Information Security Monitor

December 2021

DeNederlandscheBank

EUROSYSTEEM

Content

Observations

Financial sector threat analysis

Outlook for oversight of cyber risks

Sources

Introduction

DNB considers information security and the associated cyber risks to be one of the key operational risks in financial institutions. The number of cyberattacks is on the rise, and their disruptive impact is also increasing steadily. Cyberattacks can seriously damage the continuity of business operations. We therefore share examples to manage these risks in Q&As and Good Practices, conduct sector-wide and individual supervisory examinations of institutions and work with the financial sector in various areas to further strengthen the resilience of institutions.

This 2021 Information Security Monitor presents the latest observations on IT and cyber risks, based on supervisory examinations and information obtained from pension funds and insurers. It also includes a threat analysis and a look ahead to the supervisory activities planned for 2022. Our supervisory meetings and examinations of banks show that the observations presented in this Information Security Monitor are also relevant to the Dutch financial sector as a whole.

The observations in this Information Security Monitor are based on the examinations conducted in 2020-2021 and sector-wide requests for information sent to pension funds[1] and insurers. These sources have been supplemented with signals and incident reports from institutions and information exchanged with other supervisory authorities and partnerships. Where relevant, these information sources have also been incorporated – on an anonymous basis – in this Information Security Monitor.

Observations that frequently occur in our examinations have been incorporated in this Information Security Monitor. We have summarised them in the following three key observations that we wish to bring to the attention of executive board members and internal supervisors (such as key function holders, members of supervisory boards and bodies) of the institutions we supervise:

The information security risk management cycle is not sufficiently effective

Management of information security in the outsourcing chain is crucial

Resilience to cyberattacks must be strengthened

These observations have been set out in further detail in the various sections of this Information Security Monitor.

1 In cases where pension funds have outsourced their pension management, their pension administration organisations were also included in the examination.

Knowledge and expertise of the executive board and internal supervisory bodies

We believe executive board members, key function holders, internal supervisors and supervisory board members have an important and growing role in establishing and maintaining an appropriate risk management cycle for information security and cyber risks. For each element of information security, the Good Practices document on Information Security[2] provides examples illustrating the role of executive board members and policymakers. Sufficient knowledge and attention on the part of executive board members and internal supervisors helps to provide practical safeguards. We see scope to improve knowledge at executive board level in this area. Constructive input and critical questions from executive board members and internal supervisors help the institution to make appropriate strategic and tactical choices.

Cooperation

We believe further cooperation between all parties in the financial sector is essential in order to increase the resilience of institutions. The existing sectoral partnerships such as the ISACs[3] provide added value in this regard. Where possible, stepping up cooperation or entering into new partnerships is not only recommended but actually essential.

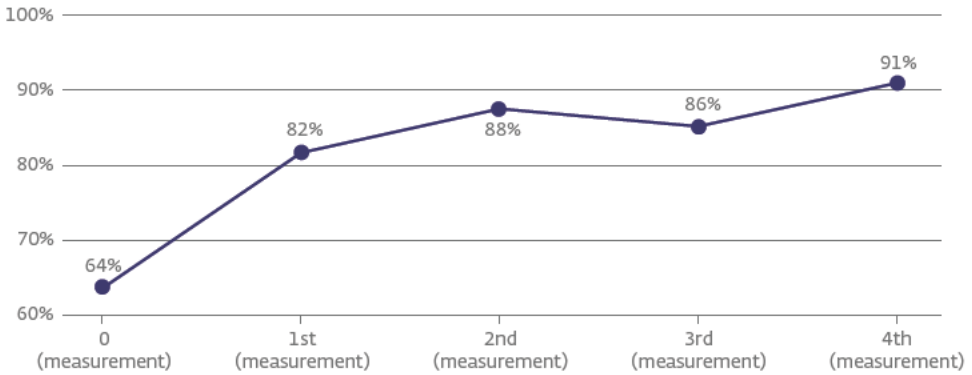
The growing sophistication of cyberattacks makes it difficult for individual institutions to retain appropriate, up-to-date knowledge and experience, but this is available across the sector as a whole. This is particularly relevant given that attackers are increasingly specialising their knowledge, collaborating and "buying in" services. We note that cooperation in sharing information and best practices in cybersecurity is not equally effective in all sectors.

We therefore call on the institutions to pursue or step up cooperation both within and outside the various sectors.

Embedding information security in the internal control framework

In addition to the substantive observations, we note, as in previous years, that the supervisory authority's baseline measurement is a starting point for the institution to structurally improve and safeguard information security. The maturity of information security measures improves as the measures become part of a planning and control cycle set up and formalised by the institution. Based on our examinations, a rising trend can be seen in the percentage of demonstrably functioning controls following an initial assessment by the supervisory authority, see Figure 1.

Figure 1 % level controls per measurement



2 See our Good Practices on Information Security and the accompanying Q&A: Q&A Assessment Framework for DNB Information Security Examination
3 An Information Sharing and Analysis Centre (ISAC) is a sectoral partnership aimed at improving digital resilience.

In practice, we observe that the system for measuring, reporting and improving information security measures becomes a permanent part of the organisation's internal control framework in institutions where various measurements have been carried out, which is a positive development. At the same time, follow-up measurements show that these institutions also have potential to achieve greater maturity in some areas. In these institutions, we often see a shift from implementing to maintaining security standards and to more efficient demonstration of the functioning of the security framework.

Conclusion

Technology plays an important role in all activities of financial institutions. In order to cope with evolving cyberthreats, it is very important for the institutions to be able to rely on a strong foundation of information security – a foundation that on the one hand provides a solid structure on which to organise the management of risks and on the other hand adapts to current developments. In this regard, controls are not static. It is still important to maintain a risk-based approach whereby controls are adapted in line with the trend of growing cyberthreats. Like ESG factors, the Technology ("T") factor has become a more central theme of institutions' policies and related decision-making in the past year.

