Financial Stability Institute | BIS

FSI Briefs

No 17

Safeguarding operational resilience: the macroprudential perspective

Jermy Prenio and Fernando Restoy

August 2022

FSI Briefs are written by staff members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), sometimes in cooperation with other experts. They are short notes on regulatory and supervisory subjects of topical interest and are technical in character. The views expressed in them are those of their authors and not necessarily the views of the BIS or the Basel-based standard setting bodies.

This publication is available on the BIS website (www.bis.org). To contact the BIS Media and Public Relations team, please email press@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2708-1117 (online)
ISBN 978-92-9259-593-7 (online)

Safeguarding operational resilience: the macroprudential perspective[1]

Highlights

- *Financial firms' increased reliance on technology and the additional complexity and interconnections that technology has brought to the financial ecosystem pose risks to the operational resilience not only of individual institutions but also of the financial system.*
- *Many authorities have chosen to have separate policies or guidelines related to risk management, business continuity management and third-party management to achieve operational resilience, while a few have put all these things together to come up with a holistic operational resilience policy.*
- *Among those with an operational resilience policy, the definition of important operations/services takes a macroprudential view, but setting standards of resilience for these operations/services and testing against these standards are left to individual firms.*
- *There is scope for operational resilience policies to be explicit about the need to perform system-level assessment, monitoring and testing.*
- *Given their implications for system-level operational resilience, there may be an argument for subjecting critical technology providers to an oversight framework, which, when relevant, should be coordinated internationally.*
- *Given the increased importance in the financial system's value chain of big tech groups that conduct diverse activities and are subject to significant internal interdependencies, there is also value in considering establishing group-wide requirements on operational resilience for these entities.*

1. Introduction

In recent years, new technologies, and new players more adept at these technologies, emerged in the financial system. The pandemic highlighted the importance of and reliance on new technologies in the provision of financial services.[2] At the same time, these technologies resulted in new business models.[3] In particular, open finance now enables different players to "plug and play" and provide financial services to customers. Platform-based business models, on the other hand, enable financial firms to provide services based on the licences they have while the front-end customer platform is owned by a technology firm. Decentralised finance, meanwhile, aims to provide financial services without intermediaries, using automated protocols enabled by distributed ledger technology and smart contracts to facilitate transactions.[4]

[1] Jermy Prenio (jermy.prenio@bis.org) and Fernando Restoy (fernando.restoy@bis.org), Bank for International Settlements. The authors are grateful to those that provided helpful comments, including Stefan Hohl and Takao Miyamoto, and to Theodora Mapfumo for administrative support. This paper builds on a presentation prepared by the authors for the Bank of England Conference on Macroprudential Policy (London, 7–8 July 2022).

[2] Crisanto and Prenio (2020).

[3] BCBS (2018a).

[4] FSB (2019a).

The emergence of big techs also resulted in a number of technological interconnections and interdependencies due to big techs' different interactions with the financial system. Big techs may provide the customer-facing platform where different financial firms offer their services, or big techs could offer the services directly. Big techs may also partner with financial firms on specific products or services or provide third-party services to firms and financial market infrastructures (FMIs).[5]

Firms' increased reliance on technology and the additional complexity and interconnections that technology has brought to the financial ecosystem pose operational risks not only for individual institutions but also for the financial system.

These developments highlight the importance of enhancing authorities' ability to assess and address the operational risks posed by developments in the technological environment from a systemic perspective.

This paper looks at operational resilience through a macroprudential lens. Section 2 examines progress in developing frameworks for operational resilience and compares the main guidelines that have been issued. Section 3 explains the macroprudential concerns of operational resilience and offers some ideas on how to address them. Section 4 concludes.

2. Progress in developing frameworks for operational resilience

Operational resilience policies are basically related to risk management (including for cyber security), business continuity management and third-party management policies. In simple terms, the objective of operational resilience policies is to ensure that financial firms and FMIs remain able to operate, particularly in terms of the provision of their important or critical services, through a disruption.

Separate policies or guidelines related to each of the different components of operational resilience can contribute to achieving the same objective. Nevertheless, a few authorities have chosen to put all these things together to come up with a holistic operational resilience policy.

