FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TATAI HOKOHOKO - NEW ZEALAND

January 2021

Market Operator Obligations Targeted Review – NZX

Findings from the FMA's targeted review of whether NZX is meeting its licensed market operator obligations

www.fma.govt.nz

AUCKLAND OFFICE | Level 5, Ernst & Young Building | 2 Takutai Square, Britomart | PO Box 106 672 | Auckland 1143
WELLINGTON OFFICE | Level 2 | 1 Grey Street | PO Box 1179 | Wellington 6140

Contents

Executive summary

About this review

As a licensed market operator, NZX is required to meet certain general obligations imposed under section 314 of the Financial Markets Conduct Act 2013 (FMC Act), as set out in Appendix A.

One of those obligations requires NZX to have sufficient technological resources to operate its licensed markets properly. This includes ensuring, to the extent reasonably practicable, the availability, security, capacity and maintenance of its trading platforms, settlement systems, internal market monitoring systems and other related systems.

As a licensed market operator, NZX is also required to:

- have adequate arrangements for:
    - notifying disclosures made to it under a disclosure obligation; and
    - continuing to make those available; and
- to the extent reasonably practicable, do all things necessary to ensure that its licensed markets are fair, orderly and transparent.

In 2020, NZX suffered two significant technology incidents, both of which caused disruption and halted market activity, put investor confidence at risk, and negatively impacted Participants and the broader market ecosystem. Those failures relate to:

- volume-related system issues and a market outage experienced in March and April 2020
- distributed denial of service (DDoS) attacks in August 2020.

Later in August 2020, NZX also announced that its Trading System was unable to trade debt securities at zero or negative yields as it prepared for the prospect of negative interest rates on New Zealand (or other) debt securities.

Following the volume-related issues, we launched a review to assess whether NZX is meeting its obligation to have sufficient technological resources. The scope of the review expanded to include the subsequent issues. In carrying out our review, we also considered whether any failure to have sufficient technological resources has impacted NZX's ability to meet its other general obligations.

In FMA's view, NZX, as New Zealand's only regulated financial product market, is systemically important to the country's economy, and compliance with its general obligations should be assessed through that lens. A failure by NZX to operate efficiently would be damaging to confidence in our capital markets and could potentially dissuade Issuers and investors (both domestic and foreign) from participating.

In carrying out our review, we have been mindful of the critical role NZX plays in the New Zealand economy when measuring NZX's performance against its market operator obligations. In particular, we note that the effective operation of New Zealand's listed markets is dependent on a highly integrated ecosystem, with each participant in that ecosystem performing an important role. As the entity at the centre of that ecosystem, with the power to set rules and methods for connecting to its markets, NZX has responsibility, to the extent that it is reasonably practicable, to do all things necessary to ensure that each of its markets is fair, orderly and transparent. Given its central role, it is important for market confidence that NZX is, and is seen to be, able to operate through a crisis.

We further note that technology is central to the effective operation of our capital markets. It is the conduit through which participants in the ecosystem are connected to each other. NZX provides critical technology for trading, and clearing and settlement, which ensures the listed market can fulfil its function of providing liquidity.

We do acknowledge that as a relatively small stock exchange, the NZX's resources are not as deep as some other organisations. Like many other stock exchanges, there will always be a need to balance the desire to provide a return to shareholders with the need to meet minimum standards of operability and resilience.

As a more general comment in relation to the DDoS attacks, the threat from cyber-attacks is growing rapidly. Attacks are becoming more prevalent and more difficult to defend against. All entities, private and public, face this threat and need to evolve rapidly to counteract it. The pace of change is such that standing still or planning patiently for the future exposes organisations and the information they hold. For entities providing critical infrastructure the impact of attacks on their customers, suppliers or markets can be significant. This is a major challenge for all of us and has rapidly risen to the top of many organisations' risk identification and crisis planning.

In the finance sector, both the Reserve Bank of New Zealand (RBNZ) and the FMA have pointed their regulated populations to these threats and the focus and commitment needed in response. Both regulators will continue to work with their licensed entities to support their work in this area.