Observations

Observation 1: The information security risk management cycle is not sufficiently effective

It is clear from pension funds and insurers that IT risk management needs attention in order to grow to the required maturity level. In some cases, there is no evaluation of whether the risk management framework is adequate and of sufficient depth to actually implement fundamental control improvements and measure their impact on information security risks. Furthermore, information security risk is often not an integrated part of an organisation's overall risk management framework.

The Good Practices on Information Security (GP IS) document describes what we understand by the risk management cycle:

> The institution must identify and analyse the relevant information security and cybersecurity risks on a regular basis. Based on this risk analysis, the institution determines its response, takes measures to mitigate risks and accepts any residual risks (possibly temporarily). Accepted residual risks are periodically re-evaluated and submitted for acceptance.

The GP IS also describes the tools and maturity levels required for the proper fulfilment of the risk management cycle. We believe good risk management is a key prerequisite for the structural embedding and adaptation of information security. We associate this with a higher maturity level "4" for risk management controls. The GP IS states that the risk management cycle must function effectively (level 3) and that institutions must regularly evaluate the effectiveness of their risk management (level 4). In other words, there must be a verifiable mature process that is regularly evaluated.

> In the Good Practices on Information Security (GP IS) we provide tools to determine maturity levels from 0 to 5. To reach maturity level 4, the institution must periodically evaluate the design of its controls. In doing so, we expect the institution to evaluate whether its risk management could be structured better or differently and whether the mix of controls is effective or possibly requires adjustment.[4]

An evaluation addresses questions such as: Is the design of this process still adequate? Are all the sub-checks still effective? Have the latest scenarios (including attack scenarios) been considered? What alternative best practices are we aware of? Are those alternatives better suited to us?

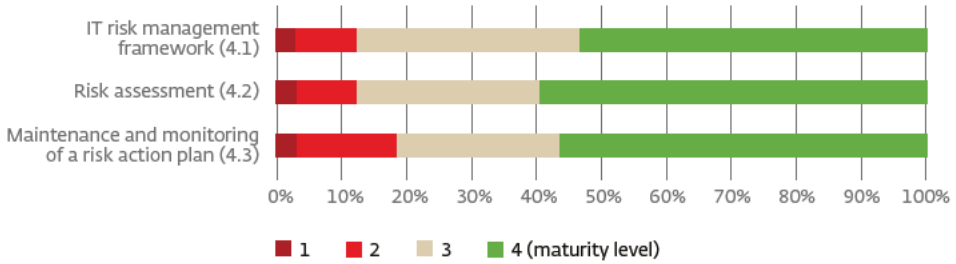
The executive board also has a role in evaluating the risk management cycle. Factors include the appropriateness of information security governance and an assessment of the effectiveness of the mix of controls in staying within the institution's risk tolerance limits.

4 A detailed description of the criteria for each maturity level can be found in the Good Practices on Information Security. See the Good Practices document and accompanying Q&A: Q&A Information Security (dnb.nl)

Results of supervisory reviews

The results of the supervisory reviews show that over 40% of the reviewed institutions have not reached maturity level "4" for the three controls in the risk management cycle.

Figure 2 Risk management cycle



Examples of observations in institutions with a lower maturity level are:

- No evaluation whatsoever of the risk management cycle.
- The information security framework is not part of the organisation's overall risk management framework.
- Insufficient depth in evaluations to actually achieve improvements, for example not using scenario analyses as a risk management tool.
- The scenario analyses used do not reflect the institution's recent threat assessment. This may be due to the lack of a specific scenario for a successful ransomware attack or insufficient operational implementation of the scenario, for example in the form of a run book, test plans and/or exercises.

Failure to evaluate the IT risk management framework, or failure to do so on time, increases the information security and cyber risks for the institution. An institution selects, implements or modifies internal controls based on the results of risk analyses, with the aim of continuing to operate within the specified risk tolerance limits. These risk analyses are therefore an important basis for the creation of a customised IT risk management framework that mitigates the most important specific risks. By periodically updating these risk analyses, institutions can evaluate whether the current set of controls is and remains adequate.

Cyberthreats are highly variable. If this evaluation does not take place or does not take place on time, there is a risk that institutions will rely on controls that do not adequately mitigate the changed cyber and other threats. In this regard, controls are not static. It is still important to maintain a risk-based approach whereby controls are adapted in line with the trend of growing cyberthreats. Like ESG factors, the Technology ("T") factor has become a more central theme of institutions' policies and related decision-making in the past year; this is supported by the full inclusion of information security risks in internal control frameworks.

Experiences based on TIBER tests[5]:

TIBER tests have shown that institutions mainly think from the perspective of the institution itself and much less from the perspective of possible attackers when identifying risks. This leads to "internal tunnel vision". TIBER tests have shown that attackers regularly pursue targets other than those the financial institution has identified itself.

For example, a significant proportion of institutions are particularly concerned about attackers seeking financial gain, whereas many attackers also have other intentions, such as sabotage, disruption and economic or political espionage. Penetration tests based on current threat information are a valuable tool in determining relevant risks. They are also used to test the design and operation of the risk management framework.

The GP IS includes examples relating to the risk management cycle.
The examples below are derived from these:

- An institution surveys and evaluates the measures taken on the basis of scenarios. It periodically adapts the scenarios on the basis of threat analyses geared to the institution. A good example is a ransomware attack scenario.
- When evaluating the risk framework, the executive board explicitly assesses the extent to which information security risk management is part of – and consistent with – the organisation's integral risk management framework.
- The institution identifies its "crown jewels", evaluates them on a regular basis and relates them to current threats and risk controls. It takes additional control measures where necessary. It adjusts, replaces or terminates any controls that are ineffective or no longer adequate.
- It includes all the outsourcing chain risks in its risk analysis. It periodically assesses the action plans of service providers in the chain to ascertain their relevance and the extent to which the services still meet (or can meet) the institution's requirements. If any deviations are observed, the institution enters into agreements with the parties concerned to mitigate the risk to an acceptable level within its risk tolerance limits.

