NOMENTIA

EBOOK

Are your cash outflows safe from fraud?

CONTENTS

www.nomentia.com

ADJUSTING TO AN EVER-EVOLVING THREAT LANDSCAPE

Cyber-attacks, data fraud and theft have made it to the top-5 of the global risk landscape. Cyber-attacks alone are identified as the biggest threat to doing business in Europe, North America, East Asia, and Pacific[1]. Several international studies show that today's treasurers need to fight against this faceless enemy causing major operational risks and losses tjat can be counted in millions.

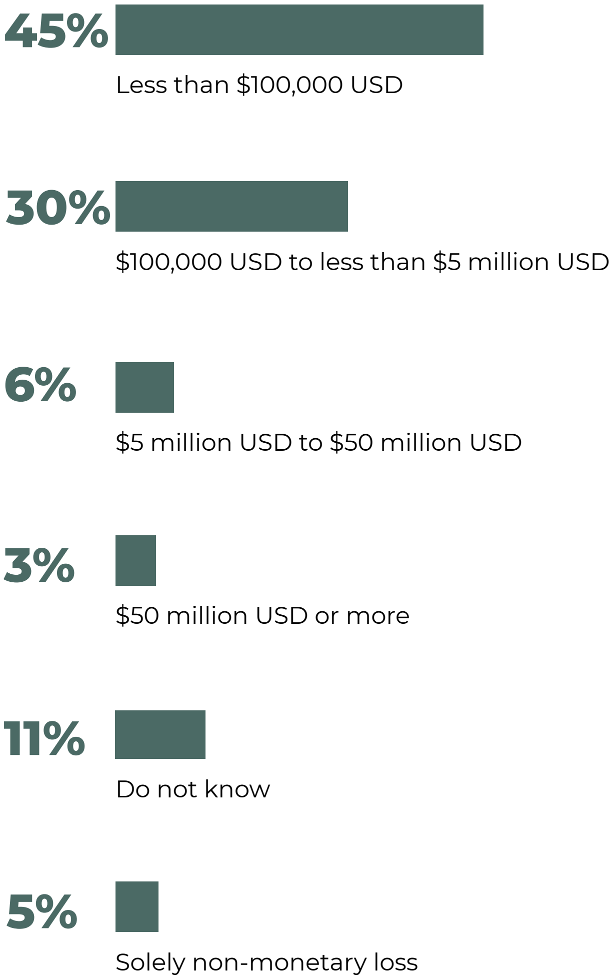
The share of the merchant revenue lost to fraud continues to grow year by year, and more than one third of companies report being victimized by economic crime[2].

42%

of companies said they have increased funds used to combat fraud and/or economic crime[3].

The amount of direct monetary losses to fraud

Direct monetary losses due to fraud can be substantial



[1] The World Economy Forum Global Risks Report 2018

[2] Lexis Nexis True cost of Fraud study 2016

[3] PwC Global Economic Crime and Fraud Survey 2018

The first threat that comes to mind are cyber criminals, increasingly targeting personal finance, corporates, financial institutions, as well as governmental payment infrastructures. Organizations' purchase-to-pay chain and payment process are attractive targets, as these are the processes where cash actually flows out of the company.

The fraudsters gather their prey from organizations of all sizes. They have time to prepare for the attacks and they also have access to sophisticated low-cost tools shared in the dark nooks of the Internet. The term *whaling* describes how cybercriminals first identify and then stalk their potential targets, to learn weaknesses of their future victims, and to develop a plot that is often so detailed that the victim gives access to cash before realizing what has happened.

Business email* compromise-losses exceeded

$12.5 bn

in 2018

**Source: FBI, Internet Crime Complaint Center (IC3)*

But the corporate payment security extends well beyond preventing cyber-attacks and external fraud. Despite all noise about external risks, fraud and theft are more likely to be committed by an internal actor than an external one[1]. Mitigating these internal risks require that you take a completely different perspective regarding payment security. Security of cash outflows also means eliminating mistakes in the processes themselves.

At the moment and most often, organizations fall short in taking a holistic view of the payment process. For instance, corporations are very interested in the approval chains that the payment processing software supports to prevent fake invoices but are neglectful in protecting their vendor master data from false supplier information. Security is taken into consideration in different steps of the process, when the focus should be in tracking the flow from purchase to payment, end-to-end.

