

The infrastructure of independence

How central bank independence rests on foundations that statutes never contemplated

OLIVER WYMAN
A MARSH BUSINESS

REINVENTING
BRETTON WOODS
COMMITTEE

The conditions under which central banks exercise their mandates are changing in ways that formal independence statutes were not designed to address. The infrastructure through which independence is exercised — including the platforms, networks, data services, and trading systems on which monetary policy, market operations, and financial stability depend — has accumulated strategic vulnerabilities that most institutions have not examined at the governor level. This paper covers the forms those vulnerabilities can take, the dependencies through which they arise, and the institutional choices that determine whether independence holds in practice, as well as in statute.

Central banks have designed robust protections for their formal independence. The infrastructure beneath it deserves the same rigor.

1 | How independent are central banks really?

Every major central bank statute — whether it's fixed terms of office, prohibitions on monetary financing, or constraints on government instruction — was designed against one adversary: an overbearing, domestic chief of state seeking an excessive expansion of leverage, avoiding the political costs of tightening, or using monetary policy to generate growth. While the protections, for the most part, have worked over the years, they still fail to address the infrastructure through which independence is actually exercised.

The platforms used for policy analysis were treated as technical matters, distinct from the constitutional question of independence itself. The communications networks through which decisions reach markets, the payment systems through which they take effect, and the reserves held to defend them were treated as technical matters, distinct from the constitutional question of independence itself.

That assumption no longer holds. A bond market intervention that the market expects before it begins has already failed. An interest-rate decision reached on compromised analysis is not an independent one. A reserve portfolio that cannot be mobilized is not a reserve.

The most consequential failures of independence may not look like disruptions at all. They may look like institutional caution: a position not taken, an option not pursued, or a decision shaped by an unspoken awareness of where practical independence ends.

© Oliver Wyman

Exhibit 1: Where strategic vulnerability can sit beneath the mandate

Mandate function	What independence requires	External infrastructure beneath it (non-exhaustive)
1. Monetary policy		
Reserve management	Ability to access and mobilise reserves when required	Custodian platforms; SWIFT messaging; cross-border settlement infrastructure
Market operations	Confidentiality of intervention strategy; ability to transact at scale and speed in markets; integrity of price and market data informing decisions	Trading platforms and order management systems (Bloomberg, TSOX, Tradeweb); prime brokerage and clearing infrastructure; counterparty networks for repo, FX and bond market operations; commercial data and index vendors
Policy formulation and analysis	Independent analysis; confidentiality before announcement; ability to implement decisions	Cloud-hosted analytical platforms; commercial data and AI services (Bloomberg, LSEG); hyperscale infrastructure
CBDC	Domestic control over monetary transmission; continuity of issuance and redemption; integrity of the ledger	Distributed or centralised ledger infrastructure; wallet software vendors; cloud hosting for core ledger; identity and authentication systems
2. Financial stability and macroprudential policy		
Systemwide surveillance	Independent surveillance; ability to identify emerging risks across institutions and markets	Market surveillance platforms; shared cloud and AI providers; commercial data vendors
Macroprudential decision-making	Access to timely, high-integrity data; confidentiality of deliberations before announcement	Supervisory data infrastructure; cloud-hosted analytical platforms
Crisis coordination	Ability to communicate and coordinate with counterparts under stress; access to crisis management infrastructure	Secure communications platforms; cross-border coordination networks; messaging infrastructure
3. Prudential, conduct and market supervision		
Supervisory data collection and analysis	Integrity of supervisory judgment; access to accurate and timely firm-level data	SupTech analytics platforms; regulatory reporting infrastructure; third-party data providers
Authorization and enforcement	Continuity of licensing and enforcement processes; integrity of supervisory records	Case management systems; legal and regulatory databases; identity and authentication infrastructure
Supervisory communications	Secure exchange with supervised firms and international counterparts	Secure messaging and document exchange platforms; supervisory college infrastructure
4. Payments and market infrastructure oversight		
Settlement and payment finality	Continuity of settlement; payment finality under stress	RTGS and payment system software; correspondent banking networks
Messaging and interoperability	Strategic access to critical cross-border messaging infrastructure	SWIFT and equivalent messaging infrastructure; cross-border interoperability platforms
Oversight and surveillance	Ability to monitor and intervene in payment systems and FMIs	Payment system monitoring platforms; data feeds from FMIs; supervisory access to settlement data

Source: Oliver Wyman analysis

© Oliver Wyman

2 | How geopolitical pressures create strategic vulnerabilities

The foundations of central bank independence were built around decades of stable alliances. Given the current geopolitical landscape, the logic behind many of those pacts may no longer hold true.

