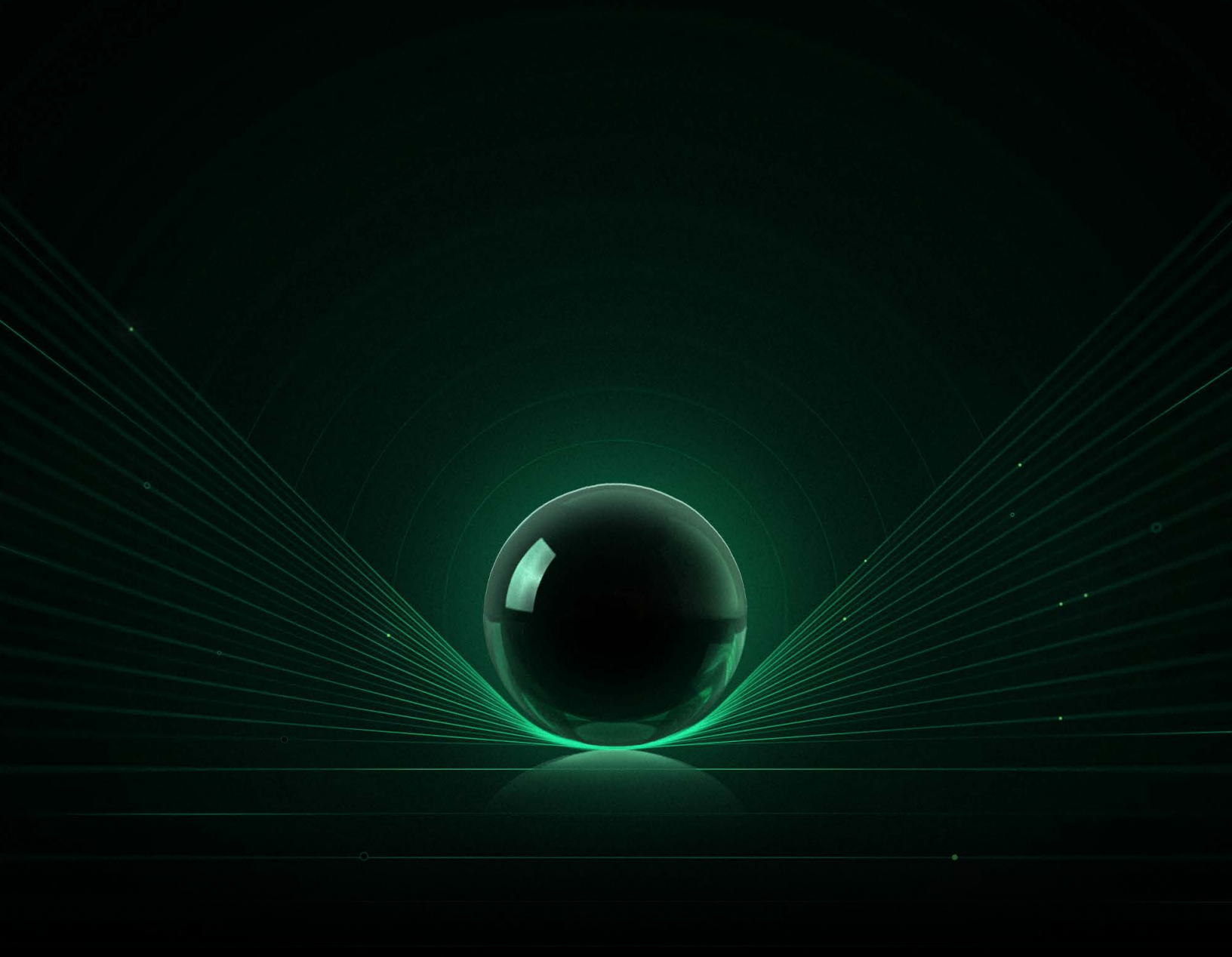




The private company playbook for *cyber resilience*

Shifting the mindset from IT defense to operational preparedness

October 2026

For most private companies, cybersecurity is often handled like a reactive game of whack-a-mole: patch a server after an alert, reset a password after a suspicious login, and hope the daily fire drill does not become a crisis. But playing catch-up can be exhausting and does little to make the business safer over time. Operating outside the public spotlight does not make private companies immune from deliberate, sophisticated attacks.

Increasingly, private companies are preferred targets of cyber criminals because they hold the same valuable data as publicly traded companies in their ecosystem, and the same access into enterprise networks, often with far less defense standing in the way. Cyber criminals also commonly target private companies because they don't face the same regulatory scrutiny as public peers.

True resilience requires a mindset shift. It is not about satisfying a checklist or eliminating every risk; it should be an active strategy that builds structural discipline, anticipates threats, aligns leadership, and strengthens the business over time.