Key findings, NZX's acknowledgement, and next steps

We have assessed that NZX failed to meet its market operator obligations by not having sufficient technological resources. Consequently, for some periods this meant that NZX:

- did not have adequate capacity in its platform to enable and support trading at the volumes experienced in March and April 2020. As a result, the FMA has concluded that NZX was not doing, to the extent reasonably practicable, all things necessary to ensure a fair, orderly and transparent market; and
- did not have adequate arrangements for notifying disclosures made to it from Listed Issuers, and for continuing to make those disclosures available.

Our key findings were:

- When considered in the context of its market operator obligations and noting the systemic importance of the infrastructure it provides, NZX did not have adequate technology capability across its people, processes and platform to ensure compliance with those obligations. The performance of its systems therefore did not meet regulatory requirements or expectations for fair, orderly and transparent markets in those respects. In our view, a trading market that is not operating is not performing in a way that provides fair, orderly and transparent markets for its users – whether that be issuers or investors.
- Fundamental tools and practices were either lacking, insufficiently robust or not fully utilised, which impacted NZX's ability to ensure a high quality of system health and resilience in the respects identified.
- Crisis management planning and procedures were basic and did not address known points that could cause disruption in the event of failure. While the exact nature and extent of both the volume-related issues and DDoS attacks could not have been predicted with any certainty, significant volume increases and DDoS attacks were nonetheless well-known risks that NZX had not adequately prepared for. For the DDoS attacks in particular, adequate crisis planning would have minimised disruption to the market. Many other exchanges worldwide have experienced significant volume increases and DDoS attacks but we have not seen any that were disrupted as often or for such a long period.
- Cultural issues contributed to NZX's failure to meet its general obligations, with NZX needing to be more outwardly focused and better understand and manage its interdependencies with the wider NZX markets ecosystem.

We wish to acknowledge that while NZX did not accept all of our key findings, it was prepared to accept quite a number of them as part of its engagement with us, including:

- accepting the importance of the infrastructure that it provides
- accepting that in certain respects NZX breached its market operator obligations in relation to its technology resources

- accepting that improvements can be made (for example, to crisis management planning and procedures, to NZX's IT organisational structure, and to NZX's understanding of, and relationships with, the broader market ecosystem) and committing to deliver on these improvements.

We also acknowledge that NZX has taken significant steps to improve its systems and processes. However, in order to meet its obligations, we consider NZX still needs to:

- implement formal crisis management planning and procedures, and share these, where necessary, with stakeholders who form a critical part of crisis management resolution
- bolster its IT organisational structure to ensure NZX keeps pace with emerging cybersecurity threats and best practice
- take steps to improve its understanding of, and relationships with, the broader market ecosystem.

We are pleased that in its submissions to us, NZX undertook to ensure matters are addressed to our satisfaction.

The findings in this report will form the basis of a formal action plan between the FMA and NZX. We will monitor progress against that plan and publicly report on progress. We expect this plan to be in the form of a well-disciplined, time-bound change programme, which is suitably funded, specifically addresses the identified technology capability issues, is incrementally achievable, and will be delivered in a way that is visible to all stakeholders.

We have met with the NZX Board and acknowledge their assurances that they take responsibility for driving the required capability and change, in particular by demonstrating willingness to prioritise stabilisation and resilience, and making the investment required to progress these priorities quickly.

Targeted review and continuing oversight

Background and approach

As a licensed market operator, NZX is required to meet certain general obligations imposed under section 314 of the FMC Act, as set out in Appendix A.

Under section 338 of the FMC Act, the FMA may, at any time, carry out a review of how well NZX is meeting any or all of its market obligations. Where we have assessed that NZX is not meeting any or all of its obligations under section 340 of the FMC Act, we can require NZX to submit an action plan, which details the steps that will be taken to remedy any failings.

In March and April 2020, NZX experienced volume-related system issues, which impacted the fair, orderly and transparent operation of its markets. This prompted us to commence a review to understand the nature and cause of those issues, assess the appropriateness of NZX's response, and consider NZX's governance and strategic management of technology more generally. Given technology is a specialist area, we engaged specialist expertise to assist with our review.