At the international level, the Basel Committee on Banking Supervision (BCBS) issued its *Principles for operational resilience* in March 2021.[6] As the name suggests, these are high-level principles focusing on strengthening banks' operational resilience, largely derived and adapted from existing guidance that have been issued by the BCBS or national supervisors. The BCBS principles expect banks to identify their critical operations, which should be consistent, when relevant, with their recovery and resolution plans; to define their tolerance for disruption for these operations, in line with their risk appetite; and to test against them.

At the national or regional level, three initiatives are worth mentioning:

In the United Kingdom, the Bank of England (BoE) and the Financial Conduct Authority (FCA) issued their joint policy on operational resilience in March 2021.[7] The UK policy requires firms to know which of their services for end users are most important and understand how they are delivered (the approach is therefore customer-centric). This was followed by a policy statement from the UK HM Treasury on critical third parties to the finance sector,[8] which in turn was the basis for the BoE/FCA discussion paper on operational resilience and critical third parties.[9]

5 Crisanto et al (2022).

6 BCBS (2021).

7 *Operational resilience: Impact tolerances for important business services*, which was accompanied by separate policy documents issued by the Prudential Regulation Authority, FCA and BoE.

8 UK HM Treasury (2022).

9 BoE/FCA (2022).

In the US, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency issued a joint paper on operational resilience in October 2020.[10] The paper focuses on critical operations (like the BCBS approach) and core business lines (disruption of which could lead to a material loss of revenue, profit or franchise value).

In the EU, the draft Digital Operational Resilience Act (DORA)[11] was published in September 2020 and is expected to be finalised and adopted in Q3 2022. As the name suggests, DORA focuses on firms' ability to manage and remain resilient to information and communications technology (ICT) risks. It builds on the existing European Banking Authority (EBA) guidelines on outsourcing and ICT and security risk management.

Comparing the different operational resilience guidelines

In terms of scope, the BCBS and US guidelines are targeted at banks. The UK and EU guidelines more broadly target financial firms, including not only banks but also, among others, insurance companies, investment firms, payment institutions and financial market infrastructures.

The BCBS, UK and US approaches are quite similar. Financial firms are basically expected to identify which important operations/services should be made resilient; understand how these operations/services are delivered; set standards of resilience for these operations/services; test against them; and address identified vulnerabilities or weaknesses (Figure 1). Hence, they look at all potential causes of operational disruption – whether they be internal or external, or due to people, processes or systems.

Framework for operational resilience — Figure 1

Source: FSI illustration based on general framework followed by the guidelines examined for this paper.

DORA, on the other hand, focuses only on ICT-related disruptions. It does not require financial firms to identify important operations/services explicitly, but instead requires firms to identify, classify and adequately document all ICT-related business functions. In managing ICT-related incidents, however, DORA requires firms to classify incidents according to their priority and to the severity and criticality of the services affected.

Table 1 provides a broad comparison of the key elements of the different guidelines, and these are explained further below.

All four guidelines require mapping of internal and external interconnections and interdependencies. In the case of the BCBS, UK and US guidelines, this involves identifying the people, processes, technology and information required to deliver the important operations/services. Given the

[10] Board of Governors of the Federal Reserve System et al (2020).

[11] EC (2020).

focus of DORA, it is mainly concerned with information assets supporting ICT-related business functions and the ICT system configurations and interconnections with internal and external ICT systems.

In terms of setting standards of resilience, the UK guidelines require firms to define their impact tolerances, ie the maximum tolerable level of disruption to important business services. The UK authorities express the view that impact tolerances are different from risk appetites. The former assumes the particular risk has materialised and so the disruption it causes needs to be managed. The latter focuses on managing the likelihood of operational risks occurring. The BCBS, US and EU guidelines, however, have not fully disassociated the setting of firms' "tolerance for disruption" (or risk tolerance in the case of DORA) from their risk appetites.

The BCBS, UK and US guidelines refer to "severe but plausible" disruption scenarios. The US guidelines specify that these scenarios should include operational incidents identified by the firm's operational risk management function, independent audit, business continuity management and recovery and resolution planning activities. The UK guidelines go even further by specifying that previous incidents and near misses across the financial sector and in other sectors and jurisdictions should also be included. DORA, on the other hand, requires firms to have risk scenarios relevant to their ICT-related business functions and information assets.