5 Threat intelligence-based ethical red teaming, see section 5.2

Observation 2: Management of information security in the outsourcing chain is crucial

Outsourcing and chain cooperation have become an indispensable part of financial institutions' operational management. Managing information security in outsourcing requires specific knowledge and measures. Studies show that institutions find it difficult to set up this control of the entire chain in a transparent and adequate manner.

Developments such as the creation of partnerships, unbundling of the value chain and outsourcing[6] mean that institutions' management of information security transcends the boundaries of their own organisation.
Horizontal unbundling, for example, may allow the contact between the consumer and a traditional financial institution to take place through a FinTech operator's environment. Consumers can then view a summary of all their accounts at different banks through a single party.

Vertical unbundling in the value chain means that service providers take over one or more links in the value chain from financial institutions, for example through outsourcing. The proportion of outsourcing is increasing every year. A comparison between DNB research from 2017 and 2021 shows that insurers' outsourcing expenditure almost doubled in four years from 20% to 36% as a percentage of total operating costs. This rise is borne out by empirical observations. Many insurers launched outsourcing projects in 2017. It is likely that these projects were scaled up, leading to this structural rise. In the case of pension funds, we are not (yet) seeing this strong rise throughout the outsourcing chain, but the degree of outsourcing in the first link of the chain is already quite high (e.g. outsourcing of pension and asset management activities).

Our sector-wide analyses show that many institutions' critical or important processes are highly dependent on IT service providers. This is illustrated in Figure 3 below.

Figure 3 Degree of dependence on IT service providers

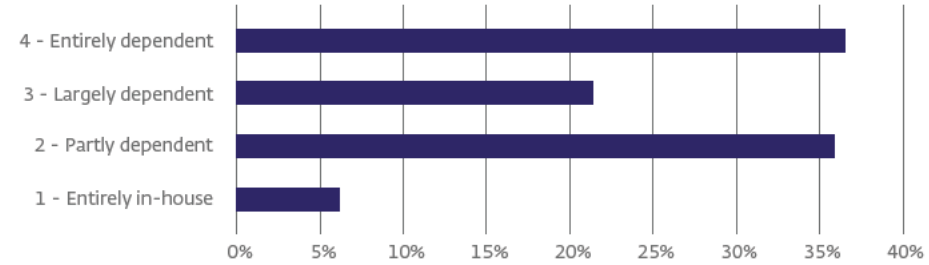


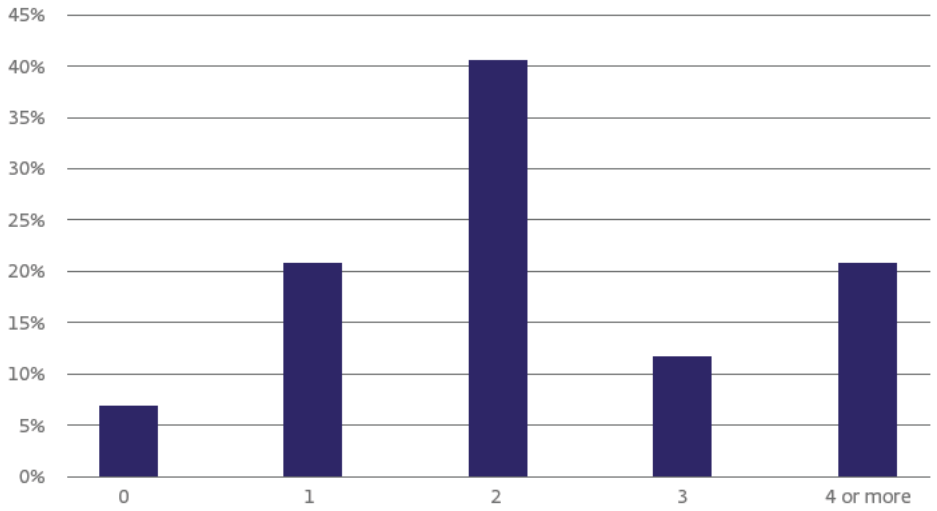
Figure 3 shows that over 35% of institutions depend entirely on IT service providers for the operation of their critical or important IT processes. Furthermore, there is a discernible tendency for institutions to rely heavily on one or more cloud service providers (CSPs) for the operation of a critical or important business process. This is illustrated in Figure 4 below.

Figure 4 shows that over 20% of institutions have to deal with four or more CSPs involved in critical or important business processes.

Vertical and horizontal unbundling means that the institutions are increasingly part of and dependent on a chain of service providers for the performance of their primary tasks. As a result of these developments the information security risks are also shifting towards the chain of which the institutions form part. Institutions will have to gear their controls and maturity levels to these risks and also manage

6 On this subject see also the report: Changing landscape, changing supervision – Developments in the relationship between BigTechs and financial institutions, "Rise of BigTechs requires adjustments in financial supervision" (dnb.nl)

Figure 4 Number of cloud service providers involved in critical or important business processes (% of institutions)



outsourcing relationships in such a way that the level of maturity of the controls is demonstrably maintained. In the GP IS this is described as follows:

> Institutions remain ultimately responsible for the activities performed by service providers. In order to fulfil this responsibility, it is important that the institution enters into agreements with service providers on appropriate controls and that it reviews, monitors and regularly assesses them with regard to effectiveness in accordance with the risk profile. The institution should take additional control measures where necessary.

