REPRINTED FROM
Risk.net
Risk.net June 2016

Connecting the dots: how DTCC manages contagion risks

DTCC managing director and group chief risk officer Andrew Gray offers a template for managing the risk of interconnectedness

As the Lehman Brothers bankruptcy in 2008 demonstrated, the failure of one highly interconnected entity can spread rapidly across the global financial system and have a devastating impact on financial stability.

The level of financial interconnectedness cannot be overstated. Banks and other financial institutions are linked through intermediation chains that span the globe, creating an elaborate web of mutual interdependencies.

This is particularly true for financial market infrastructures (FMIs), which sit at the heart of this intricate network. FMIs provide the processing systems that enable markets to operate with unprecedented speed and efficiency. However, they can also serve as a conduit for contagion.

The impact of the failure of an FMI can spread rapidly and extensively – to the point where it can cause worldwide financial instability.

Global financial regulators have taken notice. Today, interconnectedness is one of five categories that determine which banks are systemically important. The importance of managing interconnectedness risks is also enshrined in the *Principles for financial market infrastructures*[1] (PFMIs), which are a key standard that global regulators consider essential to strengthening and preserving financial stability.

Building an interconnectedness risk management programme is a significant undertaking given the inherent complexities and lack of precedents. While the specifics will likely differ from one organisation to another, each programme shares three basic building blocks that are universally applicable: **identifying** interconnectedness risks; **prioritising** them; and **mitigating** them.

Interconnectedness risk is defined as the risk that an organisation faces as a result of its reliance on entities with which it has contractual agreements, operational arrangements and other types of functional or financial dependencies. These risks materialise whenever an interconnected entity fails to perform as expected, regardless of the underlying cause.

[1] *www.bis.org/cpmi/publ/d101.htm*

1. Identify

Identifying interconnectedness risks requires an organisation to systematically map out the ecosystem of interconnected entities with which it interacts.

The first step must be to **identify broad categories** of interconnected entities – such as investment counterparties or liquidity providers – and to create a comprehensive taxonomy that includes all the parties that directly or indirectly contribute to an organisation's business or the creation and delivery of its services.

While this may seem straightforward, it requires detailed business expertise and the input of many different departments. It is important to include guidance from product management and operational staff in addition to legal experts, given that entities can be financially interconnected even if they are not contractually obligated to each other. For instance, a paying agent's failure to make timely interest and principal payments can affect investors, even though there is no legal contract between both parties.

The second step is to **map individual entity names** to these categories. Special attention should be given to names that appear in multiple categories, as the failure of a highly interconnected entity could have a compound effect and impact several processes or services at the same time. While the broad categories of interconnected entities should be relatively static, individual entity names can change dynamically, depending on the nature of the underlying relationship.

2. Prioritise

Once an organisation has identified its interconnectedness risks, it should prioritise them, so that the most important threats are addressed first. Risks are typically assessed based on probability data and estimates of the potential severity of their impact if they materialise. While these criteria are equally valid for prioritising interconnectedness risks, firms should also consider other factors, such as the substitutability of their interconnected entities, the concentration risk they present and the extent to which they can influence or control these risks.

Assigning probabilities to interconnectedness risks may be difficult for several reasons. First, the failure of an interconnected entity to perform as expected could itself be the result of a wide range of underlying causes, ranging from a bankruptcy to an operational problem. Second, history suggests the likelihood of any of these scenarios occurring is very low, making it even harder to estimate probabilities with any degree of accuracy.

Andrew Gray is managing director and group chief risk officer of DTCC

DTCC is using a multi-pronged approach that focuses on further analysis and continued risk mitigation ... Addressing interconnectedness risks is a work in progress that will continue to evolve as our understanding of the underlying dynamics matures

The **severity of impact** of an interconnected entity's failure depends primarily on the importance of the services it provides or supports. Clearing and settlement banks, for instance, support core functions at the heart of FMIs. As such, the impact of their failure is inherently more severe than the breakdown of other interconnected entities that play a more auxiliary role.