During the course of our review, NZX also:

- experienced repeated market outages as a result of DDoS attacks in August 2020
- announced in August 2020 that its trading system was unable to trade debt securities at zero or negative yields.

These issues were also considered as part of our section 338 review.

Scope of the review

- We reviewed extensive information provided by NZX, including board papers and minutes, process and procedure documents, risk registers, and NZX's strategic roadmap.
- We reviewed findings of a review of the volume-related system issues and outages, commissioned by NZX and undertaken by EY.
- We reviewed findings of a review of the DDoS attacks, commissioned by NZX, undertaken by InPhySec.
- We interviewed:
    - relevant NZX staff and Board members
    - Participants
    - back office system vendors
    - NZX's settlement system vendor
    - NZX's technology suppliers.

We ordinarily publish our views on how well NZX is meeting its obligations as a market operator annually in June. The findings of this review are being shared in addition to that annual report, pursuant to section 339 of the FMC Act, which applies when we carry out any interim review under section 338(1).

Continuing oversight

Our oversight of NZX is performed on a risk basis, which means we focus on the areas where we consider there is evidence to indicate obligations are potentially not being met and where the impact of potential deficiencies could be

significant. In determining risk areas, we give consideration to information that is provided by NZX (including quarterly sampling of regulatory files), regular engagement with NZX, feedback from stakeholders, issues that may have arisen during the relevant period, and information provided by NZX in its annual Market Assessment Report. The information provided by NZX in its Market Assessment Report is self-certified as being materially accurate by the NZX CEO.

Our risk assessment of NZX's technology to date has largely been based on the absence of significant or prolonged market disruptions, the satisfactory resolution of individual issues, and information provided by NZX as part of its annual Market Assessment Report. The Market Assessment Report covers, amongst other things, cybersecurity and technology and systems, as well as business continuity planning.

Given the events of 2020 and the findings of our review, we intend to continue increasing our focus on NZX's technology until we have greater confidence that the capability and culture issues have been addressed.

Review areas

Volume-related technology issues

Background

In March and April 2020, NZX experienced nine volume-related technology incidents, including one trading system outage, which affected the fair, orderly and transparent operation of its markets, and negatively impacted Participants and the broader market ecosystem. With the exception of the trading system outage, which affected all Participants, the other eight incidents affected different participants to varying degrees. The incidents included:

- a market outage
- delayed messaging to and from registries for shareholder balance enquiries, which in some cases led to delays in order placement and trading
- disruptions to clearing and settlement, including delays in processing, failures in messaging, and a requirement for data to be extracted and provided manually for reconciliation purposes (which erroneously had both missing and duplicate transactions).

The incidents caused concern, frustration and additional work and cost for many Participants and vendors (although it is important to note that there were disparate outcomes for different groups of Participants and vendors). The nature and frequency of the incidents undermined confidence in the market.

Findings

We consider, at the time of the issues, NZX was failing to meet its obligation to have sufficient technological resources by not having adequate capability across its people, processes and platform in the respects identified. The market impact of the technology failures, when considered in the context of NZX's arrangements, meant that at times NZX was also failing in its obligation to do all things necessary (to the extent reasonably practicable) to ensure its licensed markets were fair, orderly and transparent.

Our review also highlighted issues with culture, as described below, which contributed to NZX's failure to operate its markets to an appropriate standard.

We note that NZX believes the volume-related issues in March and April 2020 were unforeseeable, given volumes reached six times the daily average. However, it is our view that NZX was running so close to the margins in terms of capacity that even a smaller unexpected volume spike may have resulted in similar issues. This view was shared by most of the Participants, who have informed us they were identifying issues with system lag in mid to late 2019.

Market events that cause significant spikes in trading volumes are not unusual. A combination of NZX's own developments to increase on-market liquidity and the growth of retail trading platforms should in our view have prompted more rigorous capacity planning. In addition, NZX was aware of the capacity limitations of its core back-end processing system (BaNCS), particularly as daily trading volumes had increased in the last three years. These factors combined mean that we would have expected, as did stakeholders, that NZX would have been taking concrete and planned steps, including effective contingency and crisis management planning, to mitigate any impacts that volume-related technology issues would have on its market operations.

