

# Staying on top of a never-ending war

PwC's Thailand Economic Crime and Fraud Survey 2020



# Content

4

Overview

5

Respondents' experience with fraud

8

Calculating the impact

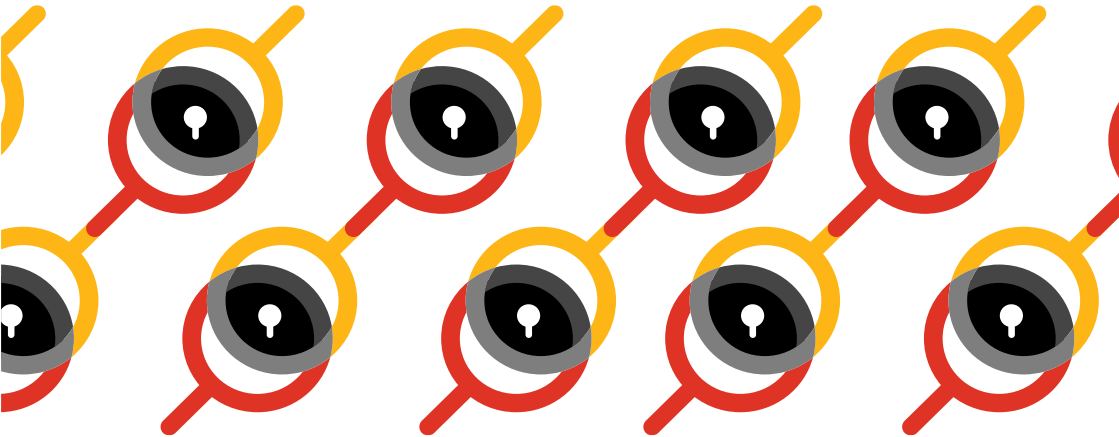
11

Who is committing fraud, and how is it being detected?

14

How to win the war, even if you lose some battles





# Preface

PwC's Thailand Economic Crime and Fraud Survey 2020 found that one-third of Thai companies had been affected by fraud, corruption and other economic crimes during the last two years, well down from the 48% who reported being victims of at least one attack in 2018. We believe this response tells us more about companies' preparedness to detect and respond to crime than it does about how much crime is actually occurring.

We believe that when reported incidences are higher, as they were in 2018, this indicates that companies are investing more in the fraud detection programmes, specialized staff and technology needed to detect crime. And when reported incidences fall, like they did this year, this could mean fraudsters are winning the war, evolving their methods and using new technologies to breach defences undetected.

Today's companies need to take on board that the risk of economic crime is not going away any time soon. If anything, companies are becoming even more exposed as the business environment changes to take advantage of new technologies.

The fight against economic crime and fraud is a never-ending war. Especially in this increasingly complex world, companies need to focus more than ever on assessing their defences against fraud, and their readiness to respond with effective fraud-fighting measures when they discover an attack. Companies that take appropriate steps today can turn the table against fraudsters and can start to win the war.



**Shin Honma**

Partner

Forensic Services,  
PwC Thailand

# Overview

The battle against fraud, corruption and other economic crimes is a never ending one, and companies can pay a steep price if they leave themselves exposed.

In addition to direct financial losses, companies also face less tangible damages such as brand damage, a loss in market position, and declining workforce morale.

This survey is an essential part of the toolkit for companies that want to stay on top of the battle against economic crime. It provides extensive insight into the types of crime that companies are at risk from, who is responsible, and the impact companies face if they get hit.

Most importantly, the survey shows what the most successful companies are doing to protect themselves from fraud and other financial crimes, as well as how some companies have responded to being attacked to build an even stronger organisation out of the experience.

The key message is that economic crime is an ever-present and constantly evolving threat. Companies need to protect themselves by assessing their vulnerabilities, putting effective defences in place, and responding quickly and appropriately if they discover they have been attacked.

Even though the war may be never-ending, companies that approach the risk head on stand the best chance of coming out on top in each and every battle.

# Respondents' experience with fraud



**286**

Respondents in Thailand



**33%**

Experienced fraud



**44%**

Experienced between two and five cases



**44%**

Respondents were from manufacturing and automotive industries

One-third (33%) of Thai companies that responded to PwC's Thailand Economic Crime and Fraud Survey 2020 said they had been affected by fraud, corruption and other economic crimes during the last two years.