The risk posed by interconnected entities should also reflect their **substitutability** – that is, the availability of alternative providers and the ease and speed with which their services can be put to use. Obtaining services from an alternative provider may require lengthy contractual negotiations when time is of the essence. In addition, the infrastructure required to interface with a particular service provider may be very specific, making it costly and time-consuming to switch. In addition to these technical and contractual obstacles, a lack of competition among service providers may also impede substitutability. Given the high degree of consolidation in the financial services sector in recent years, this concern should not be underestimated. Finally, when assessing the level of substitutability, it is also important to keep in mind that alternative providers may be more readily available in normal circumstances than in times of crisis, when substitutability is often most needed.

Concentration risk is another key factor, applying both within a given service as well as across services. The greater the market share of a provider for a given service, the more damage its failure can cause. However, the wide range of services provided by highly interconnected entities also creates concentration risk across services. This second dimension of concentration risk is much harder to assess and mitigate because it points directly to the essence of interconnectedness risk: the potential for the failure of a single entity to impact multiple services simultaneously and in ways that are not immediately transparent.

In addition to applying the criteria above, organisations should also analyse to what extent they can control and influence their interconnectedness risks. Service providers may operate in oligopolistic markets, which inherently limit their clients' ability to mitigate interconnectedness risk through diversification. Interconnectedness risks may reside outside of a firm's control – for instance, as a result of choices made by clients. As a general rule, organisations should focus first on mitigating those interconnectedness risks they can influence, while trying to limit the potential damage caused by threats beyond their control.

3. Mitigate

Addressing interconnectedness risks is a multi-faceted challenge that should be tailored to the specific characteristics of the risk and the unique way it manifests itself. To tackle this challenge, it may be helpful to follow a three-pronged approach: first, **review** existing rules and procedures; then, **dimension** the risks; and finally, **develop** mitigants.

a) First, carefully **review the existing rules and procedures** – if any – that relate to the failure of a particular type of interconnected entity. Unlike many other risks, the ramifications of the failure of an interconnected entity are poorly understood, simply because such failures are extremely unlikely, and sometimes unprecedented. An organisation's course of action and the potential tools it might have at its disposal may be similarly unclear. In order to develop a common understanding of relevant risks and controls, it is crucial to include operational, legal, product management and other subject matter experts in cross-functional meetings.

These meetings may reveal that specific procedures to address the failure of an

interconnected entity are vague or missing altogether. Even if procedures do exist, it is important to assess their feasibility in terms of having adequate manpower, reports and other supporting tools. This aspect is easily overlooked, as these events are typically unprecedented. Additionally, guidelines or procedures designed to address the failure of an interconnected entity must be consistent with existing contractual agreements, which reinforces the importance of including legal subject matter experts.

The end goal of this review is to reveal and remediate process gaps, and clearly document the rules and procedures that govern how an organisation should handle the failure of an interconnected entity.

b) Second, **risk should be dimensioned**. This is helpful in assessing the systemic impact of the failure of an interconnected entity, which – in turn – can inform the risk prioritisation process. It can also be used to monitor risks and provide insights into how threats evolve over time.

Finally, quantifying these risks is useful for evaluating the effectiveness of mitigating actions.

Some interconnectedness risks, such as investment counterparty risk, can be measured fairly easily. Other types of interconnectedness risks – vendor risk, for instance – are very hard to quantify precisely. Organisations should devise the most appropriate method for dimensioning each relevant type of risk, carefully weighing their overall objectives, their resource constraints and the maturity of their interconnectedness risk management programme.