All risks around central bank independence rise when there is geopolitical instability. An external actor might spot a strategic vulnerability, assess its value, and wait for the point of greatest leverage. That may be when the institution is most reliant on a capability and least positioned to substitute it, such as during a financial crisis or a period of acute geopolitical stress. It might even apply to the hours before a market-sensitive announcement.

Strategic vulnerability can take four distinct forms: denial, disclosure, distortion, and leverage without use — each calling for a different institutional response.

Exhibit 2: Modes of strategic vulnerability

Mode	What it means	Why it matters	Example
Denial	Access to an asset or capability is withdrawn or made conditional through sanctions, export controls, license restrictions or support constraints.	The capability may become unavailable precisely when the institution needs it most.	SWIFT's disconnection of Iranian banks in 2012 removed access to international payment messaging overnight.
Disclosure	Pre-announcement information, such as a forecast, intervention plan or liquidity decision becomes accessible to an external party before it is public.	For a central bank, confidentiality can itself be a condition of effective policy. Premature access can move markets, compromise an intervention, or expose a named institution.	Under the US Clarifying Lawful Overseas Use of Data Act, American technology companies can be compelled to produce data held on their systems and prohibited from disclosing that a request was made.
Distortion	The analytical basis for a decision is corrupted rather than denied. Data feeds, models, or tools may be altered or degraded in ways that are not apparent to the institution.	The institution may continue operating while the integrity of the evidence informing its judgment has been compromised.	A small number of commercial providers underpin monetary policy analysis and market surveillance at virtually every major central bank. Because no independent reference point exists against which to verify what the institution is receiving, a corrupted or manipulated feed may not trigger an alert.
Leverage without use	The capacity to deny, disclose, or distort is itself sufficient to shape behavior without any action being taken.	Independence can be restricted before there is any observable incident, formal instruction, or decision to reverse.	A central bank negotiating access to emergency dollar liquidity knows that the counterpart controls infrastructure it cannot replace. It reaches a deal. It believes the terms reflect its negotiating position. It has no way of knowing how different those terms would have been if the dependency did not exist.

Source: Oliver Wyman analysis

© Oliver Wyman

Leverage without use deserves particular attention because it is the hardest mode to see. A central bank negotiating access to emergency dollar liquidity knows that the counterpart controls infrastructure it cannot replace, and that awareness shapes the negotiation before either party has said anything about it. The institution may believe the terms it accepts reflect its own judgment of what the situation requires, with no means of knowing how different that judgment would have looked if the dependency did not exist.

An institution that knows it could be denied access to a capability or sensitive information could be extracted without its consent may quietly adjust its behavior without any overt pressure and without any record of having done so. The most consequential failures of independence may not look like disruptions at all. They may look like institutional caution, a position not taken, an option not pursued, or a decision shaped by an unspoken awareness of where practical independence ends.

An institution that knows it could be denied access to a capability or sensitive information could be extracted without its consent may quietly adjust its behavior without any overt pressure and without any record of having done so.

© Oliver Wyman

3 | Two tests of independence: execution and integrity

The four modes fall into two distinct dimensions of independence. Denial and leverage threaten what the institution remains able to do. Disclosure and distortion threaten the integrity of an impending action. The distinction matters because the two problems require different safeguards.