Capability

When considered in the context of its market operator obligations and noting the systemic importance of the infrastructure it provides, NZX did not have adequate technology capability across its people, processes and platform to ensure compliance with those obligations. The performance of its systems therefore did not meet regulatory requirements or expectations for fair, orderly and transparent markets in those respects. We observed the following:

- NZX was not:
    - adequately monitoring use or performance of BaNCS
    - carrying out adequate performance tuning
    - addressing inefficient system usage.

  System capacity and system updates did not appear to be keeping pace with business developments to increase on-market trading.
- BaNCS processing capability had a number of constraints. In particular, it was designed for daily maximum trading volumes that by 2019 were being approached on peak trading days. In addition, BaNCS' processing capacity was compromised by the fact that it had been designed to allow Participants to receive trade confirmation messaging. In addition, BaNCS was also used to process messages between Participants and the registries for shareholder balance enquiries. At high daily trading volumes this functionality was placing pressure on system capacity and processing ability. While NZX was aware of these issues, Participants do not consider that NZX had adequately communicated its preference for Participants to use the trading system rather than BaNCS for trade confirmation messaging, nor had NZX published recommended standards for use.
- NZX did not promptly or adequately address system constraints once alerted to issues. In particular:
    - System delays and messaging problems, raised by Participants in 2019, were addressed on a piecemeal basis and did not fully address capacity constraints. The onus of a longer-term solution was put on Participants to change how their systems interact and rely on BaNCS – though this position does not appear to have been adequately communicated to Participants.
    - Warnings from the system vendor in late 2019 that the system was nearing capacity were not addressed with any urgency. We note it is NZX's position that this information was never communicated to them by the system vendor.
- NZX's internal IT capability was consistent with a small to medium-sized New Zealand corporate, but not of a standard expected for systemically important infrastructure. The technology was largely managed in-house, but the level of staffing was not sufficient to adequately manage mission-critical technologies, as well as provide appropriate risk management and security protection. At the time of the review, the team was mostly limited to day-to-day operations, defect management and making small incremental improvements.
- Fundamental tools and practices were either lacking, insufficiently robust or not fully utilised, and that impacted NZX's ability to ensure a high quality of system health and resilience in the respects identified. This included a lack of:
    - continuous version management and upgrades of supported software
    - performance monitoring and alerting
    - full testing lifecycle capability
    - capacity planning/management and fail-over capability
    - robust and recoverable processing standards
    - appropriate internal staffing, knowledge sharing and contractual arrangements to access external expertise.
- NZX did not appear to have appropriate risk management planning, which should focus on known single points of failure and risk mitigation plans. There was a lack of documented standard practices, and Participants did not have a common understanding of the recovery procedures. NZX's crisis management and decision-making appeared ad-hoc.
- NZX's technology-related strategic direction is sound and achievable, but requires a continued focus on performance and sustainability, and a commitment by the Board to invest appropriately. At present the blockers to achieving its technology strategy are:

- a steady series of business change initiatives that distract from work required to stabilise the current position
- a lack of critical IT roles needed to address 'key person' risk, improve operating standards and implement change management disciplines
- no dedicated relationship manager(s) for key stakeholders, which amplifies issues related to a lack of commercial service-level arrangements with Participants and failure to respond to participant concerns.

Culture

We consider there are internal cultural factors that have contributed to NZX's failure to have adequate technological resources, which in turn has at times resulted in an inability to operate a fair, orderly and transparent market.

NZX, as a licensed market operator, is part of a broader ecosystem, with each participant in that ecosystem performing an important role in the provision of fair, orderly and transparent capital markets more generally. NZX sits at the centre, being the participant with the most information and control, and having a legislated obligation to, to the extent reasonably practicable, maintain fair, orderly and transparent markets. We consider a failure to fully understand and manage its interdependencies with the wider ecosystem has been detrimental to NZX's strategic planning, issue identification, and appropriate crisis response and resolution.

