ul style="list-style-type: none"> <li>• Claims adjudication procedures not being followed</li> <li>• Overriding of manual or system generated rules</li> <li>• Incorrect coding of claims detail</li> <li>• Overpayment of claims</li> </ul>

**Coverage verification**

Health insurers may offer insurance plans with a variety of coverage benefits. Upon receiving a claim, the claims processor must verify that the individual had insurance coverage as of the date of the claim and that the incident or procedure is a covered benefit under the policy.

If the insurer has an outdated claims processing system and offers a variety of health plans and coverage benefits the verification may be a manual process.

However, as insurers continue to become almost entirely automated, this verification can be done by the claims system software. Rules can be written into the claims software to integrate enrollment and policy information from the policy administration system. The claims system is then able to align the coverage dates and claims to automatically verify coverage. Similarly, provider information should be aligned with member and claim information to confirm coverage for submitted claims.

As with EDI claims submission, you will need to work with IT to audit coverage verification checks. The business rules are either activated within an off-the-shelf claims system or are configured internally by individuals within the insurance company. It is important to understand how the software logic is requisitioned, tested and ultimately approved in order to audit the business rules. In instances where the process is manual, you should test whether the claims processor has documented the verification of coverage.

Another important consideration is that an insured may have coverage from more than one insurance plan. Claims processors need to determine whether other coverage exists and then ensure the claim is paid under the appropriate insurance plan. The claims processor should document within the claims file whether coverage was available from another insurance plan. In automated systems, coverage under other plans is included the system rules.

## Claims adjudication

Insurers processing a certain critical mass must try to automate the adjudication of claims as much as possible. Similar to doctors ruling out certain diagnoses, insurers rule out certain claims that can be paid automatically once coverage is verified. Business rules within the claims software auto-deny or “pend” claims. Claims that successfully flow through the business rule filters are designated for payment.

Some of the more common denials are auto-denials denoting no coverage at the time of the claim, benefits not covered by the plan, duplicate claims, or pending claims based on the claim exceeding a certain dollar threshold that require adjuster or supervisor review.

When the claimant is determined to be a covered individual and the billed service or procedure is a covered service, the proper amount to be paid to the provider or the insured must be determined.

The EDI process should follow the American National Standards Institute 837 format.

The insurer typically has contracts with providers that specify the amount to be paid for covered services, thereby making determining the payment a straightforward process. This is another instance where configuration of the claims software helps automate the process. However, depending on the various business rules that are in place to pend certain claims, it may also require some manual intervention.

For automated adjudication rules, a key step involves understanding the process by which the business rules are identified, worked, tested and ultimately approved into production. In a manual environment, you should obtain the executed contracts with providers to confirm the existence

of a contract. Also, you should consider reviewing the documentation that supports the claim payment prepared by the claims adjuster, including evidence of a supervisory review.

Business rules within the claims software auto-deny or “pend” claims.

It is also important to test the authority limits of the individuals approving claims for payment and signing or authorizing checks or direct deposits. You will also want to understand how authority limits are reviewed and approved by management on a regular basis.

## Quality assurance

Health insurers depend heavily on automated systems and the proficiency of the claims adjusters. Supervisors may be required to approve the more expensive claims or claims for unusual conditions. However, the largest volume of claims may be handled by only one processor. A best practice concerning the claims process may include instituting a quality review control to ensure high-volume/low-severity claims are handled correctly.

You will need to understand the quality assurance process and include a review of it as part of audit testing. Consider whether sample claims are selected in an appropriate manner, the individual in charge of quality assurance is following the established guidelines, mistakes identified are promptly corrected, and remedial action is taken to improve the work quality of claims adjusters. Key metrics to consider include payment accuracy and procedural accuracy.

## Timeliness of claims processing

Timeliness of claims processing is a frequent source of complaints by insured and providers. Claims managers should track the timeliness of processing to ensure claims are paid in accordance with contract terms. An automated system should provide an aging of claims. Your review should include an assessment of claims processing times.

Claims that become too outdated can result in interest charges to the insurer. When a third party handles claims adjudication and payment, the vendor management agreement should clearly define any recourse against the third party provider for interest or penalties incurred for untimely payment of claims.

A key step involves understanding the process by which the business rules are identified, worked, tested and ultimately approved into production.

### Reserving

Insurers are required to record liabilities for unpaid claims. The insurer's accurate financial reporting and even solvency depend heavily on the adequacy of these recorded claims reserves. Actuarial specialists assess the adequacy of the claims reserve process. The actuaries study historical patterns of claims settlement and use this information to project the ultimate cost of incurred claims.

Claims reserves are recorded for unpaid claims, including claims that have been reported and claims that have yet to be reported. Unreported claims are referred to as incurred, but not reported (IBNR). Individual claims may be recorded based on the expected payment amount for each individual claim or on actuarially determined amounts for similar claims. Actuarial projections are also made for the IBNR claims based on actuarially determined patterns.

Public accounting firms devote extensive resources to test the adequacy of claims reserves. They test the underlying data, and will engage the assistance of a specialist or actuary. Internal auditors may consider testing the accuracy of the underlying data used for the actuarial projections and the controls relating to this data. The public accountants may consider using the work performed by internal audit in order to reduce their own testing.

### System testing

Testing the accuracy of claims is challenging because of the large volume of claims. However, routine samples may not provide adequate coverage of the population. You may need to consider advanced testing techniques to examine the controls built into the automated claims processing system. This can also help to reduce the substantive testing that is required.

When gaining your understanding of the system and identifying the control activities, ascertain which controls are performed manually and which are automated by the software application. Automated controls are also known as application controls.

The benefit of testing application controls is that you only need to test a sample of one. For example, if you are testing to ensure that only approved claims are paid, you can test substantively by selecting a sample of paid claims and

looking for the authorization for each sample. By testing the application control, you test to ensure that the system does not allow a claim to be paid unless it is approved.

There are two approaches for testing this application control; either one is considered sufficient by itself.

The first method is testing the configuration. Often there is a configuration screen or menu that will allow system administrators to select to enforce the control. A screen print of this configuration will suffice as evidence.

The second approach is used when the configuration screen is not readily accessible, or when the enforcement of the control is hard coded into the system. In such situations, you should ask a user to attempt to pay a claim that has not been approved. If properly configured, the system should display an error message saying a claim cannot be paid without approval (or similar meaning). A screen print of the error message is considered sufficient evidence for this test.

If a screen print is not feasible, observation of the error message and a memo to that effect is adequate.

Remember that placing reliance upon any application control is only possible if there are also strong IT general controls in place. IT general controls include things such as system development, change control, physical security, logical security, backup and recovery and operations.

For example, if there are weak change controls, you cannot place reliance upon the application control because it could be changed tomorrow, or could be different than it was yesterday. If there are weak logical access controls, an unauthorized individual may be able to override an application control.

### Conclusion

Claims processing presents a variety of risks and a complex array of processes. An excellent understanding of these areas is an important first step for internal auditors to develop. Insurers are heavily dependent on the utilization of automated systems and internal auditors must develop meaningful approaches to evaluate the embedded controls in these systems. **NP**