Exhibit 3: Execution and Integrity tests using cloud as an example

Test 1: Execution **What must remain executable, whatever an external party decides?**		**Test 2: Integrity** **What must remain protected from external access, whatever an external party could be compelled to do?**
• If this provider was designated under a sanctions regime, which critical functions would stop, and how quickly? • Does your exit plan assume you would have time to switch? • How many of your fallback arrangements run on the same underlying infrastructure as the thing they are supposed to replace? • Your concentration risk assessment maps your direct suppliers. Does it map what they all have in common underneath? • When did you last test your contingency arrangements under adversarial conditions, and not a scheduled drill?	**Cloud-based analytical platform**	• Could a foreign government compel this provider to hand over your pre-announcement data without telling you? • If the model shaping your inflation forecast was quietly degraded, would you know before you acted on it? • When your cloud provider and your AI tools come from the same company, how much of your analytical independence is real? • Your concentration risk assessment shows multiple vendors. Does it show what sits beneath them all? • Your data is protected by contract and technical controls. But contractual assurance and sovereign control are not the same thing — who ultimately decides?

Source: Oliver Wyman analysis

On execution, the question is what must remain operative, whatever an external party decides. Implementing a policy decision, mobilizing reserves, and maintaining payment finality must be achievable regardless of what any provider, government, or legal jurisdiction chooses to do. A decision that cannot be implemented is not, in any meaningful sense, independent. These failures of independence leave no formal trace. While no statute is overridden and no instruction is issued, the constraint is nonetheless real.

© Oliver Wyman

On integrity, central banks hold information with value that depends entirely on its confidentiality. A rate path forecast, an intervention plan, a collateral haircut change, or liquidity provision to a named institution can all be market-moving before they are public. Where analytical work runs on infrastructure subject to a foreign legal jurisdiction, confidentiality can ultimately depend not only on technical and contractual safeguards but also on the legal powers of that jurisdiction. The US Clarifying Lawful Overseas Use of Data Act permits US authorities to compel American technology companies to produce data held on their systems, including on servers located outside the United States. Contractual assurance and sovereign control are not the same thing.

The same vendor relationship can implicate both tests. A cloud-hosted analytical platform can be denied access, cutting off a critical capability, while the data on that platform may also be subject to legal compulsion.

Most institutions have built governance around the first test. Very few have seriously mapped where they stand on the second.

© Oliver Wyman

4 | How technology has extended strategic vulnerability

Reserve custody, correspondent banking, and payment infrastructure have always involved external reliance that geopolitical conditions could test. What has changed is how far that reliance extends and how difficult it has become to see where it sits.

Monetary policy analysis, market operations, payment finality, supervisory surveillance, and crisis coordination increasingly run on infrastructure provided by a small number of firms in a handful of jurisdictions. The extraterritorial reach of US law over cloud infrastructure and the use of chip export controls as instruments of strategic competition are not theoretical risks. They are live mechanisms already applied in other contexts.

The reliance runs deeper than a list of suppliers suggests. Different applications from different vendors may draw on the same underlying cloud platform, the same foundation models, or the same data infrastructure. An institution can believe it has diversified across multiple vendors while remaining concentrated at the infrastructure layer beneath them. Cloud is the most discussed and most governed of these layers — regulators in several jurisdictions have begun to respond through sovereign cloud requirements and national assurance schemes — but it is primarily a question of where data sits and who can reach it. The harder questions sit further up the stack.

Data and AI reach directly into the quality and independence of institutional judgement. Monetary policy analysis and market surveillance at virtually every major central bank depend on a small number of commercial data platforms. The governance conversation around that concentration is not proportionate to its scale. AI compounds the problem in a unique way: A foundation model shapes the framing of a question and the range of answers it surfaces before the analyst has formed a view. Unlike a corrupted data feed, there is no alert. The institution believes it is reaching its own conclusions. It is not.

Market operations remain the least examined dependency of all. The infrastructure through which central banks intervene in bond and money markets, including trading platforms, order management systems, counterparty networks, and real-time price data, is provided almost entirely by commercial firms operating under foreign jurisdiction. A bond market intervention depends on confidentiality of strategy, speed of execution and integrity of market data simultaneously. Each rests on infrastructure the institution does not control. The conditions most likely to trigger a large-scale intervention are precisely those under which that vulnerability is most likely to be tested.

CBDC sits at the intersection of these questions and deserves to be treated as such. Designed well, with domestically controlled infrastructure, it can reduce certain dependencies — on commercial banks for monetary transmission, on correspondent networks for cross-border settlement. Designed without that discipline, it creates new strategic vulnerabilities while appearing to address old ones. The infrastructure decisions being made now will determine which it becomes.