Today's threat landscape is evolving fast, driven by the rise of frontier artificial intelligence (AI) and increasingly nimble bad actors looking to attack weakened digital systems. But this isn't a cause for alarm. It's a reason to act.

The very same technologies these threat actors are weaponizing are now at your disposal to defend, adapt, and build organizational maturity faster than ever before. For private enterprises, agility is one of your greatest assets. By shifting from a defensive, reactive posture to a proactive blueprint, you could turn a costly IT headache into a foundation for potential long-term growth and credibility.

The *accountability* gap

Public companies operate under a regulatory microscope; investor scrutiny, disclosure rules and audit committees force them to maintain a baseline of security discipline. Private companies, by contrast, operate in what we call an "accountability gap": without that top-down pressure, security posture often comes down to internal will alone. When budgets get tight, it's often pushed to the back burner in favor of immediate, revenue-generating projects.

The need for cybersecurity is especially important for private-equity-backed companies preparing for an exit, where a clean cyber record directly protects transaction value during the due diligence process. In today's market, cyber posture is now a standard part of the mergers and acquisitions (M&A) checklist.

And to make it even more pressing, enterprise clients are getting far stricter about cybersecurity controls of their third-party suppliers. Many now won't sign or renew contracts with vendors that can't prove they have strong security controls in place. For a private vendor business, losing a flagship customer is a much faster, more painful feedback loop than any regulatory fine.

There's a reason enterprise clients have gotten so strict. Attackers increasingly use smaller vendors as a stepping stone into a larger partner's network, a pattern known as island hopping. Once that's discovered, the vendor relationship rarely survives intact: the larger, buyer partner either mandates a remediation plan on a deadline or walks away entirely.

Tiffany's take

"Private equity firms and family offices are realizing that cyber posture isn't just an IT issue, it's a direct valuation driver. During due diligence, a single unpatched legacy system or a sloppy access policy can instantly stall an exit or trigger a costly valuation write-down."

Tiffany Kleemann, Managing Director, Cyber & Strategy Risk Leader, Deloitte & Touche LLP

Business resiliency is not about preventing every attack. It is about building the operational stamina to absorb disruption and keep core services running—and turning that stamina into a story you can tell customers, insurers, acquirers and more.

According to the *Deloitte Private Family Business Cybersecurity Report*, **74% of family and private enterprises globally experienced at least one cyber incident in the past 24 months¹**, making zero risk an unrealistic standard.

True resilience acknowledges that bad actors will test your boundary. Your objective is that those events

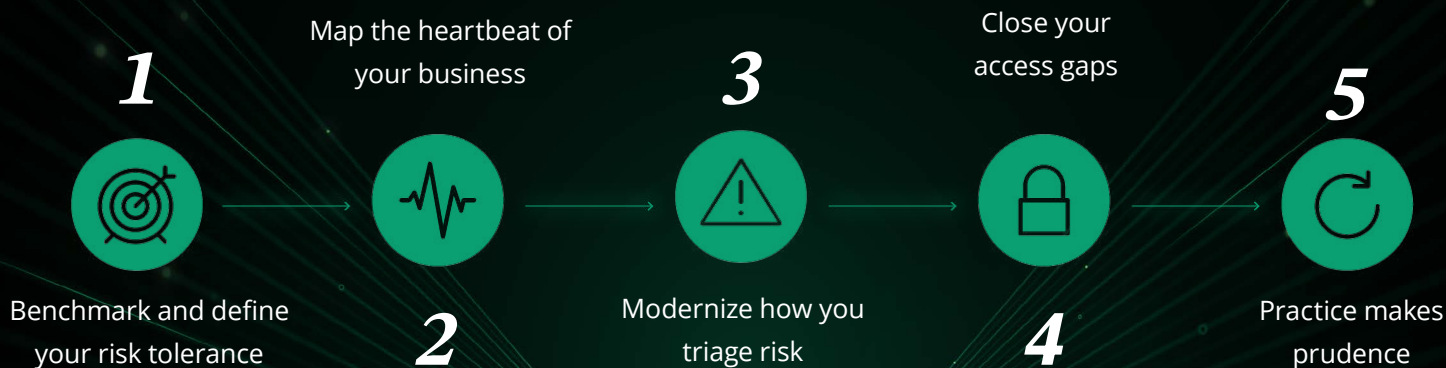
remain manageable rather than existential. When approached strategically, a mature cyber posture helps protect enterprise valuation, satisfy customer vendor requirements, and support long-term continuity.

So how do you close the gap and increase operational resiliency?

Resiliency isn't a single fix; it's a sequence of steps and commitments to taking time to make sure that things are done well. Each step below builds on the one before it, starting with a question only your leadership team can answer:

How much **risk** are you willing to carry?

The five steps to **cyber resilience**



Step 1

Benchmark and define your *risk tolerance*

Resiliency doesn't start with buying new software. It starts in the C-suite and boardroom with an honest look at where you stand and what approaches you've been taking to your cyber infrastructure.