On testing standards of resilience against defined scenarios, the BCBS and US guidelines focus more on testing business continuity plans. The UK guidelines, on the other hand, encourage firms to leverage existing testing arrangements irrespective of whether the testing is required by other policy areas or driven by commercial interests. These could include, for example, tests related to ICT security, business continuity and operational risk. Meanwhile, DORA requires firms to have a digital operational resilience testing programme. The kind of tests included in the programme would depend on the firm's size, business and risk profile, and ranges from vulnerability assessments and scans all the way to threat-led penetration testing.

Broad comparison of operational resilience guidelines Table 1

Guidelines	What operations or services need to be resilient	How these operations or services are delivered	Standards of resilience for these operations or services	Testing against these resilience standards	Address identified vulnerabilities or weaknesses?
BCBS: Principles for operational resilience	Critical operations	Mapping of internal and external interconnections and interdependencies	Tolerance for disruption in line with risk appetite	Incident response and recovery procedures reviewed and tested	Yes
EU: Digital Operational Resilience Act	All ICT-related business functions	Mapping of interconnections with internal and external ICT systems	Risk tolerance in line with risk appetite	Digital operational resilience testing programme based on a firm's size, business and risk profile	Yes
UK: Operational resilience: impact tolerances for important business services	Important business services	Mapping of internal and external interconnections and interdependencies	Impact tolerances	Encourages firms to leverage a whole range of existing testing arrangements	Yes
US: Sound practices to strengthen operational resilience	Critical operations	Mapping of internal and external interconnections and interdependencies	Tolerance for disruption in line with risk appetite	Test business continuity plans	Yes

Source: FSI analysis.

Other important elements of the guidelines

An important element of all four guidelines is third-party management. The guidelines expect firms to have an assurance process about the operational resilience (or ICT security standards, in the case of DORA) of third parties, including having exit plans. The UK guidelines specify further that firms should exercise their access, audit and information rights in respect of material outsourcing arrangements. DORA expects the same provisions to be included in firms' contracts with ICT third-party service providers, and for the providers to fully cooperate with the competent authorities and resolution authorities of the financial firm. The UK guidelines have explicitly recognised the challenges that firms, particularly smaller ones, face when undertaking this assurance process. For example, they encourage an industry solution if there are synergies across assurance work from firms on third parties such as certifications. They also acknowledge that for some firms it may not be appropriate to carry out sophisticated testing on large third-party providers. If this is the case, firms should seek alternative ways to gain assurance of their operational resilience such as desktop testing.

DORA and the recently issued BoE/FCA discussion paper explicitly provide for an oversight framework for critical ICT third-party service providers. In the case of DORA, critical third-party service providers will be designated by the European Supervisory Authorities (ESAs). These service providers will be subject to supervision, including on-site inspections and ongoing oversight, by a lead overseer. Financial firms can only use the services provided by critical third-party service providers established in the EU. Competent authorities may require financial firms to suspend or terminate the use of service provided by the critical ICT third-party provider if the risks posed by the provider are not or cannot be addressed. In this context, the ESAs are asked to foster international cooperation on ICT third-party risk

through the development of best practices for the review of ICT risk management practices and controls, mitigation measures and incident responses. In the case of the BoE/FCA discussion paper, the UK HM Treasury will designate critical third parties in consultation with the supervisory authorities and other relevant bodies. It does not propose that critical third parties be required to be located in the UK.[12] The discussion paper envisions subjecting critical third parties to operational resilience requirements consistent with those imposed on financial firms.

Finally, DORA aims to harmonise and streamline regulatory reporting of ICT-related incidents. It also provides that financial firms may set up arrangements to exchange amongst themselves cyber threat information and intelligence, and that firms notify competent authorities of their participation in such arrangements. The BCBS principles mention communication plans, including incident reporting to regulatory authorities. The US guidelines mention internal reporting but not reporting to regulators. The UK explicitly excludes regulatory reporting in the scope of its operational resilience guidelines. The BCBS, US and UK guidelines do not refer to information-sharing arrangements among financial firms.