With this e-book, we will take a comprehensive look at corporate payment security and provide you with all the different perspectives you should examine your process from. The aim is to give you a checklist of sorts, with concrete advice, based on which your treasury, finance department, as well as IT and business units can act on to improve security.

[1] PwC Global Economic Crime and Fraud Survey 2018

MITIGATING THE RISK OF BOTH EXTERNAL AND INTERNAL FRAUD

Are you on top of the situation?

Fraud related to corporations' extended purchase-to-pay (P2P) processes is very common. In fact, it is so common that you should be able to count the fraud attempts against your organization's cash outflows from the last six months. Otherwise you are most likely not managing the risks correctly. And if the fraud attempts go unnoticed – how sure are you that fraud has not already happened?

78%

of companies say they were victims of Payment Fraud in 2018*

**Source: AFP 2018 Payment Fraud Survey*

The frequent news of both fraud attempts and fraudsters that have succeeded in scamming tens of thousands or even millions have already prompted organizations into taking a closer look at their payment processes and how secure and up-to-date their practices are. But usually, organizations are only urged to take action in one specific part of the payment process. The specific part might be, for example, tightening payment approval practices or updating password policies. This approach might leave an unsafe gap elsewhere in the process.

In addition, even if companies take measures to protect themselves against the external threats, they tend to turn a blind eye to the risks coming inside their own walls. In the end, most of the economic crime comes from internal as opposed to external parties, with senior and middle management representing the largest source of internal fraud.

For a holistic approach, organizations should be aware of and mitigate the risk of both external and internal payment fraud. The following categorization presents some of the most common risk areas.

INTERNAL RISKS

- **Fake vendors**: Vendor master data has been compromised and a non-existent supplier has been registered. Another typical scam is to lure in an account number change for an existing supplier.
- **Dangerous duty combinations**: A person has the rights to initiate payment orders and approve them for payment, for instance.
- **Supplier kickbacks**: An internal and external fraudster team-up to create invoices on goods that were never delivered. A company employee checks the goods' receipt note in exchange of a kickback that the supplier pays after being able to send a false invoice to the company.
- **Travel expenses falsification**: An employee falsifies expense claims due to manual or inefficient processes.
- **Manipulating data at rest**: Payment processes usually include steps of moving unsecured payment data (ie. only by folder permission). Key personnel in IT and finance usually know all such weaknesses and could manipulate the process without leaving an audit trail.
- **Payment anomalies**: In addition to fraud and theft, anomalies and mistakes can cause leaks in cash outflows.

EXTERNAL RISKS

- **Fictitious invoicing**: The fake invoices issued by fraudsters to organizations are getting harder to recognize and may slip through without proper control.
- **Social engineering**: The phishing attempts to gather system access or confidential information are getting more and more clever.
- **CFO attacks**: Fraudster pretends to be a company executive and manages to convince finance
- employees to initiate urgent payments via email requests.
- **Malware, ransomware, and other viruses**: Cybercriminals lure executives or finance administrators to install malicious software via e-mail or websites to take control of their computers.