© Oliver Wyman

Exhibit 4: Mandate dependencies across the stack

Stack layer	1. Monetary policy	2. Financial stability and macroprudential policy	3. Prudential, conduct and market supervision	4. Payments and market infrastructure oversight
1. **Raw materials/ critical minerals**	The hardware underpinning every mandate function depends on critical minerals concentrated in a small number of jurisdictions and subject to export controls			
2. **Semiconductors**	Processing of reserve transactions; execution speed for market intervention; compute underpinning macroeconomic modelling	Compute for systemic risk modelling and stress-testing	Processing underpinning supervisory analytics	Transaction processing across RTGS and settlement
3. **Hardware**	Cryptographic hardware protecting reserve authorisation, intervention signing and pre-decision data	Secure infrastructure for stability data and surveillance	Secure supervisory infrastructure	Cryptographic hardware for payment authentication; RTGS servers
4. **Connectivity**	Cross-border custodian communications; real-time market data feeds; secure communications before policy announcement	Crisis coordination communications	Supervisory data exchange with firms and counterparts	Cross-border payment messaging
5. **Cloud/ hyperscale**	Reserve management and trading platform hosting; analytical platform hosting; sensitive pre-decision data	Surveillance platforms; financial stability data repositories	SupTech platform hosting; regulatory data repositories	Payment system and settlement infrastructure hosting
6. **OS and middleware**	The operating environment for every mandate-critical system runs on software concentrated among a small number of providers			
7. **Cybersecurity tooling**	Detection, response and protection infrastructure for mandate-critical systems is concentrated among a small number of providers whose telemetry transits foreign infrastructure			
8. **AI foundation models and compute**	Macroeconomic forecasting; MPC briefing preparation; intervention impact modelling	Systemic risk modelling; contagion assessment	Supervisory assessment and enforcement analytics	Fraud detection and transaction monitoring
9. **AI applications and agents**	Reserve portfolio optimisation; inflation nowcasting; policy briefing tools	Early warning and contagion monitoring tools	Cross-institution exposure analytics	Payment anomaly detection; liquidity monitoring
10. **Productivity software**	The drafting of policy papers, intervention strategies and supervisory findings, and the email, video and messaging infrastructure through which governors deliberate and coordinate, sit on platforms provided by a small number of providers subject to foreign jurisdiction			
11. **Payment systems**	Cross-border reserve transfers; clearing and settlement of bond and FX operations	Payment system stress monitoring	Supervisory access to payment and settlement data	Core mandate: RTGS, retail rails, correspondent networks
12. **Data and digital identity**	FX and custody data for reserve valuation; market microstructure and conditions data	Cross-institution exposure and contagion data	Regulatory reporting data; entity identity infrastructure	Payment flow and liquidity surveillance data
13. **Quantum technologies**	Quantum computing threatens current encryption standards across every mandate function; quantum-resistant cryptography is not yet embedded in most central bank infrastructure			

Source: Oliver Wyman analysis

5 | Independence requires design

External reliance will remain both necessary and valuable across most of what a financial authority does. Global technology markets provide capabilities that no institution could replicate domestically at comparable quality, and the goal is deliberate management of where dependencies sit rather than their elimination. What that requires is visibility of strategic vulnerabilities, a conscious decision about which ones sit within the institution's risk appetite, and a governance structure capable of reassessing that position as conditions change.

Practical independence has three dimensions, each of which the others depend on. The institution must be able to act through disruption, adapt as circumstances change, and reach decisions on the basis of genuinely independent judgment. Continuity without adaptability leaves the institution operating inside a constrained model with no means of changing it.

The ability to adapt without the governance to make informed decisions about when and how to do so produces optionality that nobody exercises. All three must be in place together, and the weakest determines how much practical independence the institution retains.

Practical independence is not secured through any single decision. It accumulates or quietly erodes through the ordinary run of choices. A cloud migration approved by the technology committee, an AI analytics tool adopted by research, or a data contract renewed on commercial terms may each be entirely reasonable in isolation. Taken together, across functions and over time, they determine how much practical freedom the institution retains when conditions change. The conversation about strategic vulnerabilities is one that most institutions have not had.