This is much lower than the 47% of respondents who reported being attacked globally, and big drop from the 48% of Thai companies who reported being victims in our 2018 survey.

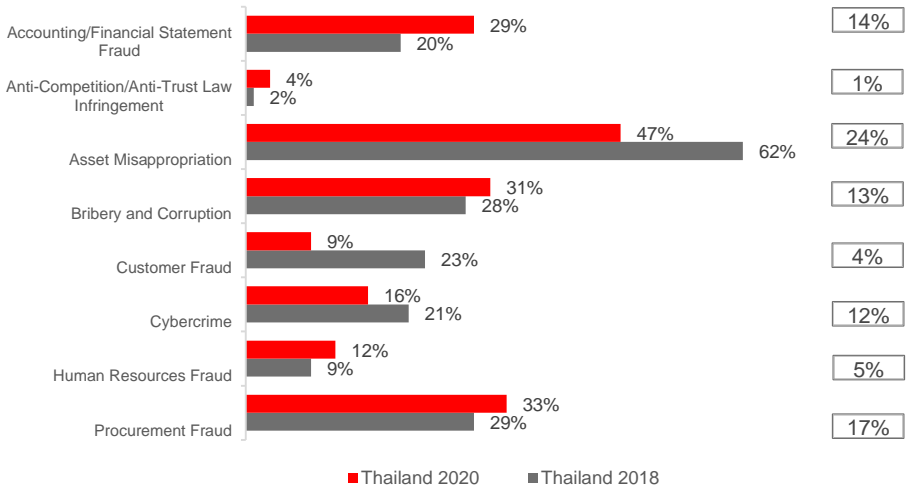
Because a lot of economic crime goes undetected, we believe this response tells us more about companies' preparedness to detect and respond to crime than it does about how much crime is actually occurring.

When reported incidences are higher, as they were in 2018, this indicates companies are investing more in the fraud detection programmes, specialized staff and technology needed to detect crime. And when reported incidences fall, like they did this year, this could mean that fraudsters are winning the war, evolving their methods and using new technologies to breach defenses undetected.

Of the Thai companies that reported being affected, around one-fifth (22%) reported a single incident and 44% reported between two and five attacks. Almost one in ten (9%) were hit more than ten times.

# Type of crime experienced and most disruptive crime

Stated most disruptive economic crime 2020



Asset misappropriation was the most common issue for the majority of respondents with 47% of affected companies reporting at least one incident. This type of crime was also the most disruptive for the highest proportion of respondents, with almost a quarter (24%) saying asset theft had had the biggest impact on their company. This result is possibly a reflection of the fact that almost half of respondents were in the manufacturing and automotive industries, which are typically more exposed to this crime.

The 47% incidence of asset misappropriation is markedly lower than the 62% in our 2018 survey. Our experience suggests this could be because fraud schemes involving theft of assets are evolving and becoming more complicated and difficult to detect, with internal staff colluding with suppliers or vendors to hide their tracks under multiple layers of fraud.

We believe these increasingly complex fraud schemes are evolving in response to companies deploying stronger controls and detection measures against theft, pitting companies and fraudsters against each other in a never-ending war of attrition.

Procurement fraud is also an ongoing battle, with the proportion of companies reporting at least one incident increasing from 29% in 2018 to 33% in this survey, making it the second most common type of crime.

Our experience shows that most organisations view procurement as a high-risk area and have robust programmes in place to prevent and detect fraud, which perhaps is why the incidence has remained relatively stable.

Bribery and corruption also remained relatively stable, affecting 31% of respondents, up from 28% in 2018. Almost one-in-five (18%) respondents admitted being asked for a bribe, and the same proportion said they believe that they lost an opportunity to a competitor who paid a bribe.

However, globally, the proportion that reported being affected by bribery and corruption (30%) was very similar to the proportion (29%) that reported being asked to pay a bribe or that said they lost an opportunity as a result of a competitor paying a bribe (30%).

It is difficult to account for the difference from survey results alone, but it raises the possibility that companies in Thailand are under-reporting requests for bribes or that they need to put better measures in place for employees and managers to report being approached for a bribe.