Modeling the risk of fraud and cybercrime in the extended purchase-to-pay scope

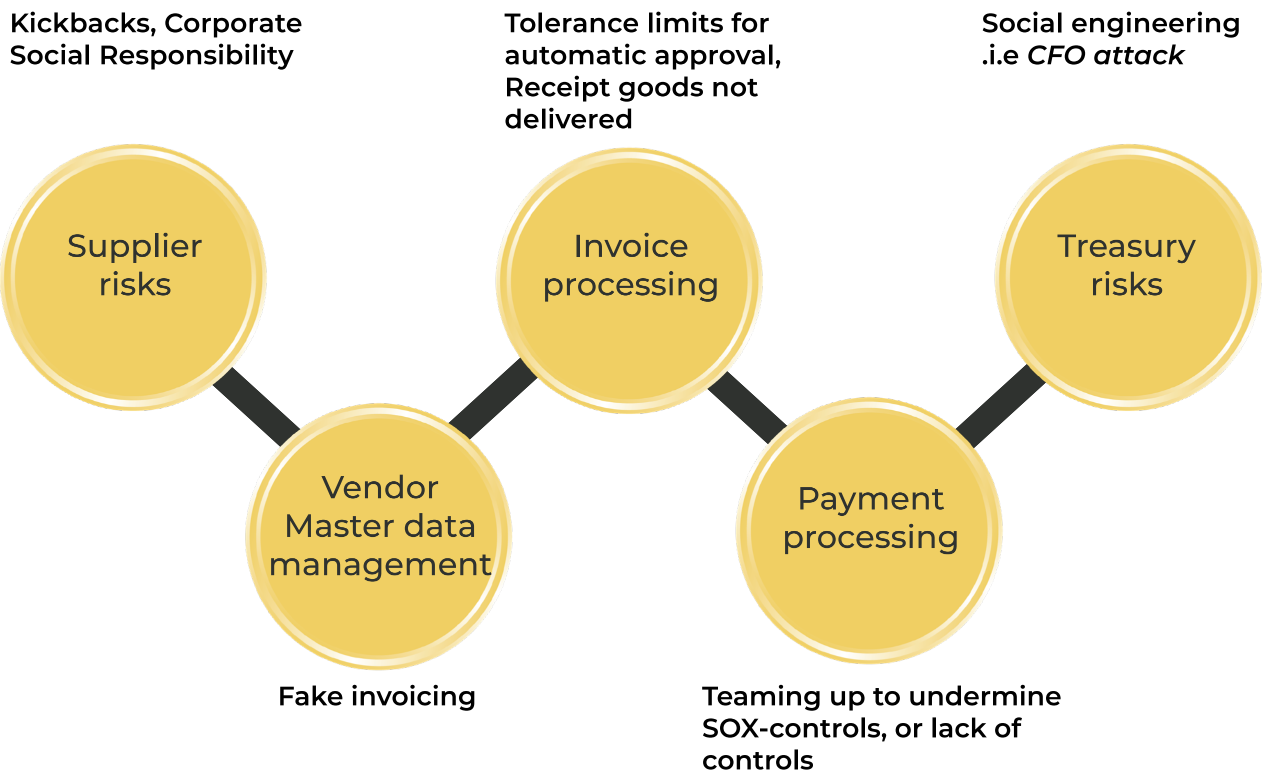

Kickbacks, Corporate Social Responsibility
Tolerance limits for automatic approval, Receipt goods not delivered
Social engineering .i.e *CFO attack*
Supplier risks
Invoice processing
Treasury risks
Vendor Master data management
Payment processing
Fake invoicing
Teaming up to undermine SOX-controls, or lack of controls

Figure 1. An organization's purchase-to-pay process is one of the most attractive business processes for fraudsters to target. A safe, proactive approach eliminates weaknesses in all of the steps of the extended P2P chain.

In a risk landscape that is this multifaceted, it is not enough to ensure safe payment processing. To really be on top of the situation, organizations need to eliminate weaknesses in all the phases of the end-to-end P2P chain related to the payments (Figure 1).

In the following chapters, we will go through the different aspects that build up payment security against the above-mentioned and several other risks. We will have a look at the processes, the technology, and the people and their actions involved in the process. By looking at the issue from all angles, we will provide you with a thorough list of things to consider when examining the state of your organization's payment process.

BUILDING SOLID PROCESS TO WITHSTAND FRAUD ATTEMPTS

Take the proactive approach

Payment fraud has become a true threat to organizations of all sizes. Corporate cash managers and treasurers are forced to increasingly combat fraud while also mitigating the other risks in the volatile economic and political environment. Against the backdrop of the current risk environment, it is surprising that only a minority of organizations conduct risk assessment on a regular basis, at least once a year. Astonishingly many organizations admit that they never analyze the safety of their processes.

Most often the risk analysis is performed on an ad-hoc basis, which usually means that something has already happened to trigger the need to take a closer look at the processes' safety. To get ahead of the game and prevent fraud before it happens, you need to proactively plan and build processes that protect your organization’s payment flows.

RISK

10% of companies have not performed any risk assessments in the past 2 years.*

**Source: PWC Global Economic Crime and Fraud Survey 2018*

Eight steps to improve your payment process

1. Assign an owner to the process

It’s typical that the payment process is a shared responsibility of the finance department. There should be a clear process owner with a strong mandate from the senior management in charge of both the performance and the safety of the process. With clear responsibilities, also the security perspectives tend to get more actively promoted. It also helps to put emphasis on the planning of the reactive measures if something goes wrong in the payment process.