Most governance frameworks ask who approves a significant technology contract but leave the cumulative picture in nobody's line of sight. Whether the aggregate effect of many smaller decisions is visible to someone with the authority to act on, it's a question current frameworks are not designed to answer. The gap is structural rather than incidental, and closing it requires explicit accountability for the institution's overall strategic vulnerability position, not just for individual procurement events.

The urgency of this is sharpest precisely when it is hardest to address. Sanctions escalations, acute geopolitical stress, and systemic financial crises are the conditions most likely to expose strategic vulnerabilities, and they are also the conditions under which emergency liquidity operations, crisis coordination, and monetary policy are most critical.

Practical independence is not secured through any single decision. It accumulates or erodes through the ordinary run of choices.

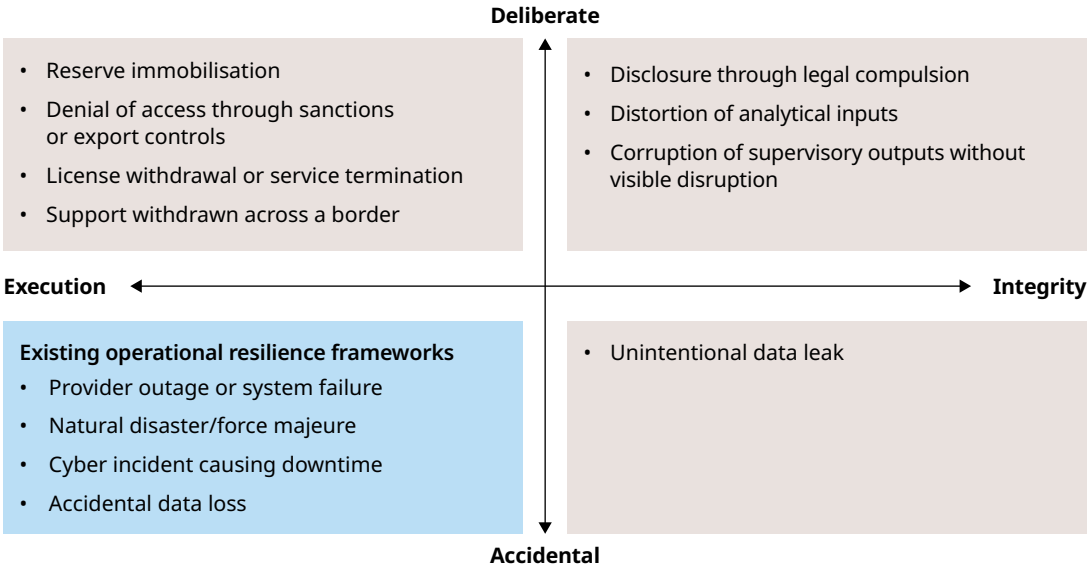
© Oliver Wyman

6 | The limits of operational resilience for financial authorities

Many financial authorities already have well-developed frameworks for concentration and critical third-party risk. The Digital Operational Resilience Act (DORA) in Europe, the critical third-party powers granted to the Bank of England and Financial Conduct Authority under the Financial Services and Markets Act 2023, and the Financial Stability Board's global toolkit are built from a common concern that a small number of vendors sit beneath enough of the financial system that disruption at one of them becomes systemic rather than firm-specific. The response has been greater visibility of concentration, resilience testing, exit planning, and, increasingly, direct oversight of critical vendors.

That machinery provides an important starting point for understanding where external reliance sits, how concentrated it is, and whether operations can continue if a provider fails. Strategic vulnerability asks something different: whether that reliance could be exploited deliberately through denial, disclosure, distortion, or leverage. A relationship can be well managed from an operational resilience perspective and still leave the institution strategically exposed because the question resilience frameworks ask and the question strategic vulnerability asks are fundamentally different ones.

Exhibit 5: Where existing operational resilience frameworks stop



Source: Oliver Wyman analysis

© Oliver Wyman

Financial authorities face strategic vulnerabilities that are distinct from and more consequential than those facing the firms they oversee. The same vendors and infrastructure that sit beneath the regulated system also support payment systems, market surveillance, policy analyses, and crisis responses. Authorities have a systemwide view of outsourcing, concentration and third-party exposure that no individual firm can replicate.