The increase in reports of this type of fraud may be in part due to increased detection as companies have implemented or strengthened controls, introduced more robust compliance programmes, and increased the frequency of risk assessments. Our work with clients indicates that they are working hard to fight this type of fraud. The increasing coverage of high-profile financial fraud cases in the Thai media indicates that this effort is not limited to just our clients.

Typical accounting and financial statement fraud schemes that we have investigated include accounting staff inflating revenues or delaying the recognition of expenses in order to hide poor performance and/or meet short-term targets set by stakeholders, and books being altered to cover up other crimes like asset misappropriation. The impact can be substantial, with 14% of respondents saying a crime of this type had the most disruptive impact on their business, behind only asset misappropriation (24%) and procurement fraud (17%).

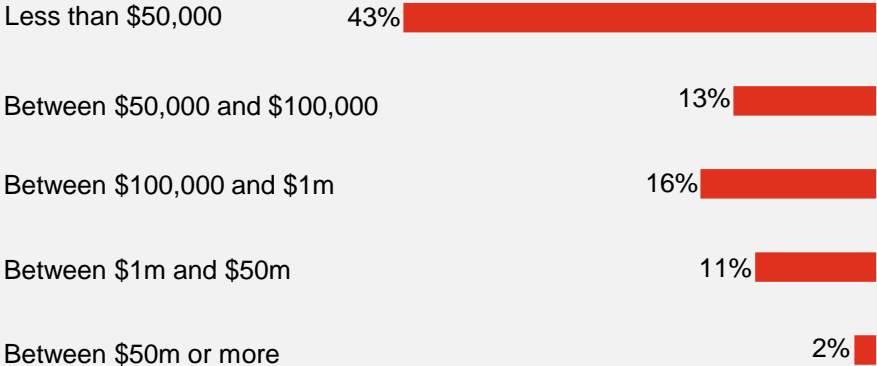
18%

18% of Thai respondents said they'd been asked for a bribe.

18% also said that they believe they lost an opportunity to a competitor who paid a bribe.

# Calculating the impact

## Direct financial loss from an alleged fraud incident in the last two years




The most obvious impact when we think of fraud is financial. How much money did the organisation lose as a direct result of the crime? In most cases, the loss is relatively minor, which could explain why so much financial crime goes undetected.

Almost half of all Thai respondents (43%) reported direct losses of less than USD 50,000 from an individual fraud incident, and another 13% lost up to USD 100,000. A further 16% lost as much as USD 1 million, while 11% of criminal attacks resulted in direct losses of more than USD 1 million. A small number (2%) led to substantial losses between USD 50 million and USD 100 million. 41% of companies also had to pay fines or penalties as a result of these incidents.

Not all costs are so easily calculated. Other typical impacts from economic crime might even outweigh these direct financial losses. For instance, the organisation may suffer brand damage and loss of market position that can take years to recover from, and they might also lose significant future business opportunities as a result. The scale of the impact is often a direct result of how effectively the organisation responds, and how quickly.