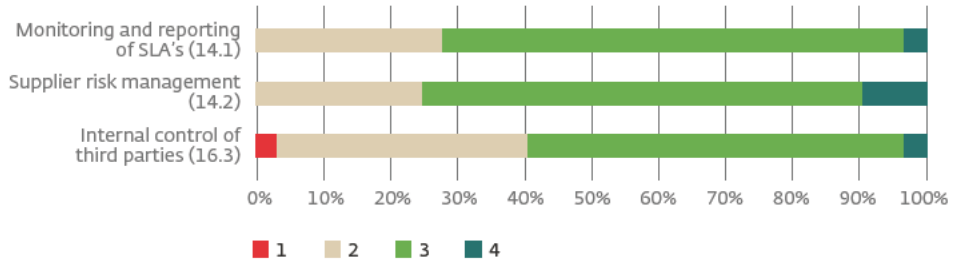
Results of supervisory examinations

Our examinations reveal the following key findings with regard to outsourcing:

1. **Institutions are not demonstrably verifying, monitoring and measuring the extent to which service providers and subcontractors are complying with their agreements in the field of information security, cybersecurity and business continuity.** Institutions have controls with insufficient maturity levels in this area. An example is where an institution does not ascertain whether contractual agreements have been sufficiently implemented in the service provider's processes and controls and does not receive a corresponding report. Another example is where an institution has insufficient visibility on the business continuity safeguards and the ability to leave the service provider.
2. **Institutions have not established sufficient risk management processes with regard to their service providers.** As a result of the coronavirus pandemic and large-scale homeworking we saw institutions carrying out additional risk analyses on their critical service providers. It is nevertheless clear that institutions lack sufficient maturity in this area. A frequent observation is that the service provider to which operations are outsourced is unable to give the institution information on the specific risks involved.
3. **The reviewed institutions lack sufficient information on the design, existence and effective operation of controls of critical service providers and any subcontractors involved in the outsourcing chain.** Possible remedies include requesting and assessing assurance reports or conducting inspections on the service provider's premises. A concern with regard to assurance reports is that service providers' statements often omit parts of the chain (carve-out), even though they contain critical data and information concerning the institutions. The scope of the statement consequently does not cover all the controls relating to information security along the entire chain.

These are controls #14.1, #14.2 and #16.3 of the GP IS. Figure 5 shows the maturity levels of these controls.

Figure 5 Controls regarding the outsourcing chain



Too little expertise and knowledge at the executive level of institutions and inadequate controls relative to the risk profile can lead to:

- The risk that an institution, when entering into the contract, does not sufficiently ensure that the IT chains relating to critical or important processes are fully understood, documented and laid down in adequate contractual agreements, resulting in insufficient control of the subcontracting risks.
- The risk that institutions lack sufficient insight into their service providers' execution of the contract and control of cyber risks, for example due to inadequate agreements on performance and internal control and the associated reports.

This may expose institutions to risks that exceed their risk tolerance limits.

Observation based on TIBER tests

The growing influence of third parties on institutions is also observed within the TIBER programme. When these third parties are not included in the testing, the results give a less clear view of the actual state of these institutions' cyber resilience. After all, the introduction of an increasing number of third parties means the attack surface is becoming larger, but the part that can be tested in the institution itself is becoming smaller in relative terms. The role and function of third parties is thus increasingly becoming an integral part of TIBER scenarios and tests.

Case study

In February 2021 it became known that a significant number of confidential patient records of US citizens had been publicly accessible for some time. The data was held by a medical research company and included confidential patient information and scans of identification documents. The cause of this data breach turned out to be an incorrectly configured web server operated by a cloud service provider. According to security researchers, such errors are occurring more frequently due to uncertainty about the division of responsibility for data security between the cloud service provider and its customers.

The GP IS includes examples relating to outsourcing. The examples below are derived from these.

- An institution has drawn up a risk analysis on the continuity and reliability of services for which it can use the service provider's expertise. Risks of parties to which the services are subcontracted are included in the risk analysis.
- An institution tests its critical systems and processes annually, with the outsourced parts being included in the tests.
- An institution includes specific annexes on compliance and information security in the outsourcing contracts. These include agreements to fully map and document the IT outsourcing chains for critical or important processes to provide visibility on significant subcontracting. Adequate contractual agreements have also been made with service providers in order to comply with applicable legislation and internal policies.
- An institution receives and assesses independent audit and assurance reports on the management of risks relating to information security and cybersecurity of the service provider and the main subcontractors involved. The reports are in line with the agreed services, which include the controls from the GP IS.
- A group of institutions decide to pool their knowledge in order to manage their outsourcing risks. They exchange good and best practices and share experiences. The institutions' monitoring is consequently better aligned with the outsourcing risks and the common service provider can report in a more standardised way on many areas. Pooled audits are also conducted on the common service providers.

Observation 3: Resilience to cyberattacks must be strengthened

The combination of preventive, detective and corrective measures and cyber resilience testing is very important in order to ensure that an institution is resilient to cyberattacks and to mitigate their impact. Some institutions, however, have not set up mature controls in all cases.

In order to repel or mitigate the impact of digital attacks, the following measures are important: good cyberhygiene as the basis for prevention, adequate attack detection, setting up recovery processes and regular cyber resilience testing.

- Preventive measures limit the probability of success of a digital attack by applying and maintaining security standards. The mix of these measures is summarised below under the cyberhygiene heading.
- Detection and response consists of tooling and processes to monitor and respond to attacks.
- Recovery processes enable the institution to limit the damage and safeguard the continuity of its business operations.
- In cyber resilience testing, resilience is strengthened by simulating and learning from digital attacks on production systems.

These elements are closely linked, so we have combined them into a single observation. A series of elements are detailed below.