That view creates a higher standard they should apply to the infrastructure beneath their own mandate, one that extends beyond resilience to the deliberate assessment of strategic vulnerability.

Operational resilience remains a necessity, but it is incomplete for this purpose.

Continuity arrangements, outsourcing registers and third-party risk frameworks test whether an institution can withstand disruption and recover from failure. They are less well suited to a situation in which another actor can choose whether, how and when to exploit a vulnerability. Nor do they fully address the second test of independence, where the concern is not continuity at all, but whether confidential information, analytical inputs and institutional judgment remain protected from external access or influence.

For an authority, the consequences are also harder to transfer elsewhere. Monetary authority and crisis coordination cannot be moved at comparable speed if the institution itself is constrained. The task is not to replace operational resilience, but to extend it.

Existing frameworks help authorities understand and manage external reliance, but the current gap is extending them to capture strategic vulnerabilities from adverse actors.

© Oliver Wyman

7 | From awareness to action

Digital sovereignty has moved from a policy aspiration to an operational agenda. Governments and supranational bodies across different political and regulatory traditions, from the European Commission's Tech Sovereignty Package to Japan's Economic Security Promotion Act and the US CHIPS Act, are treating concentrated dependency on foreign-controlled technology infrastructure as a strategic vulnerability requiring a deliberate policy response. Central banks are operating inside that broader shift. Most have not yet applied its logic to their own mandates, though the conditions that make it urgent for governments apply equally to the institutions responsible for monetary policy, financial stability, and crisis response.

Not every authority starts from the same position, and the distance between where most institutions currently sit and where they need to be is not covered in a single initiative. The stages below map that progression, from dependencies that are inherited and unexamined to an institution that has deliberately designed independence into the infrastructure beneath its mandate.

Exhibit 6: The strategic vulnerability management maturity curve

Stage	Characteristics	What it looks like in practice
1 Unexamined strategic vulnerability	Strategic vulnerabilities are implicit or inherited. Technology and procurement are viewed as operational support. No defined risk appetite for strategic vulnerability.	No consolidated view of where external constraint could affect the mandate. Vulnerabilities become visible through incidents or external events rather than deliberate assessment.
2 Compliant resilience	DORA-grade continuity arrangements and third-party risk frameworks are in place. The focus is whether the institution can keep operating through disruption.	Necessary, and well served by the market. Answers the operational question, but not the strategic one.
3 Deliberate positioning	Mandate-critical capabilities are identified. Strategic vulnerabilities are mapped. Acceptable external reliance is consciously determined against the two tests.	The institution can say specifically which capabilities require greater control and why, where credible alternatives are needed and where market reliance remains acceptable.
4 Independence by design	Risk appetite embedded into procurement, architecture, governance, and investment. Strategic vulnerabilities reviewed continually as conditions evolve.	Independence is actively designed, not assumed. Sovereignty is a standing discipline, not a periodic exercise.

Source: Oliver Wyman analysis

© Oliver Wyman

Progressing through these stages is not a one-off exercise. Strategic vulnerability shifts as vendors consolidate, technology evolves, and geopolitical relationships change, which means the assessment needs to be revisited as the environment changes and new decision points emerge. For authorities looking to move forward, five questions provide a practical starting point for understanding where they currently stand and what needs to change:

1. Can the institution name the capabilities where independence is genuinely at stake?

Not every external relationship, and not a catalogue of systems and suppliers. The task is to identify where denial, disclosure or distortion could materially constrain mandate delivery or the integrity of institutional judgment — payment finality, the analytical infrastructure for monetary policy, crisis communications, emergency liquidity. Most institutions have not done this with the specificity the question requires.

2. Can the institution accurately map the vulnerability beneath each one?

For each capability, the authority needs to understand the form of strategic vulnerability, the parties and jurisdictions through which it could arise and where concentration is greatest. Those assumptions should then be tested under deliberate geopolitical pressure rather than accidental disruption alone. An alternative that exists in normal conditions may disappear during sanctions escalation or geopolitical rupture. An exit that takes eighteen months to execute is of little value if the capability is needed tomorrow.