## Employee morale can also take a significant hit.

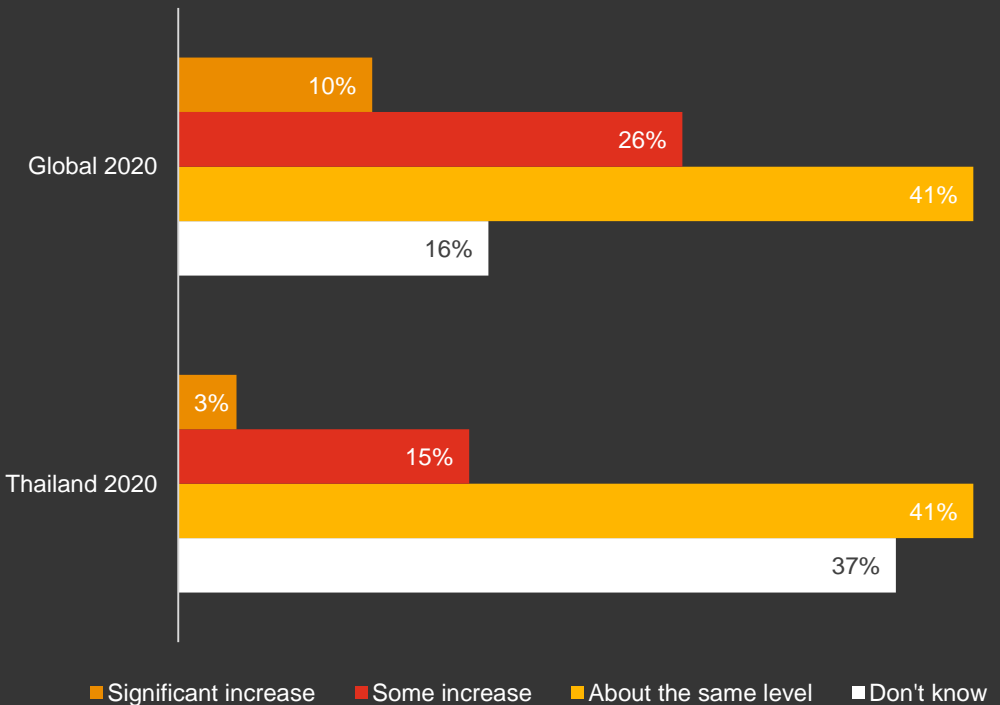
Respondents were asked about the impact of economic crime on employee morale and reported a range of negative emotions including distrust, resentment, worry, anxiety and anger. Our experience working with companies when a fraud scheme is uncovered bears this out; there is a natural tendency for management to wonder who else might have been involved, causing them to distrust all staff. Staff may in return lose confidence in management and the organisation's controls. If not handled well, this can quickly spiral and lead to an uncertain workplace by anger and anxiety.

These negative effects can be managed and turned around. Some 20% of organisations that responded to a fraud incident said their people felt resilient in the aftermath, showing how organisations that act appropriately and at pace can improve morale even as they tighten defences against the next attack. We will look more closely at how companies respond to fraud in a later section.

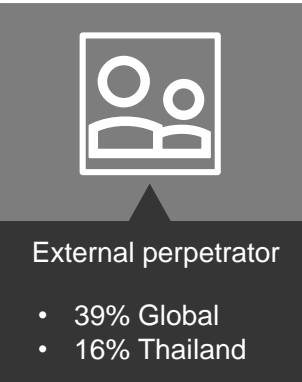
The response to fraud is critical, but doesn't need to be expensive. More than half of Thai respondents said they spent money to respond to fraud and repair the damage but this was typically less than USD 50,000. Only a few companies said they spent USD 1 million or more on response and remediation.

Going forward, the majority of respondents (41%) said they plan to maintain their spending on combating fraud, corruption and other economic crime at about the same level over the next 24 months, and only 18% planned to invest more or significantly more funds. Thai respondents are significantly more complacent in this regard than their global peers, 36% of whom plan to spend more or significantly more defending themselves from economic crime in the immediate future.

### Future spending on combatting fraud in organisations



# Who is committing fraud, and how is it being detected?



Fraud not only comes in multiple shapes and sizes, it can also hit from many directions. In Thailand, 59% of fraud was perpetrated by insiders and a further 18% resulted from collusion between someone on the inside and an external actor, such as a customer, vendor or hacker. Just 16% of incidences were caused by an external party acting alone.

This is a marked contrast to global results, where the perpetrators of fraud were more evenly split between inside parties (37%) and external parties (39%), while collusion accounted for a further 20%.

Top perpetrators
46% Operational staff
35% Middle management
17% Senior management

Looking at internal crime, the majority of internal fraud cases in Thailand were perpetrated by operations staff (46%), with middle management committing 35% and senior management 17%. Globally, operations staff were only responsible for 31% of incidences, with middle management committing 34% of the crimes and senior management 26%.



It is easy to see how companies are more vulnerable to fraud if insiders are complicit in the crime. This is particularly important in Thailand, where our work with companies shows the persistence of a workplace culture in which some managers and employees feel it is their right to skim something off the top, often justifying it on the grounds that ‘everyone is doing it’ and that it is a victimless crime that no one will notice.

Many companies that we work with are putting a lot of effort into instilling a zero tolerance for crime culture in the workplace, and this is mirrored by anti-corruption efforts led by the government and being adopted throughout the business community. Responses from organisations about how they found out they had been robbed or defrauded shows that these efforts in changing workplace culture might be paying off.