Cyberhygiene. Cyberhygiene means that the foundation of information security measures is and remains mature and in good order. This includes basic measures such as staff awareness, access security, virus/malware scans, change management and back-ups. An important part of this is understanding potential weaknesses and resolving them as quickly as possible. Possible weaknesses could be: backlogs in patch management of systems and systems that are no longer maintained by vendors.

The GP IS states as follows with regard to vulnerability management (#19.2):

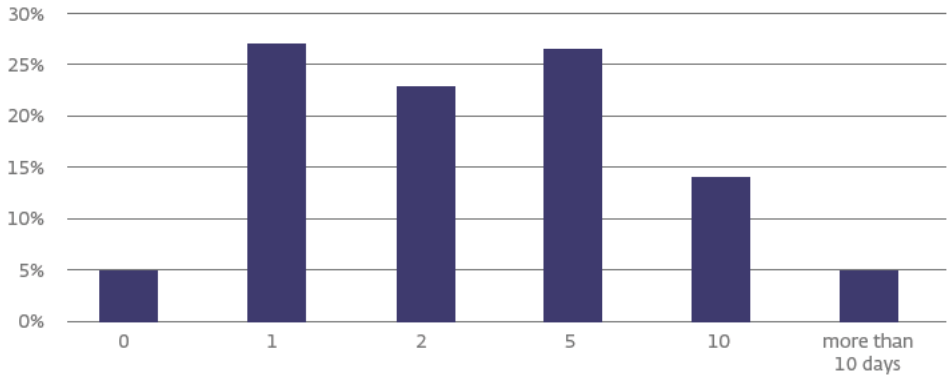
> The main IT assets are identified on the basis of a risk analysis. Partly on the basis of threat intelligence and vulnerability scans, the institution regularly performs checks of IT assets to identify any cyber or other vulnerabilities, and determines the impact of these on its processes. Based on the impact, risk mitigating actions are determined for threats falling outside the institution's risk tolerance.

More attention should be devoted to understanding potential vulnerabilities in IT systems and the associated risk assessment. Our reviews show there is insufficient maturity in vulnerability management. In many cases this manifests itself in the lack of a clear overview of the main IT assets or an understanding of their potential cyber and other vulnerabilities.

Once the IT assets have been identified, it is important to continue to monitor them for vulnerabilities. One of the aspects that can be monitored is the speed of applying critical patches to resolve vulnerabilities in IT systems. The speed of patching reduces the risk of systems being susceptible (or more susceptible) to external attacks.

Figure 6 shows the speed of patching based on our 2021 sector-wide analysis. We note an improvement in the speed of patching compared to our examinations in previous years. However, this figure also clearly shows that 5% of institutions say it takes them more than 10 days on average to implement critical security patches on IT production systems.

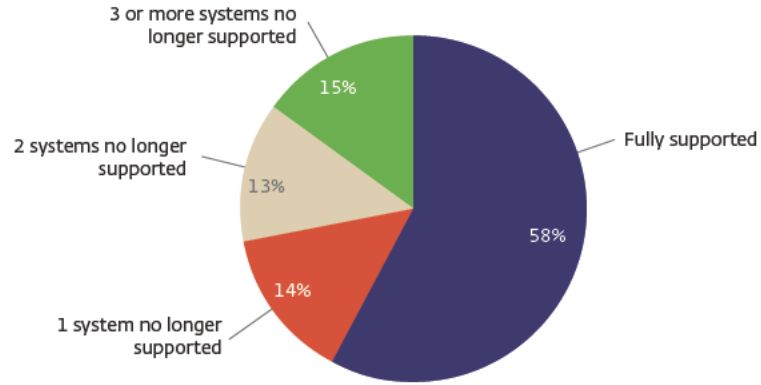
Figure 6 Speed of implementation of critical patches (in days)



An accurate, complete and up-to-date record of all IT systems used by an organisation is important to ensure that those systems are being maintained and/or phased out in a timely manner, so as not to compromise the desired level of information security. We note that there is still (sometimes substantial) room for improvement, both in the registration and timely maintenance and phasing out of IT systems. Institutions using IT systems that vendors are no longer supporting with security updates are at risk of possibly permanent security vulnerabilities.

A total of 58% of institutions indicate that all their identified critical systems[7] are supported by vendors; 42% have one or more critical systems that are no longer supported (end-of-life systems, see Figure 7).

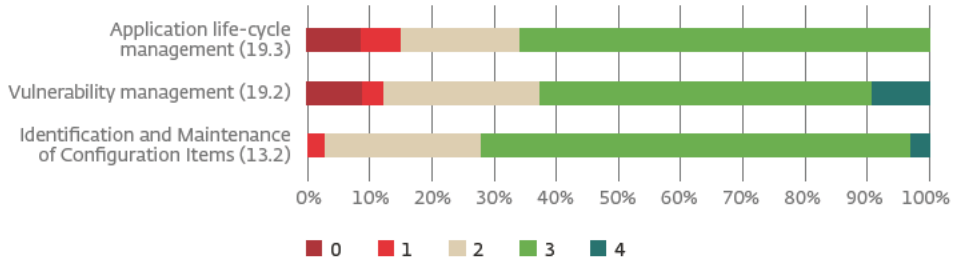
Figure 7 Institutions whose systems are no longer supported by vendors



Those are sufficient grounds to pay continued attention to the management of these risks. By way of illustration, the results for the reviewed institutions are shown below (Figure 8).

7 These include operating systems, database systems, network systems and policy administration systems

Figure 8 Cyberhygiene maturity level



In order to repel attacks or mitigate their impact, it must be possible to detect them. Adequate monitoring is a basic prerequisite for this. Historically, organisations have devoted a lot of attention to preventive measures in the field of information security and cyber risks. When these measures prove inadequate, it is important that detective measures are in place for the timely detection of an attack or an unauthorised act by an employee.