3. A macroprudential view of operational resilience

As mentioned above, the interconnected use of technologies within the financial ecosystem can affect operational resilience at the system level. It is therefore not enough to assess and monitor the operational resilience of individual firms. Authorities need to also adopt a macroprudential perspective when addressing risks of operational disruptions in the provision of financial services.

Assessment of operational resilience at the system level could, for example, involve objective metrics such as the number of technology firms providing critical services or number of systemically important financial institutions (SIFIs) or FMIs relying on a big tech's services. The FSB Financial Stability Surveillance Framework[13] already looks at reliance on third parties in assessing operational vulnerabilities in the global financial system.

The definitions of important or critical operations/services in the BCBS, UK and US guidelines actually use a macroprudential lens. The BCBS principles talk about critical operations "the disruption of which would be material to the continued operation of the bank **or its role in the financial system**". The US guidelines refer to critical operations "the failure or discontinuance of which would **pose a threat to the financial stability of the United States**". The UK guidelines consider important business services "that, if disrupted, would **impact the supervisory authorities' objectives and thereby the public interest as represented by those objectives**".

While the identification of important operations/services takes on a macroprudential view, setting the standards of resilience for these operations/services and testing against these standards are left to individual firms. Therefore, there may be scope for authorities to undertake these activities at the system level. This is already done to some extent, particularly for cyber resilience testing, where supervisors and banks conduct industry-wide and sometimes even cross-border exercises.[14] Industry-wide exercises based on other operational disruption scenarios may also be useful.

Authorities also need to assess how technology used at individual firms is connected and adopt a macroprudential view when deciding on a course of action. That approach would be particularly appropriate in two different but related domains: (i) the use by financial firms of critical technology

[12] The discussion paper, however, did not provide details on how the requirements will be imposed in practice on critical third parties that are located outside the UK.

[13] FSB (2021a).

[14] BCBS (2018b).

services, such as cloud computing services (CCS); and (ii) the provision by big techs of both technological services (like CCS) to regulated entities and a diversity of financial services to the public.

The case of cloud and other critical technology services

From a microprudential perspective, the use of cloud by a typical financial firm enhances its IT security far beyond what the firm alone can accomplish. However, from a macroprudential perspective, all firms – including SIFIs and FMIs – using the same cloud provider leads to systemic risk. The consequences to the financial system of an operational disruption on the cloud provider will be quite severe. The cloud provider in this case can be considered "systemically important". Theoretically, there is a range of options to potentially address this issue.

- The first is to require all financial firms, including SIFIs and FMIs, that acquire technology services, such as CCS, from critical third-party providers to assess the potential implications for their operational resilience. This is the prevalent regulatory approach.[15] Regulations typically require financial firms to do their due diligence in third party selection. In addition, the majority of regulations require financial firms to guarantee the "rights to inspect or audit" their service providers, including, in some jurisdictions, their significant subcontractors.[16] Recognising the challenges of auditing large third-party technology providers, some authorities now accept pooled audits (ie audits done collaboratively with other financial firms that are also clients of the third party) or independent audits performed on the third party by either its internal audit function or an external auditor.[17]

  This approach allows financial firms to focus on their main activity, which is the provision of financial products and services. Enhancements to their ICT capabilities will be outsourced to third parties that have more expertise in this area.

  The main drawback is that system-wide operational resilience basically hinges on individual firms' assessments. It puts the burden on financial firms to evaluate the effectiveness of the third party's own risk management and IT security. It is uncertain whether firms would have the right incentives and the means to perform thorough assessments of the risks posed by their interactions with critical third-party providers. In addition, having all firms performing their own audit of the same providers could be vastly inefficient. It remains to be seen whether collaboration across financial firms (as in pooled audits) would address these issues.

- The second option is a variation of the first one but would require financial firms to use a multi-provider strategy. This strategy involves the use of two or more providers for each critical service, such as CCS. It also involves planning for business applications to be portable between multiple providers. As with the first option, assessment of the operational resilience of the third parties would be left to individual firms.

  In addition to the benefits described for option 1, use of multiple providers ensures that an outage in one provider does not become a systemic problem. It can also help avoid vendor lock-in.