2. Document the process

Documenting the current process carefully is time well spent as it reveals the inefficiencies, safety issues, and irrelevant steps you may have in your payment process. Most of all, it enables you to standardize the process according to best industry practices. Create one uniform process for your organization’s payments with approval chains and clear policies related to processing the incoming invoices, as well as roles and rights. After that it is time to run the harmonization exercise over all your current banks, ERP systems, and processes.

3. Harmonize and gain visibility

Malicious trails are more difficult to find in a cumbersome and scattered ERP and bank landscape. Harmonized practices increase transparency and visibility. Uniform processes help to track cash outflows organization-wide, and thus mitigate risks for both external and internal fraud. No matter how many bank accounts your organization has, you should have central visibility to all of them, from one place. For instance, treasury accounts are often out of sight and not amidst the same controls as the other bank accounts of the company.

4. Increase automation

Complex manual processes including a lot of subjective user actions and decisions are the ones most at risk. Automated processes not only increase the efficiency but also build up the security. Eliminating phases where the users manually handle payment data takes away many opportunities for misuse. For instance, manually uploading the payment file batches from folder to the bank leaves the data open for tampering. End-to-end automated file transfers between systems increase security considerably.

Take advantage of new technology and use Robotic Process Automation (RPA) to overcome risky manual steps in your current payment and cash management processes in case your legacy systems do not support integration. Instead of having someone copying bank account statements manually every morning to the system or making changes in vendor master data, a software robot can do it in a fraction of time, safely – and without the unintentional mistakes, too.

5. Handle deviations with care

Eliminating manual ad-hoc payments and enforcing policies where only the payments with a purchase order or payments to a registered vendor are accepted, are a great way to increase safety. In practice it is next to impossible for organizations to get rid of manual payments altogether. Create a solid process for handling the exceptions in your payment process as well and use ready-made templates to create spontaneous payments. And when payments can only be approved in the payments system and not via email or phone, it keeps you protected against the CEO amd CFO attacks.

6. Avoid back doors

Be sure not to create – intentionally or unintentionally – routes that make it possible to bypass the well-designed process steps. Let's take an example. A company has enforced a policy that requires double approval for a payment and a third person to send it to the bank. But at the same time several employees have loose, direct access to the internet banking portal and are thus able to go around the approval process. Is it a risk worth taking?

7. Keep incoming cash extra safe

Implement best practices to your cash forecasting to ensure you do not have excess cash in all of your bank accounts all around the world. When a majority of cash is concentrated to treasury's accounts, and the operative accounts are topped up on needed basis only, you significantly mitigate the damages from fraud.