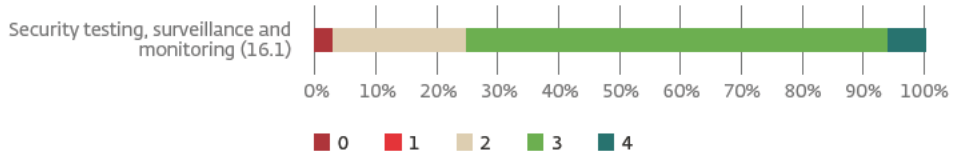
In 2021, 5% of Dutch insurers and pension funds stated that they had been the target of a successful cyberattack resulting in actual unauthorised access to internal systems or data.

To maintain resilience, it is therefore important that the institution devotes particular attention to the monitoring of its network and systems within its control framework. The GP IS includes controls relating to this monitoring. An important control in this respect is "16.1 Security testing, surveillance and monitoring". This describes the process that the institution can set up to manage the risks in this area:

> IT systems are monitored for unusual activities. Exceptions are identified and followed up. The institution uses logging tools, for example, to rapidly identify and respond to deviations in patterns.

The results of our examinations show that a quarter of the institutions do not have mature processes for detecting possible network intrusions (see Figure 9). This may lead to attackers remaining undetected for long periods and gathering information about the operation of IT systems and/or extracting data without the institution's knowledge. The impact of such an attack is therefore greater than in cases where the organisation is able to conduct close monitoring and rapidly identify intrusions in its environment.

Figure 9 Level of maturity of security testing, surveillance and monitoring

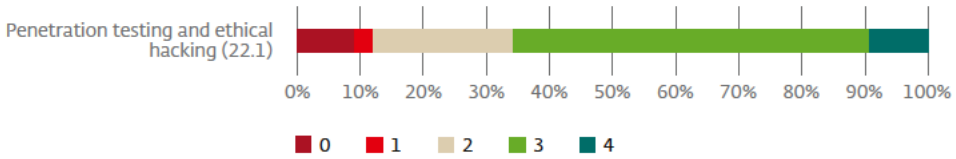


As well as paying attention to cyberhygiene, it is important that the institution conducts regular tests. A good way to periodically test the cyber resilience of the institution is to do so on the basis of a risk analysis and current cyberthreats in order to detect weaknesses and show their possible impact. This kind of testing is also called penetration testing (or pen testing) and ethical hacking. The GP IS states among other things:

> On the basis of a risk analysis and current cyberthreats, the institution determines the type of security tests to be performed, as well as their scope and depth. The nature and frequency of these tests depends on the institution's risk profile.

Based on the results of our reviews, around 34% of the institutions have insufficient controls in place in this area. Some institutions (9%) do not carry out any tests at all. 25% of institutions do not carry out sufficiently structured tests, so the process is not mature (see Figure 10).

Figure 10 Maturity level of pen testing and ethical hacking



A possible risk is that institutions may rely on controls that are no longer up to date and can be circumvented – without detection – on the basis of (possibly known) attack techniques.

Observation based on **TIBER-tests**

If an attacker is motivated and sophisticated enough, they will eventually succeed in gaining entry. This is a key finding from five years of TIBER testing. Institutions must therefore deploy a multi-layered defence. This "in-depth" defence should not only keep attackers out (prevention), but also provide adequate detection and a means of removing attackers from systems (response).

Phishing or spear phishing, for example, is an intelligence-based attack vector that is regularly used in the TIBER programme. Evaluations of these tests show that phishing or spear phishing cannot be entirely mitigated by putting more emphasis on awareness campaigns. Training and awareness campaigns reduce the number of people clicking on phishing mails, but bringing this down to 0% is unattainable. Experience therefore shows that it is dangerous to assume that any defence against phishing or spear phishing is watertight. A deep defence with multiple barriers, including an internal anomaly detection system, is therefore essential in order to detect the entry of attackers and mitigate the impact.

On the one hand, the presence of these "basic measures" is crucial for withstanding digital attacks. On the other hand, it is equally important to test and evaluate the defence layers and plans periodically, as an institution's resilience to cyberattacks only becomes really clear if "paper measures and plans" are tested in practice.

Case study: testing in cooperation with DNB

In addition to our supervisory function, we work in the TIBER programme with institutions in the banking, pension and insurance sector to improve the digital resilience of the financial sector by carrying out joint testing. See section 5.2 of this Information Security Monitor for more information on our TIBER programme.

Case study: logging

After a successful phishing attempt, a hacker is found to have gained access to an employee's account. After detecting the account breach, the institution wants to assess the hacker's activities. However, the institution has hardly any logging or specific tools in this area, so it cannot determine what the hacker has done on its systems and network. The institution therefore has to assume that the hacker had access to all data and systems and, on that basis, must assess the potential impact and take appropriate measures.

The GP IS includes examples of the monitoring of actual or potential vulnerabilities. The examples below are derived from these.

- An institution performs several types of security tests with the involvement of its outsourcing chain service providers, such as pen tests aimed at infrastructure and application security, red teaming, physical security tests and human behaviour tests in relation to information security and cybersecurity.
- An institution assesses vulnerabilities frequently (daily) on the basis of threat intelligence and uses tools to carry out automated vulnerability scanning.
- Potential attack methods can be recorded in scenarios that form the basis for generic and institution-specific use cases that are fed into the monitoring applications. The recording of use cases shows how, what, where and which threshold values need to be measured in order to detect and respond rapidly to possible attacks.
- As well as paying close attention to identifying and monitoring vulnerabilities, an institution may decide to further limit the potential impact of a successful cyberattack by micro-segmenting its network. This involves a further reduction of rights, with particular attention also being paid to the rights of administrators. The network is divided into layers and self-contained environments. This prevents an attacker – once inside – from gaining access to everything.
- Security tests also provide very useful information for other institutions, on the one hand to apply the used scenarios to their own organisation, but particularly to test the generic test findings on their own organisation. These insights are shared in various partnerships (such as the ISACs).