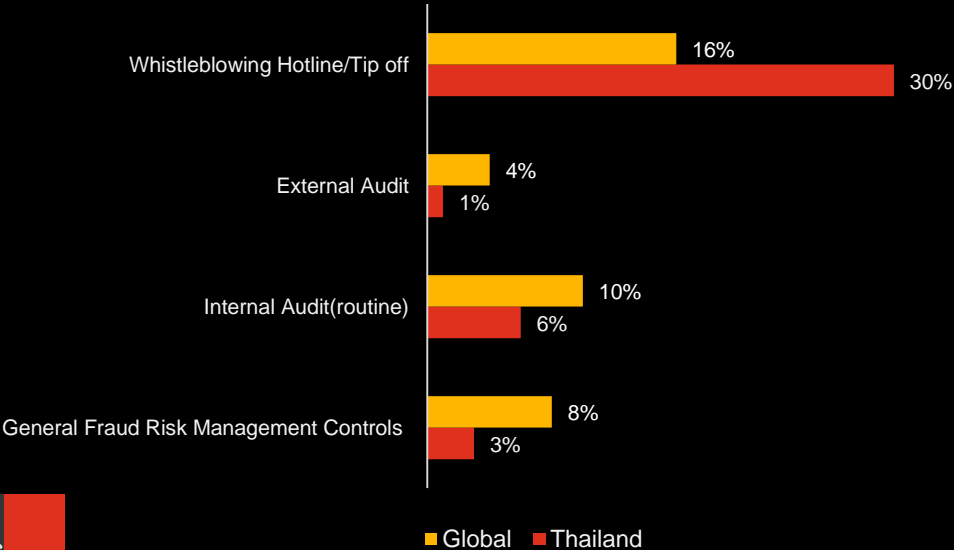
Almost one-third (30%) of crimes were discovered by someone alerting the company, either by an informal tip-off (20%) or through a formal whistleblowing hotline (10%). Globally, just 16% of incidents came to light through these means. A key factor in the effectiveness of a whistleblowing programme is trust. To ensure the hotline gets future tip-offs, a robust reporting and investigation process in which the whistleblower is protected is critical.

Investment in whistleblowing programmes should continue, but other detection channels for crime should not be neglected. Unfortunately, Thai companies are trailing their global peers in many of these detection areas. For example, internal audit detected just 6% of crimes in Thailand compared to 10% globally, external audit detected 1% versus 4% globally, and general fraud risk management controls accounted for just 3% of cases compared to 8% around the world.



The figures for internal audit are particularly alarming. In 2018, this function detected 18% of all fraud cases, and the drop to 6% this year suggests that companies have not been updating their risk profiles to keep up with constantly evolving fraud schemes.

### How fraud incidents are initially detected



# How to win the war, even if you lose some battles



The nature of fraud is changing as businesses increasingly digitise operations and connect online with their vendors, suppliers, partners and customers. In line with this, 29% of Thai respondents strongly agreed that they implemented or upgraded technology over the last 24 months to help them be more effective at fighting fraud and other economic crimes.

These technologies and techniques range from relatively simple tools like communications monitoring to organisation-wide strategic initiatives like governance risk and compliance (GRC) programmes, which align technology and business objectives to take a structured approach to managing risk.

The main obstacle to companies deploying technology to fight crime is cost, with:

**60%**

of Thai respondents who did not upgrade their technology citing this as a factor

**48%**

Almost half of respondents also said they did not have the digital skills and resources needed to deploy technology and handle the results

**21%**

A lack of support from the board and/or management was cited by 21% respondents as a reason for not investing in technology.



One in three said they don't see the value in using technology to fight economic crime. Very few Thai companies said they plan to use Artificial Intelligence (AI) as part of their technological defences.

The number of respondents that struggled to see how technology could help them fight crime was surprising. No single tool or technology will replace a comprehensive anti-fraud programme, so technology is no magic solution, but there is no doubt it has an important role to play if the basics are already in place.

Unfortunately, responses to this survey show that many Thai companies do not even have the basics of a fraud prevention programme in place. Only around half of all respondents have formal fraud programmes in place.

But fewer than 10% of fraud programmes follow best practice across a range of categories. For instance, just 8% of respondents have committed dedicated resources and compliance experts to their overall fraud programme and prioritised its budget.