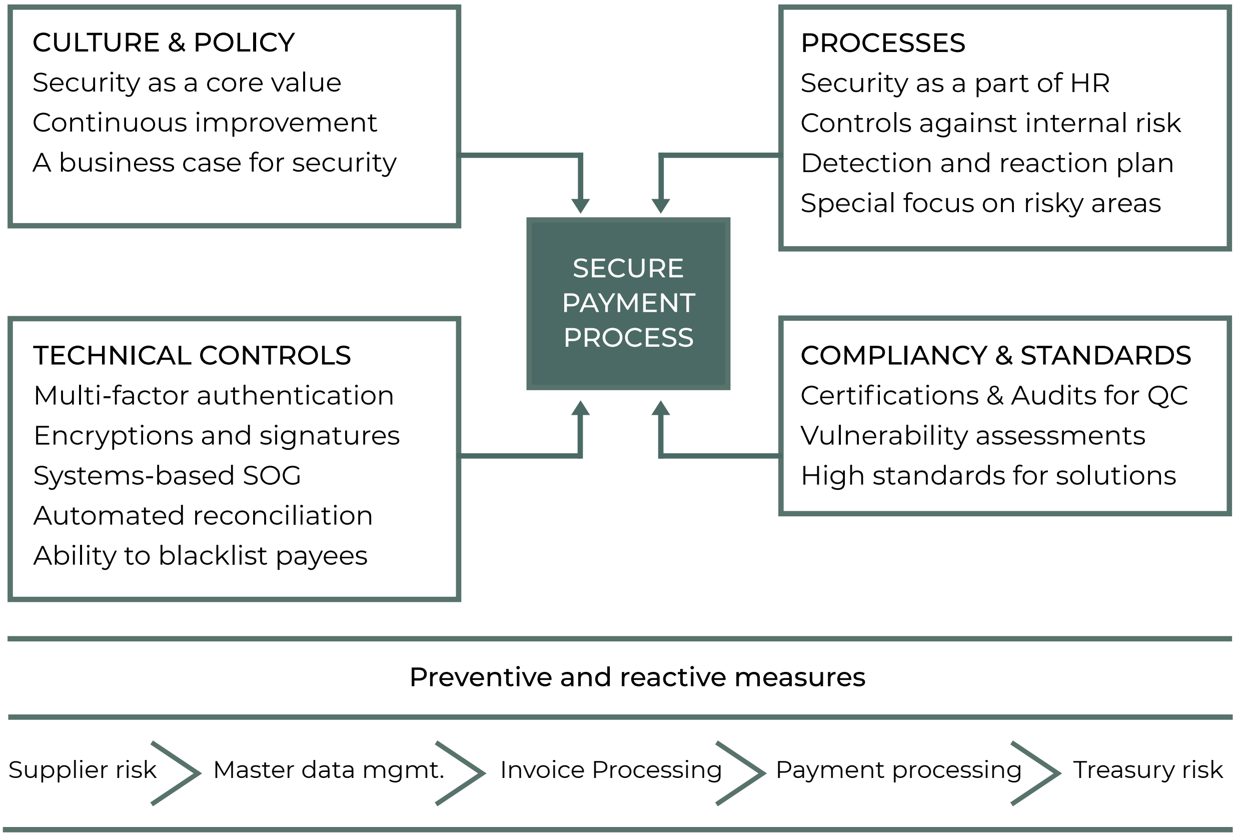
8. Audit the process

In a way, this is one of the most important aspects. It goes back to the first point of this list: the process owner responsible for the performance and safety of the process should take care of regular audits of the process as well. The threat landscape is ever-evolving – and so should your payment process be.

To sum up, the three underlying guidelines to follow are to switch from manual to automated, from responsive to proactive, and from shared to owned. Firstly, automating manual processes in invoice handling and payment processing is one of the best means to instantly increase security as it also prevents human errors and adds to the transparency, quality, and speed of payments. Secondly, carefully planned processes safeguard your organization's payment flows a long way, and when monitoring the cash outflows is a part of your proactive approach, money is not lost without anyone noticing. Lastly, to be able to develop the process comprehensively and view the security aspects from the necessary holistic point of view, the process needs a clear owner, responsible for both the functionality and the safety of the process.

Next, we will drill down into the actions you should take in order to fortify your process.

SECURING THE PAYMENT PROCESS



CULTURE & POLICY
Security as a core value
Continuous improvement
A business case for security

PROCESSES
Security as a part of HR
Controls against internal risk
Detection and reaction plan
Special focus on risky areas

SECURE PAYMENT PROCESS

TECHNICAL CONTROLS
Multi-factor authentication
Encryptions and signatures
Systems-based SOG
Automated reconciliation
Ability to blacklist payees

COMPLIANCY & STANDARDS
Certifications & Audits for QC
Vulnerability assessments
High standards for solutions

Preventive and reactive measures

Supplier risk > Master data mgmt. > Invoice Processing > Payment processing > Treasury risk