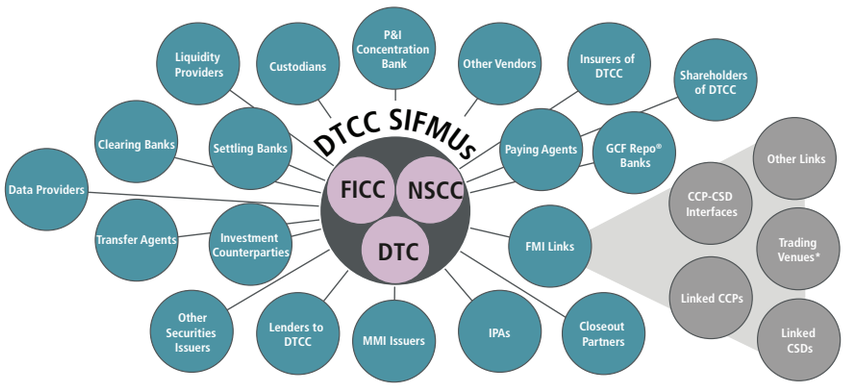
Adopting pertinent and explicit assumptions is arguably the most critical prerequisite for dimensioning risks in a meaningful way. Without a solid foundation, seemingly precise measurements can give a false and misleading sense of accuracy.

c) Once interconnectedness risks are identified and prioritised, **the final step is to mitigate them**. This is not only the most important but also the most challenging step.

Interconnectedness risks are inherently complicated and multi-dimensional. They are extremely diverse and heterogeneous and they exist in an environment that is the result of countless components that interact dynamically and often unpredictably. As such, it is impossible to be prescriptive in terms of how they should be mitigated.

That said, interconnectedness risk mitigation strategies should be built on three main pillars. First, firms should select the most robust interconnected entities and optimally diversify exposure across such entities. Second, there should be measures in place to monitor and control the performance of interconnected entities, as well as the associated risks. Third, they need to build resilience by developing mitigants aimed at minimising the impact of an interconnected entity's failure on their core functions.

DTCC interconnections



DTCC's approach

DTCC provides clearing and settlement services through its subsidiaries, three of which – the Depository Trust Company (DTC), National Securities Clearing Corporation (NSCC) and Fixed Income Clearing Corporation (FICC) – have been formally designated as systemically important financial market utilities, or Sifmus.

In 2010, DTCC created a systemic risk office – a team specifically dedicated to identifying, monitoring and containing potential systemic threats.

In 2013, our systemic risk office started a multi-year effort to identify, quantify and map the risks related to the potential failure of an interconnected entity. The overall objective of this company-wide interconnectedness risk programme was to better understand the threats to, and impact on, systemic stability that may arise from a wide range of external entities on which DTCC relies for the provision of its critical services. Integrating this programme into DTCC's risk management practices is fundamentally transforming how the company thinks about the threats it is facing in a world that is ever more connected.

DTCC first organised a series of internal meetings with subject matter experts from various departments – including product management, operations, legal, finance, and risk – to create an inventory of approximately 20 different types of interdependencies and associated risks (see figure, *DTCC interconnections*). Once this inventory was completed, we focused on settling banks, liquidity providers and investment counterparties as the initial priorities for our interconnectedness risk management programme.

After a detailed review of DTCC's rules and procedures as they relate to the failure of these types of interconnected entities, several reports were developed to dimension the associated risks. Monitoring and aggregating this information on an ongoing basis helps provide greater transparency to DTCC's management on the organisation's exposure to investment counterparties, liquidity providers and settling banks.

While our interconnectedness risk programme is still evolving, it has already led to the development and implementation of a number of appreciable mitigants, including enhancements to DTCC's liquidity programme, a significant reduction in the concentration of daily cash investments made by the treasury function, and enhancements to rules and procedures that reduce operational risks associated with the critical end-of-day settlement process.

As DTCC progresses with its interconnectedness risk programme, it is using a multi-pronged approach that focuses on further analysis and continued risk mitigation. We have also started an outreach programme to establish an ongoing dialogue with our most highly interconnected entities.

Addressing interconnectedness risks is a work in progress that will continue to evolve as our understanding of the underlying dynamics matures. As such, it represents the logical next step in the evolution of an organisation's risk management capabilities. ■