  The main drawback is the same as the first option. In addition, it is inefficient since it requires firms to take on additional costs to run the same services. In the case of CCS, this approach could also make the process of cloud configuration[18] more challenging. It could magnify the risk of

15 FSB (2020).

16 Some jurisdictions also provide these audit rights to supervisory authorities themselves.

17 BCBS (2018b).

18 The process of making sure that elements of a cloud environment can interoperate and communicate.

misconfiguration if the providers use proprietary security standards and protocols, potentially leading to security and data breaches.[19]

- The third, and extreme, option is to disallow SIFIS and FMIs from relying on third-party providers. In practice, this would mean ramping up regulatory expectations for SIFIs' and FMIs' ICT capabilities, requiring them to be fully self-sufficient in this respect. This could be justified on the grounds that any systemic institution should have the requisite resources and capabilities, including in terms of ICT, to conduct its business in a safe and sound manner.

  The advantage of this approach is that any operational incident on a third-party provider will not spread to other parts of the financial system through the SIFI/FMI. The incident will thus be contained.

  The disadvantage is that this is not really an efficient setup and could just distract SIFIs and FMIs from their main functions, which itself could have implications for their operations. ICT is not their comparative advantage, and the more efficient way of enhancing their ICT capabilities might be to acquire the services of technology firms. In addition, an operational disruption in an in-house SIFI/FMI ICT infrastructure would still have a systemic impact. While this option may be theoretically possible, it would negate the enhancements in operational resilience that individual firms have achieved with the help of third-party providers.

- The fourth option is to expand the reach of regulation to critical third-party providers in the financial system, such as cloud service providers. This is what DORA proposes and what the UK envisions in its policy statement and discussion paper on critical third parties.[20] In practical terms, technology service providers should only be able to offer their services to any financial firm if they comply with regulatory requirements.

  The advantage of this approach is that: (i) it allows oversight of these third-party providers that is consistent with the operational resilience expectations for the financial system; and (ii) it provides clarity to financial firms and FMIs about which third-party providers comply with regulatory expectations. In addition, financial authorities would have more sway than financial firms, either individually or collectively, if they demand third-party providers to introduce changes to their ICT security controls/processes.

  The disadvantage is that having financial authorities put their "stamp of approval" on third-party service providers assumes that they are better than financial firms at making such assessments. But this may not necessarily be the case given the limited resources many authorities have. This could be addressed by having joint assessments by different government bodies (eg in addition to financial authorities, those in charge of ICT, cyber security and data protection). More importantly, as seen in the case of DORA and depending on the regulatory regime, the adoption of this approach may require critical providers to establish in each jurisdiction a legal entity that would be responsible for ensuring compliance with the relevant regulation in that jurisdiction. That looks largely inefficient, not only for critical providers, which typically have a global and multisectoral scope of activities, but also for internationally active financial firms.

Given that the provision of cloud services is largely concentrated in a few global technology companies, the fourth option can be further tweaked to address the inefficiencies arising from having to comply with regulations in individual jurisdictions, which potentially could vary widely. A more effective line of action could be the establishment of an international regulatory and supervisory regime. The former could be achieved by developing specific international standards for firms offering critical services beyond a minimum threshold. The latter might require the appointment of a leading supervisory authority for each critical provider and the creation of multi-country supervisory colleges. Aside from addressing

[19] FSB (2019b).

[20] UK HM Treasury (2022), BoE/FCA (2022).

inefficiencies, cross-border oversight is also necessary given the potential global impact of a failure of some of these critical third-party providers.

The example of the regime put in place for the Society of Worldwide Interbank Financial Telecommunication (SWIFT) could serve as an inspiration.[21] SWIFT is subject to oversight by central banks of G10 countries. Being a cooperative society under Belgian law, its lead overseer is the National Bank of Belgium. An Oversight Forum was also established in 2012, which provides a venue for G10 central banks to share information on SWIFT oversight activities with central banks from other major economies. While SWIFT is not regulated as such, the overseers developed *High level expectations for the oversight of SWIFT* (HLEs).[22] The HLEs outline the expectations in five categories: risk identification and management, information security, reliability and resilience, technology planning and communication with users.