MANAGING THE USER ROLES, PRIVILEGES, AND ACCESS TO SYSTEMS

Take the reins

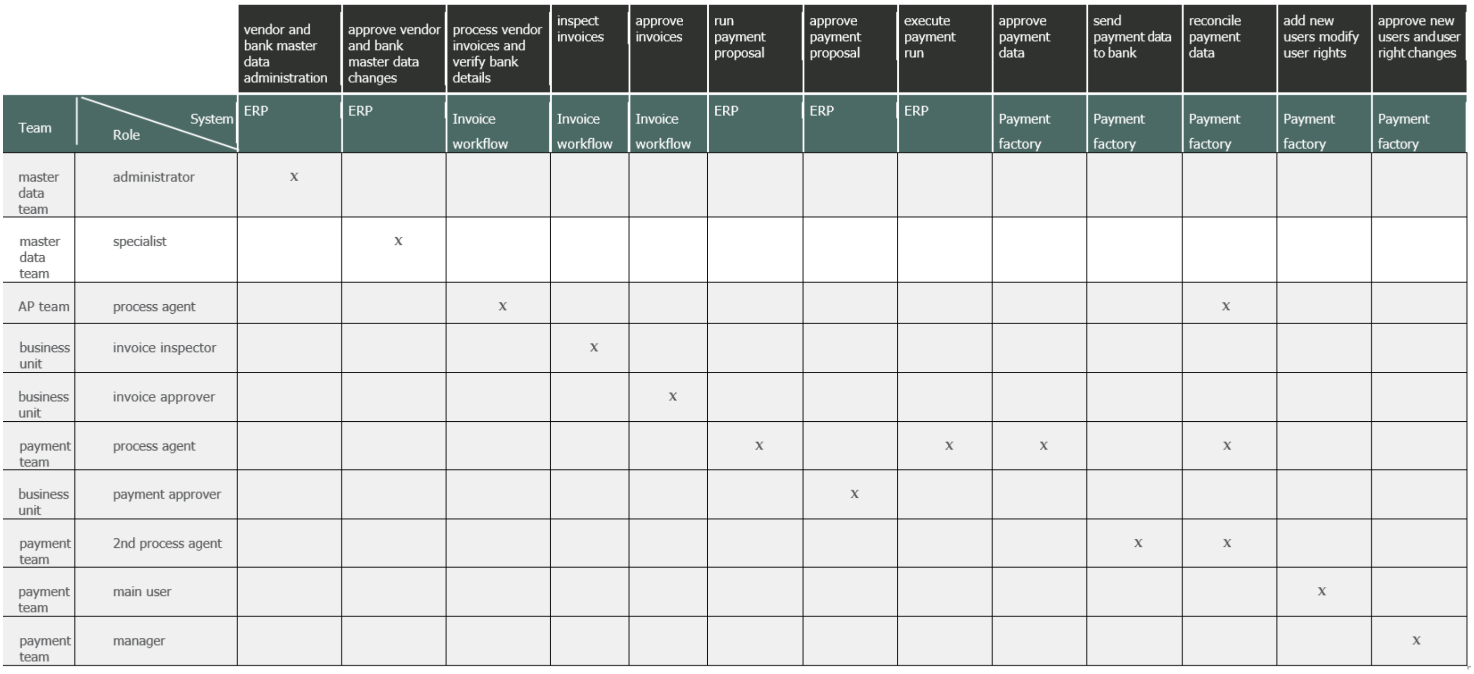
Corporate payment security should not be a one-time exercise but a way of operating each and every day. Thorough review and harmonization of your end-to-end payment process described in the previous chapter will bring you up to speed in fraud and risk mitigation, but in the long run it is not enough to keep you safe. You need to also consider the people who are involved in the different stages of your payment process.

Only 52%

of fraud is committed by internal actors*

**Source: PWC Global Economic Crime and Fraud Survey 2018*

Use an access control matrix to gain a clear overview on the user rights in your processes (Figure 2). It is an easy way to single out the points where a risk might have formed unnoticed over time and eliminate dangerous task combinations.



		vendor and bank master data administration	approve vendor and bank master data changes	process vendor invoices and verify bank details	inspect invoices	approve invoices	run payment proposal	approve payment proposal	execute payment run	approve payment data	send payment data to bank	reconcile payment data	add new users modify user rights	approve new users anduser right changes
Team	System Role	ERP	ERP	Invoice workflow	Invoice workflow	Invoice workflow	ERP	ERP	ERP	Payment factory	Payment factory	Payment factory	Payment factory	Payment factory
master data team	administrator	x												
master data team	specialist		x											
AP team	process agent			x								x		
business unit	invoice inspector				x									
business unit	invoice approver					x								
payment team	process agent						x		x	x		x		
business unit	payment approver							x						
payment team	2nd process agent										x	x		
payment team	main user												x	
payment team	manager													x

Figure 2. Access control matrix. Company-specific differences aside, a solid user control matrix should include at minimum these roles and duties.

Regardless of increasing automation in invoice handling and payment processing, there will be phases in your purchase-to-pay process that require user actions. If you are not establishing strong control and user rights management, you might end up leaving a detour open round your rock-solid process. Opportunity makes the thief: the main driver of internal economic crime is usually the opportunity. Take the reins and implement best practices to prevent malpractice and also costly mistakes.

Six Principles For Secure User Rights' Management

1. The principle of least privilege

Be careful not to assign overly broad user rights to people merely out of comfort. Users should never have more rights in any system than what they need to perform the tasks belonging to their job description and role. Continuous updating and auditing privileges is an important part of building security.