Financial sector threat analysis

This section describes a number of threats to the Dutch financial sector. In our reviews we take into account the threats included in this threat analysis, such as the evolution of risks over time and the direction in which they are moving. It is therefore an important indicator for determining priorities in the supervisory approach.

Adequate digital resilience is crucial for the functioning of the Dutch financial sector. Increasing digitalisation means that financial institutions are increasingly becoming "IT companies with operations in the financial sector". Threats to the financial sector are therefore increasingly concentrated in the digital domain. Based on multiple sources[8] and contacts with institutions, we consider the following four threats to be a priority for the sector:

- Ransomware
- Attacks on or through third parties in the outsourcing chain
- Long-term compromise
- DDoS

Ransomware

The number of ransomware attacks has risen sharply since the start of the coronavirus crisis, according to sources such as the Cyber Security Assessment Netherlands 2021[9]. Institutions in the international financial sector and/or relevant third parties are also regularly affected. Mounting a ransomware attack is becoming more accessible to an ever-growing group of criminals due to the availability of ransomware-as-a-service (RaaS).

On the dark web[10] a "service economy" of criminals specialised in carrying out parts of ransomware attacks has emerged in recent years. There are criminals who sell access to companies, while others specialise in developing and distributing ransomware. Large parts of an attack can therefore sometimes be purchased on a modular basis. There are even criminal providers that sell complete "attack packages". However, it is not only the quantity of attacks that makes ransomware a major threat, but also their changing nature. Whereas previously ransomware attacks primarily involved the encryption of data, regular attempts are now made to steal critical data. The attacker then threatens to publish or sell the data unless the ransom is paid. This is known as "double extortion". Another important reason for the popularity of ransomware is its potential profitability. The availability of RaaS means criminals only have to make a fairly small investment, whereas the potential gains are massive. Ransoms can run to tens of millions of euros.

8 Three primary sources for the Information Security Monitor are (1) Europol's EC3, (2) the NCSC's CSBN and (3) the 1Financial Threat Landscape for the Netherlands (1FTL-NL). The 1FTL-NL is a threat assessment produced by and for the Dutch financial sector through the FI-ISAC.
9 The Cyber Security Assessment Netherlands is published by the National Coordinator for Counterterrorism and Security, see https://english.nctv.nl/documents/publications/2021/08/05/cyber-security-assessment-netherlands-2021
10 The dark web is the hidden collective of internet sites only accessible by a specialised web browser. It is used for keeping internet activity anonymous and private.

Attacks on or through third parties

As stated above, digital attacks on financial institutions can have a potentially large impact, but so too can attacks on third parties. Financial institutions are outsourcing a growing number of services, systems and processes to larger and smaller digital partners. Examples are data storage, payment systems, software and workplace facilities. This digital dependence has various implications for the cyber resilience of the financial sector. The paradox is that on the one hand third parties specialise in what they do and normally set great store by security. On the other hand, they regularly appear to be attractive targets for digital attackers. There are several explanations for the recent rise in attacks on or through third parties. Firstly, there is a concentration risk. Attackers can use a single third party as a springboard to gain access to multiple customers, so attacks are easily scalable. Secondly, the use of third parties increases the attack surface for cybercriminals. They can choose multiple routes or multiple third parties to gain entry to an organisation. A third explanation is that financial institutions are partially relinquishing control over cyber resilience. Third parties often provide highly specialised services. Precisely for this reason it is difficult for financial institutions to objectively determine and test the quality of the third party's cyber resilience by obtaining reports or conducting audits. Some third parties only disclose limited details of security or incidents.

Long term compromise

A threat that is rarely perceived but nevertheless remains relevant to financial institutions is long-term compromise. This is where sophisticated groups – often at nation state level – maintain a long-term presence in a financial institution's networks and systems. The sophistication of the attacker means that such intrusions are often very difficult to detect. Attackers can thus gain a great deal of knowledge about the institution and its customers over a protracted period, without the institution being aware and able to take action. The fact that a long-term compromise is seldom detected or publicly visible is no guarantee that it will not occur. Financial institutions must therefore remain alert to these invisible but extremely damaging attacks.

DDoS

Although Dutch financial institutions have taken many steps to prevent DDoS attacks in recent years, the threat remains real. This is mainly due to the unpredictability of DDoS attacks. Sometimes several months can elapse without a DDoS attack being detected, whereas at other times attacks occur in rapid succession. Here too, criminals' ability to access tools to perpetrate a DDoS attack is a cause for concern. This cycle has been going on for as long as financial institutions have been offering online services. There is often no clear justification for the launch of a DDoS attack. It is therefore important that institutions remain alert to any upsurge in attacks, so that they can rapidly adapt their countermeasures.

Outlook for oversight of cyber risks

As a result of the ongoing developments in information security and cyber security, institutions must pay constant attention to upgrading and maintaining the quality of their information security systems. The management of technology risks occupies a prominent place in our Supervisory Strategy 2021-2024[11]. The section entitled "Responding to technological innovation" defines three focus areas:

1. Institutions and their service providers must be able to demonstrate that their information security is in order and must regularly test their cyber resilience.
2. Institutions must devote attention to increasing and updating executive and supervisory board members' knowledge of and involvement in IT and cyber risks. In order to manage the growing cyber risks it is important to have sufficient knowledge at board level.
3. Institutions increasingly transfer their data and IT processes to third parties that are not under direct supervision[12]. Institutions themselves nevertheless remain responsible for data security and regulatory compliance at all times. Our particular focus is on specific forms of outsourcing, where business or IT processes are based on an external solution provided by BigTechs, for example. In the years ahead, we will conduct more targeted oversight of these forms of outsourcing and assess whether they comply with the applicable laws and regulations and the outsourcing guidelines published by the EBA[13] and EIOPA[14].