The case of big techs

Among providers of different services in the finance value chain, big techs present a unique and interesting case. Big tech groups offer critical technological services to financial institutions alongside a number of financial and non-financial services for the public at large. Those services are offered through different subsisidairies located in different jurisdictions, but all rely on a common data and technological insfrastructure.[23] Operational risks therefore arise through intragroup interdependencies. Those risks can easily spill over across activities and over those firms that rely on the services (like cloud services or data analytics) provided by different legal entitites within big tech groups.

Therefore, given the systemic relevance of some the risks posed by big tech operations, a regulatory reaction seems warranted. Importantly, since operational risks stem from a unique business model that combines different interconnected activities, a specific entity-based regulatory framework for big techs is necessary to comprehensively address these risks at the group level.[24] In particular, it could be considered to establish some obligations for the parent company of big techs within scope – complementing sectoral requirements for their regulated subsidiaries – to properly identify and manage relevant internal interdependencies and to conduct regular group-wide planning and testing exercises for operational resilience.[25] Naturally, this would require greater cross-sectoral and cross-border collaboration among authorities.

4. Concluding remarks

Lack of operational resilience can have a significant impact on financial stability. There is therefore a clear need to view operational resilience through a macroprudential lens. This involves not only identifying financial operations/services that are critical at the system level, but also assessing, monitoring and testing system-wide operational resilience itself. There is scope to make this explicit in authorities' operational resilience guidelines.

Given the current state of the financial system, technology is among the most tangible and most likely cause of disruptions that can test system-wide operational resilience. As such, it is logical that authorities' efforts focus on exploring the implications of the use of technology (and its providers) for the

[21] The supervisory approach for CLS is similar. It is designated as a systemically important financial market utility in the US, and thus is regulated and supervised by the Board of Governors of the Federal Reserve System and the Federal Reserve Bank of New York. In addition, CLS also has an Oversight Committee composed of 22 central banks.

[22] See National Bank of Belgium (2007).

[23] See Crisanto et al (2022).

[24] See Restoy (2021) and Crisanto et al (2022).

[25] Ehrentraud, et al (forthcoming).

provision of critical financial operations/services. There are several ways that authorities may address risks to operational resilience posed by third-party technology providers. Given the implications of these risks for financial stability, there may be an argument for subjecting these technology providers, particularly the critical ones, to a new oversight framework. Moreover, given the increasing relevance in the financial industry of big tech groups that conduct diverse activities and are subject to significant internal interdependencies, there is a rationale for also considering establishing group-wide requirements on operational resilience for those entities.

5. References

Bank of England and Financial Conduct Authority (BoE/FCA) (2021): *Operational resilience: Impact tolerances for important business services*, March.

——— (2022): *Operational resilience: Critical third parties to the UK financial sector*, July.

Basel Committee on Banking Supervision (BCBS) (2018a): *Implications of fintech developments for banks and bank supervisors*, February.

——— (2018b): *Cyber-resilience: range of practices*, December.

——— (2021): *Principles for operational resilience*, March.

Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency and Federal Deposit Insurance Corporation (2020): *Sound practices to strengthen operational resilience*, October.

Crisanto, J C, J Ehrentraud, M Fabian and A Montiel (2022): "Big tech interdependencies – a key policy blind spot", *FSI Insights on policy implementation*, no 44, July.

Crisanto, J C and J Prenio (2020): "Financial crime in times of Covid-19 – AML and cyber resilience measures", *FSI Briefs*, no 7, May.

Ehrentraud, J, J Evans, A Montiel and F Restoy (forthcoming): "Big tech regulation: in search of a new framework", *FSI Occasional Papers*.

European Commission (EC) (2020): Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2021, (EU) No 600/2014 and (EU No 909/2014, September.

Financial Stability Board (FSB) (2019a): Decentralised financial technologies: Report on financial stability, regulatory and governance implications, June.

——— (2019b): *Third-party dependencies in cloud services: Considerations on financial stability implications*, December.

——— (2020): *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion Paper*, November.

——— (2021a): *FSB Financial Stability Surveillance Framework*, September.

National Bank of Belgium (2007): High level expectations for the oversight of SWIFT.

Restoy, F (2021): "Fintech regulation: how to achieve a level playing field", *FSI Occasional Papers*, no 17, February.

UK HM Treasury (2022): Critical third parties to the finance sector: policy statement.