2. The four-eye principle

For example, a purchase invoice should without exception be verified for payment by two people.

3. Clear separation of duties

Avoid risky combinations and make sure a single person cannot, for instance, sign the goods received note and approve the related payment or create a new invoice and approve it for payment.

4. Strict policy for inspecting changes

Sort out the riskiest actions, for instance adding new user rights or making changes in the vendor master data and require a pre-assigned inspector's approval for the changes in these categories before they come into effect. This is a practical tactic to spot not only fraud attempts but also unintended mistakes.

5. Secure authentication

The identity of a person allowed to access the critical functions of the payment system should be verified in more than one way. Multi-factor authentication (MFA) is based on the combination of multiple things: what you know (a user name and a password), what you have (an USB token or a mobile phone) and what you are (a bio identifier, such as a fingerprint). With the increasing phishing attempts to get user credentials, relying on a single form of authentication can weaken security dramatically.

6. Centralized identity management

Instead of having multiple system-specific usernames and passwords, you can enable single sign-on (SSO) for the users to access multiple applications by using the same identity. Centralized management makes it easy to keep track of all the systems a person has access to, and to monitor user activities throughout the employment lifecycle. Surprisingly often organizations are careless in terminating user rights when a person's employment ends. With comprehensive SSO it is easy to remove all access rights at once.

A modern system solution that supports these safe practices in user rights management gives a secure backbone to your organization's payment processing.

In the following chapter, we are going to look technology from a different perspective: the things you should consider when making sure that your payment process is run in a safe technology environment.

24%

of reported internal frauds were committed by senior management*

**Source: PWC Global Economic Crime and Fraud Survey 2018*

ENSURING THE SAFETY OF TECHNOLOGY

Assume a 360-degree approach to security

Humans are often recognized as the weakest link of security, which makes the topics of automation, strong user rights management, and secure user authentication discussed in the previous chapter very relevant in payment security. But the security concern that comes up most often when talking with organizations is actually data transfer and issues related to it.

The technology platform related to the payment process is the area where both the finance and treasury functions as well as the IT department need to come together to build a secure environment. The first step is to ensure that the selected systems and technologies used are certified, compliant, and in line with industry standards.

Secondly, you should assume a 360-degree approach to security. It means scrutinizing every aspect of your technology and system environment – where the systems are supported from, how they interact with each other, and from where the systems can be accessed from. Track the end-to-end path of the data in the process: is it signed and encrypted all the way, for whom is it available and visible to?

Five Key Points to Ensure the Safety of the Technology Foundation of Your Payment Process

1. On-premises vs cloud

More and more companies have made the strategic shift and prefer cloud-based solutions offered as SaaS, also in finance, accounting, and treasury functions. The cloud is winning because of its cost efficiency and convenience. Previously, the cloud was avoided in critical functions due to fear of data security risks but now many organizations feel that the security can be organized even better in cloud than on premise.

2. Operating system and software update policy

Whether you are using SaaS solutions or you are running your own IT, the update policy for systems and software needs to be clear. With on-premises infrastructure, you can still opt for outside professional services. With cloud-based operations, the service provider takes the responsibility of maintaining the technology, so that it is always up-to-date and consistent with the latest security features.

3. Interoperability and integrations between systems

The payment process is intertwined with several business and finance processes and their relevant systems. Again, the cloud gives you an advantage with flexible integrations. When considering the security of the data transfer, one needs to look at three different levels: how the data is transferred inside the system, between the internal systems, and from the internal systems to outside systems, e.g. to an outside bank.

4. Secure data transfer

Pay close attention to the application interfaces (API) and demand technology protocols for secure file transfer between systems: SFTP, Web Services, and HTTPS. In addition, use technologies for securing the data that is being transferred. Digital signatures guarantee the integrity and authenticity of the data, and create non-repudiation which means that the message's origin cannot be disputed afterwards. Data can also be sealed with efficient encryption algorithms, such as PGP.

5. Vulnerability and penetration testing

With the ever-evolving threat landscape, software, and systems as well as servers and platforms they are run on, need to be tested on a regular basis, preferably by an outside professional. Regular audits according to industry standards and best practices should be considered – and if the technology is provided from the cloud, these are the things that you should demand from your service provider.

True security demands cooperation from multiple stakeholders within the organization. Now we have covered the versatile proactive measures an organization should consider when aiming for a robust and secure payment process. Next, we will zone into the reactive actions every corporation should also be prepared to take to avoid fraud loss.