And while almost half of the respondents perform regular risk assessments, only 7% have a crisis programme in place to help them manage unforeseeable risks. With fraudsters constantly evolving their methods of attack, it is these unforeseeable risks that can pose the biggest threat and have the largest impact.

As companies increasingly outsource non-core competencies to contain costs, they also expose themselves to more risk of external fraud. Yet 30% of respondents said they don't have a third-party due diligence or monitoring programme in place to protect them, and another 29% only assess this risk informally.

**The response to an incident** is critical in terms of how an organisation recovers and prevents issues from reoccurring, but:

- only 59% of respondents have documented investigation and discipline processes in place.
- only 55% of respondents said they conducted an investigation after discovering an incident.
- just 12% have a formal process in place to track the outcomes of investigations so they can identify trends and make the changes necessary to shut down their vulnerabilities.

**The most common remediation** was to discipline or terminate the employees involved, with 63% of incidents resulting in the company taking this action. This is an essential response for maintaining the integrity of compliance programmes and creating a culture where internal crime is not tolerated. These compliance programmes typically received a boost following incidents, with 47% of respondents strengthening internal controls and 43% enhancing their policies and procedures in response to a fraud incident.

**The payoff for responding can be significant.**

More than half (57%) of the organisations that took remedial action in response to an incidence of fraud reported that they believe that their organisation is now in a better place in terms of its operating effectiveness, workplace morale and defences against future incidents, with just 9% reporting being in a worse place.

As many as 68% said that they streamlined and improved operations as a result of their experience with crime, 40% reported fewer repeat incidents, and 32% improved employee morale through their response.





# Contact us today

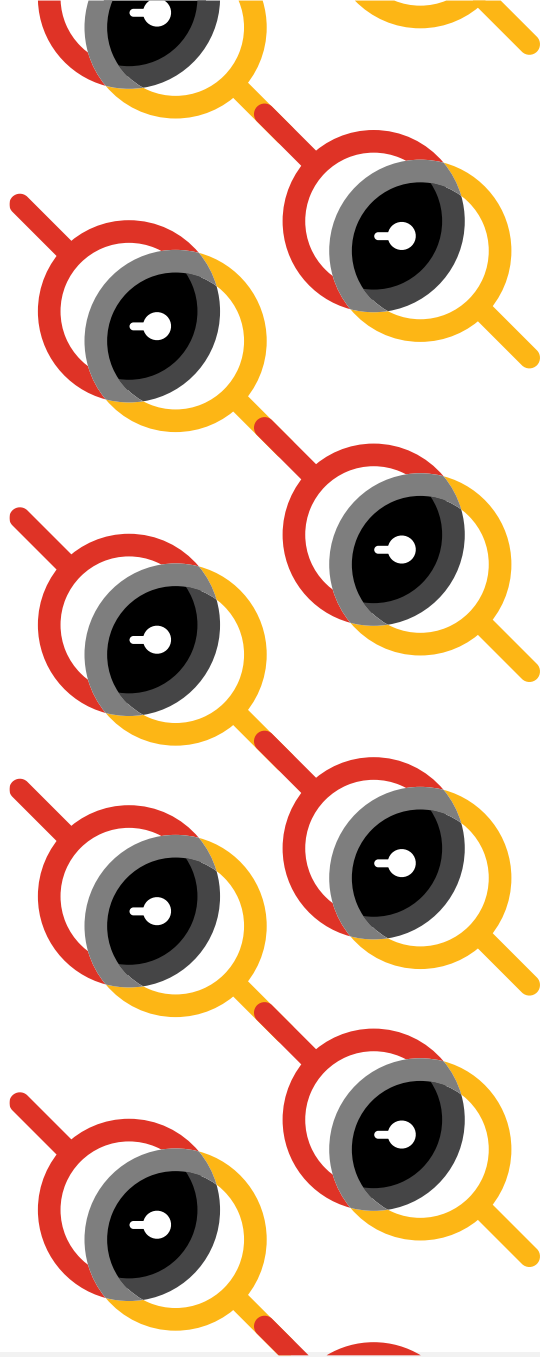
## **Shin Honma**

Partner

Forensic Services, PwC Thailand

Tel: +66 (0) 2844 1000

Email: [shin.h.honma@pwc.com](mailto:shin.h.honma@pwc.com)



© 2020 PwC. All rights reserved. PwC refers to the Thailand member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details.