The capability issues noted above, and NZX's responses to issues and incidents brought to its attention have, over time, eroded the trust and confidence of Participants. After extensively interviewing both NZX staff and Participants, we observed the following perceptions from stakeholders of NZX's stakeholder relationships:

- NZX does not take responsibility for known systemic and industry-wide issues, nor does it act quickly to remediate concerns raised.
- NZX rarely accepts fault, and is not upfront and open when things go wrong.
- NZX has a lack of awareness of (and lack of concern about) downstream operational impacts and resulting cost implications for Participants due to system failures.

We consider the lack of dedicated relationship management and service-level agreements needs to be resolved to begin the journey of repairing relationships and restoring trust.

The detailed and critical feedback received from Participants is a major concern and needs to be considered and addressed by the NZX Board and Executive. A situation where Participants feel NZX is not responsive to their concerns creates the real risk of distrustful and tense relationships at a time when growing trust and confidence in our capital markets is crucial.

Actions subsequently taken by NZX

In response to the volume-related technology issues experienced in March and April 2020, NZX has taken steps to improve its technology position. NZX has:

- Established a board technology committee. This committee's role is to provide governance over the wider NZX technology project, which is designed to respond to the issues experienced in March and April 2020.
- Established an internal management group to find immediate and medium-term resolutions for the technology challenges experienced. This response includes:
  - an upgrade of hardware used by BaNCS to process trade messages
  - working with the BaNCS service provider to identify and implement improvements to system resilience, and to utilise the application's multi-threading architecture to remove bottlenecks and lift volume throughput
  - introducing performance testing to ensure software improvements and infrastructure capacity uplift can meet significantly higher volumes

- beginning work with Participants to reduce reliance on BaNCS for trade confirmation messaging (noting that there are significant resulting technical changes relating to redesign, development and testing that will need to be made to Participants' applications)
- separating shareholder balance enquiry messaging from the settlement system.

NZX also appointed EY to complete an external review and, following that review, has agreed to a number of action points based on EY's recommendations, including the following:

- Convening an industry-wide forum that will act as an escalation point for industry feedback, concerns and prioritised resolutions. NZX is to share and collaborate on its IT roadmap and business initiatives.
- Considering establishing service-level agreements and/or setting accreditation requirements for Participants and their service providers.
- Improving its end-to-end technology testing discipline, with a focus on comprehensive performance and regression testing.
- Establishing a comprehensive software and database management practice, which defines and documents all critical system components, and ensures appropriate and timely updates and maintenance.
- Improving processes for capacity management and planning.
- Completing further work to evolve NZX's monitoring suite across all technologies, including network and connectivity tests to Participants.
- Ensuring there is appropriate spread of specialist skills and knowledge of BaNCS across the NZX technology team, to provide depth of capability within NZX.

Expectations and next steps

The EY recommendations outlined above align with the findings of our review, and should form the basis of NZX's action plan to be provided to us under section 440 of the FMC Act.

EY also recommended that NZX consider taking an architecture and business requirement-led approach to assessing the suitability and sustainability of BaNCS, to not only meet current clearing and settlement needs and requirements of all stakeholders, but to also meet future needs and wider market change that is probable or possible.

NZX has indicated it will undertake a full Request for Proposal at what it considers to be an appropriate time, for the next evolution of technology to support clearing and settlement. In our view, NZX should therefore continue to urgently focus on its current deployment of BaNCS and, working with the vendor, identify and repair poor architecture, out-of-date software, known defects and performance issues.

Additionally, we expect that NZX will:

- significantly improve its crisis management plans and procedures. These plans should:
  - identify potential points of failure in critical services and infrastructure
  - detail the risk mitigation strategies that are in place for critical services and infrastructure
  - detail potential back-up solutions for when there is a failure in any critical service or infrastructure, or for when any risk mitigation strategy turns out to be ineffective. These solutions should take into account a variety of hypotheticals, be multi-layered, and include both technology-based and non-technology-based solutions
  - be shared, where necessary, with stakeholders who form a critical part of crisis management resolution.
- establish an appropriate programme board and reporting oversight to ensure all stakeholders have confidence in the planned improvements and platform sustainability.