DETECTING FRAUD AND ANOMALIES

Keep a close eye on your payment flows

We would be surprised if we all knew how many millions are paid from organizations to fraudsters without no one ever getting wind of the theft. So far, we have examined the different aspects of a safe corporate payment process to help you prevent fraud and mitigate risks. Still, every organization should prepare itself for the reactive measures as well, in case an erroneous payment does manage to enter the system.

If the cash outflows are not properly monitored it could be that money is lost without anyone noticing, and it is not rare that economic crimes are only discovered by accident.

If a fraudulent payment gets made, time is money: if you only then start to figure out who is responsible for which actions, your chances of efficient damage control are scarce. The first step of a well-thought-out reaction plan is to contact the recipient bank and try to stop the money before it gets redirected and becomes impossible to trace and get back.

Intelligent Automation Helps You Spot the Payments That Do ot Belong

Monitoring your payment flows rigorously helps you to spot and stop suspicious payments before the money exits your bank accounts. Modern system solutions offer you support in filtering and blocking payments flows. Rapidly evolving technologies, such as machine learning algorithms and other applications using artificial intelligence, are quickly revolutionizing the system-level support in recognizing and managing deviations, categorizing payments, and issuing alerts and red flags in the accounts payable processes.

Soon, these technologies will make it possible to automate many of the monitoring functions that are today handled manually or automatically by predetermined rules. One of the best features of a machine learning-based algorithm is the fact that it self-learns the logic needed to perform a task by using historic data and human actions. Thus it continuously updated itself.

Pooling your cash daily helps you catch the exceptions. Implementing fast and automated reconciliation of all your bank accounts against your general ledger assures you at the end of each day that everything is on order.

Three Things to Keep an Eye on When Filtering Outgoing Cash Flows

1. Duplicate payments

It is not at all rare that a single payment gets entered into the system twice, and thus paid twice. For instance, if the original invoice arrives to the organization both electronically and on paper. Resolving the situation takes time and effort.

2. Odd countries

Prevent payments to countries you don't have business in. Blacklisting certain, high-risk countries helps you to stop money transfers before your bank does – and freezes your cash for the investigation.

3. The time of execution

If the payment is made outside of the normal payment schedule, it could be worthwhile to check out. Intelligent automation utilizing machine learning and AI will advance in a couple of years' time faster than many are expecting, creating new possibilities for fraud prevention in finance and procurement processes.

AFTERWORD: FINDING THE RIGHT BALANCE

In this e-book, we wanted to highlight different points of the payment process that can contain significant risks and seriously undermine the safety of cash outflows. It might all seem overwhelming at first glance. It just goes to show how many approaches one can take on payment security and that none of the approaches are more important than the other.

We also intended this guide to be a wake-up-call: too often organizations are under the impression that the security of their payment process is intact, when in fact the safety of the process has over time deteriorated without anyone noticing.

To sum up, a holistic view to payment security demands attention to processes, technology, policies, people, and corporate values. Risk mitigation cannot be a siloed action. Building a culture for security is not just a matter of finance and treasury functions, it needs to be shared as a value and guideline for operations throughout the organization.

Finally, we want to emphasize the importance of finding the right balance of security versus convenience. In the end, the main purpose of an organization's payment process is that the payments move efficiently, correctly, and on time to the right recipients, and it cannot be disrupted.

Adding proactive practices, such as approval rounds, inevitably increase bureaucracy and may add delays to the process. In addition, too rigid and cumbersome processes can cause employees to come up with loopholes and alternative ways of operating for better usability. With automated processes, system-level support for technical controls and tools, and centrally managed user rights, the inconvenience caused by the proactive approach can be alleviated greatly.

In the end, it is up to each organization to determine which risks can be accepted in their operations. To be able to do this justifiably, you still need to first find the weak points and be aware of the risks.

Authors

Markus Makkonen
Product Manager

Markus has 10 years of experience from international and complex payment factory projects. Currently, Markus is working as the product manager of the Nomentia Cash Management Platform and bank connectivity.

Jukka Estola
Product Manager

Jukka Estola has over a decade of experience in software development in various roles including tester, test automation engineer, scrum master, QA team manager, and 3rd level support. Currently, Jukka is the product manager of the Nomentia Payments platform.