In addition to the above three items from the Supervisory Strategy, we emphasise that cooperation between institutions in the financial sector can have a positive impact on the management of information security and cyber risks in all links of the outsourcing chain. We see this in various ways in practice, for example in information exchanges between institutions on current threats and the sharing of lessons learned from incidents and exercises. This can ensure that institutions are better prepared for potential threats. We also see that institutions that already have relatively high maturity with regard to information security set consistent requirements for service providers and help less mature institutions to improve by exchanging best practices.

11 Supervisory Strategy 2021-2024 (dnb.nl)
12 On 24 September 2020 the European Commission published a legislative proposal, the Digital Operational Resilience Act (DORA), to set uniform requirements for financial institutions and third-party providers of critical services to financial institutions (including the use and security of ICT). Its intention is to establish a form of European oversight of designated significant service providers.
13 The European Banking Authority (EBA) is the European prudential supervisory authority for the banking sector.
14 The European Insurance and Occupational Pensions Authority (EIOPA) conducts prudential supervision of the insurance and pensions sector in Europe.

Redesigned supervision approach

In December 2020 we informed our supervised institutions of our redesigned supervision approach[15] in which the intensity of our supervision increases the more negative the impact of the risks is on trust. The supervisory activities are therefore composed on the basis of the impact category assigned to the institution and the recorded risk scores. An institution can also be selected for review as part of a supervisory theme regardless of the assigned impact category and risk score. Cyber risk is an important supervisory theme for 2022.

Risk scores assigned to an institution (e.g. for operational and IT risk) may also trigger risk identification or risk mitigation follow-up by DNB. Risk identification is carried out by means of a risk-identifying interview, a deep dive or an on-site inspection. The supervisory activities also include (possibly recurring) data requests and round tables/seminars.

Supervisory theme 2022: Cybersecurity along the whole outsourcing chain

A development impacting the financial sector is cyber risk, which is growing fast due to the increasing dependence on digital services, processes and systems and a growing level of outsourcing and subcontracting. The trend towards outsourcing digital business processes leads to increasing dependence on third parties. This makes institutions vulnerable to any disruptions affecting their service providers. In this regard we will continue our risk-based examinations of institutions in 2022 to assess whether they are devoting sufficient, systematic attention to effective controls along the whole outsourcing chain. Our oversight will also cover the impact of new laws and regulations, such as DORA. We will also devote particular attention to the role and level of knowledge of executive directors and internal supervisors on this subject in 2022.

15 This supervisory approach does not apply to banks that are subject to SSM supervision. For more information see the DNB brochure entitled: "Our redesigned supervision approach"; ATM brochure (dnb.nl)

Sources

Research sources from our supervisory function

Research into the foundation of information security

We have been researching the management of information security and cybersecurity in the Dutch financial sector for many years. Since 2010, this research has been based on periodic self-assessments completed by the institutions subject to our supervision. As a tool to aid the performance of these self-assessments, we updated the Good Practices on Information Security and accompanying Q&A in 2019.

Sector-wide Analysis of Information Security (SBA-IB)

In 2021 we started systematically requesting information on the maturity of information security from insurers and pension funds based on the Sector-wide Analysis of Information Security (in ducth known as the: SBA-IB). The SBA-IB contains questions concerning the institution's exposure to IT risks, including information security risks. The SBA-IB also assesses the maturity of the controls in the field of information security. Information from this SBA-IB is used to identify an institution's risk profile.

Examinations and on-site inspections of supervised institutions

We carry out risk-based, targeted examinations and on-site inspections of IT and cyber risks among supervised institutions. The on-site observations in these institutions together with the inspection reports have contributed to the observations in this Information Security Monitor.

Reports, signals and incident reports from supervised institutions

DNB account supervisors are in contact with supervised institutions on a daily basis. They are the first point of contact for institutions within DNB and therefore receive frequent information on operational matters including IT and cyber risks. Sectoral legislation also requires institutions to report major cyber and other incidents to the supervisory authority as soon as possible.

Research sources based on our central bank function

Results of TIBER tests

In June 2016, as part of our central bank function, we worked with the financial sector to launch TIBER-NL (threat intelligence-based ethical red teaming), a programme developed to increase the resilience of financial institutions against cyberattacks. Hack tests on production systems, based on current threat intelligence, are a key component of the programme.

These tests show generally high levels of cyber resilience. At the same time, they show that sophisticated attackers could potentially cause a lot of damage to institutions that are essential for financial stability. Had they been genuine attacks rather than controlled tests, they would in some cases have caused failures of critical functions, losses of highly confidential information, financial losses or market manipulation.

Relevant experiences and information gained from this programme have also been included in this Information Security Monitor.

Disclaimer

This Information Security Monitor contains various examples of good practices. Good practices are non-binding recommendations for the application of legislation in the area of controlled and ethical performance (for example Section 18 of the Financial Assessment Framework Decree, Section 3:17 of the Financial Supervision Act and Section 143 of the Pensions Act) to the supervised institutions.
Good practices help us to set out our views on observed or expected behaviour in policy practice that reflects what we believe to be an appropriate application of the rules to which the good practices document pertains.

By means of good practices we aim to encourage supervised institutions to take our expectations into account in their considerations and decision-making, without being obliged to do so, while also taking into consideration their specific circumstances.
A good practices document provides insight into the behaviours we observe or expect in policy practice. It is only indicative in nature, and therefore does not alter the fact that some financial institutions should apply the underlying regulations differently, and possibly more strictly. The institutions themselves are responsible for deciding whether and how to adopt the rules.