3. Has the institution decided how much strategic vulnerability it is prepared to carry?

External reliance will remain necessary and often desirable. The strategic choice is where market provision remains consistent with independence, where stronger assurance is sufficient, where a credible alternative needs to exist, and where the consequences of constraint justify greater control. These are questions of institutional risk appetite, not technology architecture or supplier management. They require a Governor-level answer, not a procurement one.

4. Are the next decisions by the institution being made as independence decisions?

Procurement, architecture, major migrations, model adoption, and contract renewal are the points at which optionality can still be preserved at reasonable cost. Requirements that are incorporated before a relationship deepens can be relatively inexpensive. Once architecture is embedded and the number of viable alternatives narrows, the same requirements often become more expensive and cause delays. Sometimes, they turn out to be impossible to incorporate.

A decision that presents itself initially as commercial or technical may end up determining an institution's future freedom of action. The question is whether anyone in the institution is responsible for evaluating future implications of decisions.

5. Does the institution act collectively where leverage or knowledge are shared?

An individual authority may have little leverage over a provider that serves much of the global financial system. Financial authorities already know how to manage shared dependencies collectively — through swap lines, supervisory colleges, common standards, and shared infrastructure. The same instinct applies here. Common requirements, shared assessments, and coordinated engagement can alter the balance with strategically important vendors in ways that no individual institution can achieve alone.

© Oliver Wyman

Conclusion

The architects of central bank independence understood that good intentions offered no protection against political pressure. The institutional protections they designed were structural responses to a specific and identified threat, built in advance of the crises they were designed to withstand. Fixed terms, prohibitions on monetary financing and constraints on government instruction each closed off a channel through which pressure could travel.

The infrastructure beneath the mandate was never part of that original design because it was never seen as part of the independence question. The analytical platforms, trading infrastructure, payment systems, and data services through which independence is exercised in practice have accumulated dependencies that no statute contemplated and that most governance frameworks have not been designed to see. The channel of pressure runs through a technology provider or a foreign legal jurisdiction rather than a finance ministry, but the nature of the problem is the same as the one those statutes were written to solve.

The geopolitical conditions that make these questions urgent are not a temporary disruption to an otherwise stable order. Fragmentation between major powers, the weaponization of financial and technology infrastructure as instruments of statecraft, and the concentration of critical capabilities in a diminishing number of jurisdictions are structural features of the environment in which central banks will operate for the foreseeable future.

The independence statutes were written because the conditions of the postwar order made certain threats to monetary policy unavoidable and identifiable in advance. Those same conditions no longer hold, and the threats have changed with them. Designing the institutional response to those threats is the work this generation of central bankers has not yet completed.

© Oliver Wyman

Oliver Wyman, a Marsh (NYSE: MRSH) business, is a management consulting firm driven by deep industry insight, bold innovation, and a collaborative approach that cuts through complexity to help organizations navigate their most defining transformative moments. Marsh is a global leader in risk, reinsurance and capital, people and investments, and management consulting, advising clients in 130 countries. With annual revenue of $27 billion and more than 95,000 colleagues, Marsh helps build the confidence to thrive through the power of perspective.

For more information, visit oliverwyman.com, or follow us on LinkedIn and X.

Americas	Europe	Asia Pacific	India, Middle East & Africa
+1 212 541 8100	+44 20 7333 8333	+65 6510 9700	+971 (0) 4 425 7000

AUTHORS

Dominik Weh
Partner, Global Head of Central Banks and Financial Authorities Platform
dominik.weh@oliverwyman.com

Davide Taliente
Partner, Global Chair of Government and Public Institutions
davide.taliente@oliverwyman.com

Maria Fernandes
Partner, Central Banks and Financial Authorities Platform, Europe
maria.fernandes@oliverwyman.com

Alexander Ovsepyan
Global Chief of Staff, Central Banks and Financial Authorities Platform
alexander.ovsepyan@oliverwyman.com

Anika Duggal
Engagement Manager, Central Banks and Financial Authorities Platform, Europe
anika.duggal@oliverwyman.com

Marc Uzan
Founder and Executive Director, Reinventing Bretton Woods Committee
marc.uzan@reinventingbrettonwoods.org

Copyright 2026 Oliver Wyman

All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.