We expect the NZX Board to take responsibility for driving the required capability and cultural change, in particular by demonstrating willingness to prioritise stabilisation and resilience, and making the investment required to urgently progress these priorities.

We encourage Participants to fully engage with NZX throughout this process of change to ensure the best outcomes are reached for the wider eco-system.

Cybersecurity-related market outage

Background

In late August 2020, NZX (via Spark network connectivity) experienced multiple volumetric DDoS attacks. These were sophisticated, sustained and of very significant size.

The DDoS attacks caused outages of NZX.com and the Markets Announcement Platform (MAP), and disrupted other internet-based connectivity to NZX back-end systems. The DDoS attacks did not result in any security breaches of NZX's trading or clearing systems or other infrastructure. However, the inability of issuers and investors to use NZX.com and MAP to release and receive market announcements caused NZX to halt the market. NZX remained in trading halt for approximately four days, with only intermittent periods of availability.

On 31 August 2020, NZX put in place contingency arrangements for the communication of market announcements, allowing trading to resume.

Findings

NZX's lack of technology capability (i.e. level of resourcing, inadequate processes, and poor risk and crisis management) meant it failed to meet its obligation to have sufficient technological resources. These deficiencies resulted in NZX also failing in its obligations to do all things necessary (to the extent reasonably practicable) to ensure that its licensed markets are fair, orderly and transparent, and to have adequate arrangements for notifying disclosures made to it from Listed Issuers, and for continuing to make those disclosures available. We view a situation where the market is unable to operate during its standard timeframes as a breach of that obligation. NZX has questioned that view on the basis that while the market is shut it is neither unfair, disorderly nor lacking in transparency.

Our review of the cybersecurity issues revealed similar themes to those noted above regarding the volume-related system issues and outage.

NZX considers that it could not have foreseen, and therefore been prepared for, a DDoS attack of the magnitude that occurred and that the magnitude of the attacks was unprecedented in New Zealand. We consider a DDoS attack was foreseeable and that an attack of sufficient magnitude to take down the servers was at least possible and should have been planned for. In our view, given its critical importance to the continued operation of the market, NZX should have planned for the possibility that its website and Market Announcement Platform would be unavailable, whatever the cause of that unavailability.

DDoS attacks are not new, and, globally, have been increasing in intensity over time, as indicated by the CERT NZ alert published on 1 November 2019. Further, as stated above, we consider NZX should have had crisis management planning for a website outage (whether or not that outage was caused by a DDoS attack). A website outage can occur in a variety of situations, and given the criticality of NZX's website to the operation of its markets, an outage should have been a risk that was identified and managed.

Specifically we noted the following:

Capability

- Crisis management planning appears to have been rudimentary and entirely reliant on technology alternatives which may also be unavailable in the course of a DDoS attack or other cybersecurity breach. The contingency arrangements that were ultimately put in place after the DDoS attacks were available from the outset, so if NZX had had adequate crisis management planning for a website outage the arrangements ultimately adopted could have avoided the market being halted for an extended period of time.
- NZX has a small in-house IT team that, among a wide range of technology responsibilities, is responsible for managing IT security. The IT organisational structure is missing certain key roles that would bring the level of focus to IT security that is expected from a technology-dependent organisation.
- NZX had inadequate IT security processes, having only introduced IT security disciplines to the team in 2019 after a decade of inadequate standards and lack of industry good practice. NZX self-rated its IT security profile at a basic maturity level, indicating many best practices had not been adopted. This meant that, while the gap had clearly been identified, significant work was required to improve standards. As a result, from an IT security perspective, there was suboptimal robustness of applications, poor network design and unprotected infrastructure. We acknowledge that during and after the attacks, NZX improved and extended its commercial arrangements with external IT security providers.
- While NZX did maintain an IT risk register, there was a significant number of risks in the register that remained 'in progress'. This meant that progress on managing and mitigating IT risks was slow. A DDoS attack on NZX.com was included in the risk register, but its overall risk severity score (determined by likelihood and consequences) was ranked lower than many other residual risk items. The ranking itself did not seem appropriate given the escalating frequency and severity of DDoS attacks globally (including attacks on international peer exchanges), and dependency on NZX.com. It also indicates NZX had limited capacity to address a large workload of required technological repairs.
- It is hard to fully judge the scale of the attacks against NZX compared to similar attacks on New Zealand financial institutions, corporates, and government entities (some of which were contemporaneous). However, to our knowledge, both in New Zealand and globally, critical financial infrastructure such as banks, payment systems and exchanges have managed to avoid the repeated disruption that occurred to NZX.

NZX stance

Our interactions with NZX management over the DDoS attacks further illustrate NZX's lack of willingness to accept fault, as noted in respect of the volume-related issues. NZX maintains that the DDoS attacks were unprecedented, and therefore could not have been planned for. This ignores the fact that NZX was unable to defend the initial attacks which were at lower levels. Further, while we acknowledge that the DDoS attacks were at times very significant, the need to halt the market could have been avoided if NZX had had adequate crisis management planning and procedures in place.

Actions subsequently taken by NZX

To address the issues noted above, NZX has:

- engaged an expert to review its cybersecurity positioning
- created a cloud-based alternative/fail-over site for the Market Announcement Platform
- engaged Akami to provide DDoS defence (both front- and back-end infrastructure)
- improved network-managed services and infrastructure
- completed IT security reviews
- improved website capability and capacity
- added protection for legacy external connections
- improved security monitoring tools.

Expectations and next steps

The actions subsequently taken by NZX go some way to addressing the issues and mitigating potential risks. However, there are some critical gaps remaining. As noted above, NZX must establish formal crisis management plans and procedures. It is not appropriate to try implementing business process alternatives during a disruption.

We also recommend the following:

- Bolstering the IT organisational structure to include a Head of IT Security and a Head of Architecture. These roles must bring industry knowledge, experience and know-how, and be connected to or draw upon external perspectives. They are key to ensuring that NZX keeps pace with ongoing cyber-threats and best-practice defence.
- Appointing a Chief Risk Officer to bring focus to the identification and management of risks, including IT security risks.
- Revisiting the security measures that were put in place during the course of the incident, to determine whether IT security remains adequate on an ongoing basis, and whether the changes in security have potentially opened up any other vulnerabilities that need to be addressed.

Trading system unable to trade at zero or negative yields

Background

The global economic situation has caused many jurisdictions to head towards negative interest rates. Several major jurisdictions had moved to negative interest rates prior to COVID-19. Both the FMA and RBNZ had encouraged the financial services sector to ensure they were adequately prepared for such an eventuality.

On 25 August 2020, NZX notified us that its Trading System would not support yield pricing for the placement of orders entered at zero or negative yields for debt securities quoted on the NZDX.

NZX decided the upgrade to allow this functionality would be done as part of an ongoing Trading System upgrade project, which is scheduled to be delivered at the end of March 2021.

As an interim solution, NZX advised the FMA and Participants that any debt securities that moved to a zero or negative yields would need to be retroactively converted to trade on price (rather than yield). Trading debt securities by price is an existing functionality within the Trading System, albeit one that is not often used, given that debt securities are most commonly traded on yield in New Zealand.

We had some initial concerns about whether NZX's interim solution was the most appropriate for maintaining a fair, orderly and transparent market, and whether all regulatory considerations had been taken into account in reaching the solution. These concerns were subsequently strengthened by complaints from Participants. We sought clarification from NZX about its process and considerations in determining the proposed interim solution.

Findings

Following engagement with NZX, it is our view that:

- Given overseas experiences, the market environment, and its systemic importance as the only licensed market operator, NZX was late in considering whether the Trading System would be able to support trading at zero or negative yields, having only considered the issue in late May/June 2020. Earlier consideration may have meant a technology solution could have been implemented more promptly. Other countries have experienced negative interest rates over quite a long period, and the prospect of negative rates was not new.
- In determining its interim solution, NZX did not give sufficient consideration to impacts on the wider market ecosystem. While NZX consulted some Listed Issuers and other tangential stakeholders, it did not, prior to announcing its proposed solution, consult with Participants to understand whether there were any downstream

technological difficulties associated with the change or whether the change would impact reporting for investors. This is concerning. The largest impact of the interim solution would have be borne by Participants, despite the responsibility for having adequate technology resting with NZX.

- Failure to properly consider and consult on impacts across the broader ecosystem is further indicative of the internal cultural issues described above. While the interim solution was intended to ensure the continuation of a fair, orderly and transparent market, NZX did not test the workability or effectiveness of that solution with key stakeholders and, when questioned on this, expressed the view that they were not responsible for ensuring workability further down the chain.

Actions subsequently taken by NZX

Following engagement with us, NZX has engaged with Participants, addressed the majority of their feedback, and reached a more workable interim solution.

Expectations and next steps

We recommend NZX take steps to improve its understanding of, and relationships with, the broader market ecosystem.

Further, where a technology solution is available to support a better regulatory outcome, we expect that solution to be prioritised. If the technology solution is not prioritised for some reason, that decision should be fully reasoned and supportable, including showing consideration of the broader impacts of the decision.

Appendix A: Background information

Market operator obligations

In the FMC Act, 'market operator obligations' means:

- the general obligations in respect of licensed markets (section 314):
  - to ensure, to the extent that is reasonably practicable, that each of its licensed markets is a fair, orderly and transparent market
  - to have adequate arrangements for notifying disclosures made to it from participants in its markets, and for continuing to make those disclosures available
  - to have adequate arrangements for handling conflicts between its commercial interests and the need to ensure its markets operate in a fair, orderly and transparent manner
  - to have adequate arrangements for monitoring the conduct of participants in its markets
  - to have adequate arrangements for enforcing compliance with market rules
  - to have sufficient resources (including financial, technological and human resources) to operate its licensed markets properly
- an obligation to respond to a request from the FMA to make changes to market rules (section 333)
- an obligation to give the FMA an annual self-assessment of compliance with its obligations (section 337)
- an obligation to act on the directions of the FMA or the Minister, if the operator is found to be failing to meet any of its obligations (sections 340 to 342)
- any obligation imposed as a condition of a market operator's licence.

NZX licences

NZX is licensed to operate the following markets in New Zealand:

- NZX Main Board
- NZX Debt Market
- Fonterra Shareholders' Market
- NZX Derivatives Market

Details of NZX's licences are on our website.

Our oversight of NZX

As the regulator of NZX, we review how well NZX is meeting its obligations as a licensed market operator. Our oversight is performed on a risk basis, which means we focus on the areas in which we consider there is evidence to indicate obligations may not be being met.

In determining risk areas, we give consideration to information that is provided by NZX (including quarterly sampling of regulatory files), regular engagement with NZX, feedback from stakeholders, and self-certifications made by NZX in its annual Market Assessment Report.

We have a Memorandum of Understanding with NZX, which was signed in January 2015 and sets out the principles for our engagement and cooperation. This means NZX keeps us up to date about its key initiatives and developments. We also have an agreed set of protocols for communications when we deal with normal business activities concerning both of us.

Glossary

EY	Ernst & Young, referring to the global organisation, and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity
FMC Act	Financial Markets Conduct Act 2013
Issuer or Listed Issuer	Any company that is or has been listed on any of NZX's markets
Licensed markets or NZX's markets	The financial product markets NZX is licensed to operate under the FMC Act
Market operator obligations	Obligations imposed on a licensed market operator as a condition of its licence or under sections 314, 333, 337, 340, 341 and 342 of the FMC Act
Market rules	All of the rules governing NZX's licensed markets, including Listing Rules, participant rules and NZMDT rules
NZDX	NZX Debt Market
Participant	A participant in the licensed markets who has been accredited and approved by NZX under the participant rules
Participant rules	NZX rules governing participant firms
Trading System	Nasdaq X-stream platform through which orders may be entered in relation to markets