Programmatic resilience begins by benchmarking your current setup against your private company peers. By better understanding the specific threat actors targeting your sector and how they operate, you can more narrowly target your resources.

More importantly, the board and executive team should explicitly define the organization's cyber "risk tolerance statement." This isn't a decision IT or a cyber team can make. It's a decision by leadership about how much risk your business can absorb. Furthermore, because many private companies operate without a dedicated chief information security officer (CISO), the responsibility often falls squarely on the board and executive team.

Tiffany's take

"We don't do security for security's sake, we do it to manage business risk. Risk can never be reduced to zero. Resiliency is about deciding exactly how much operational disruption your business is willing to handle, and aligning your investments, insurance and processes to that standard. Tech teams cannot decide this for you; the board and the CEO should own their risk appetite."

Tiffany Kleemann, Managing Director, Cyber & Strategy Risk Leader, Deloitte & Touche LLP

1

Step
2

3

4

5

Map the *heartbeat* of your business

Once your cyber risk tolerance is defined, you can prioritize. Begin by performing a business impact analysis to find your minimum viable company (MVC)—the smallest set of services your business needs to keep delivering to stay solvent and keep revenue flowing. Bring your leadership team into this conversation: finance, operations, sales and legal. For each crucial service, map out the people,

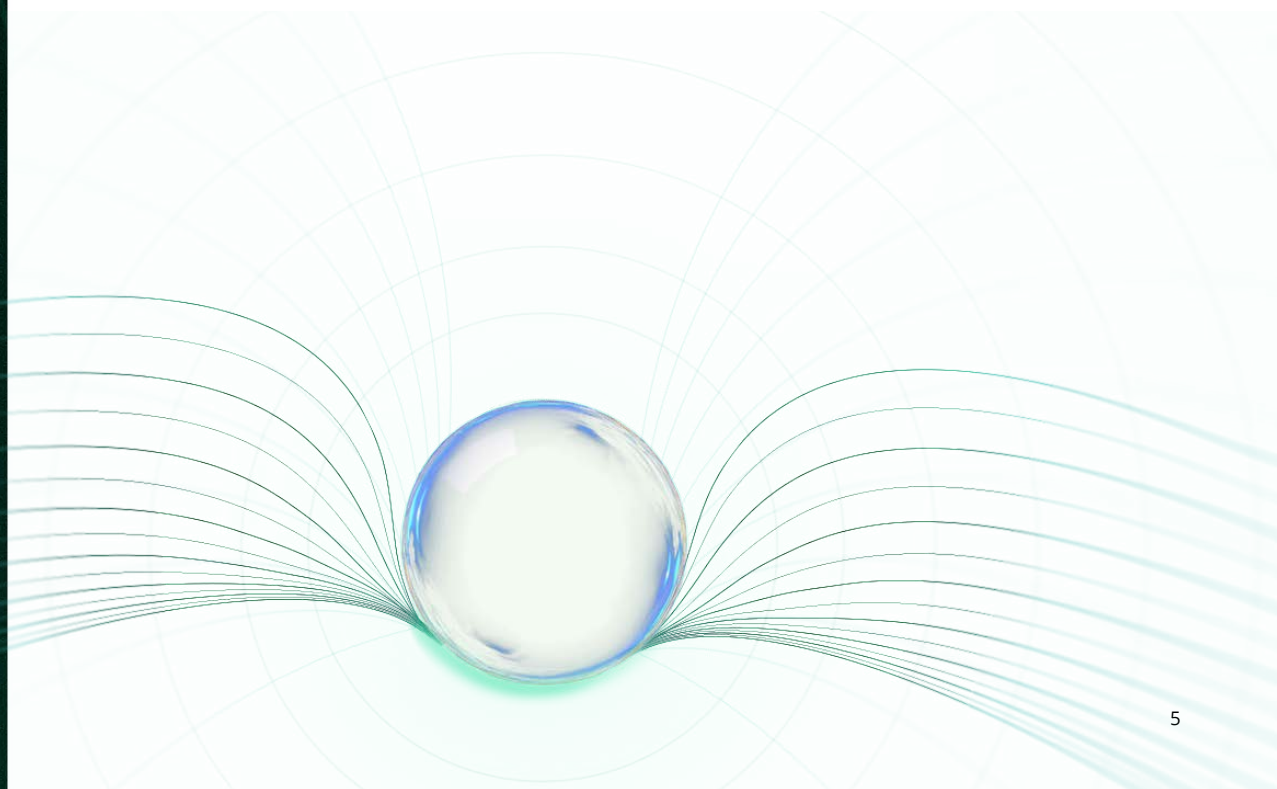
processes and technology that support it and ask: ***What breaks if this goes down?***

Once you map your key services, map your third-party suppliers to them. This immediately tells you which vendors belong at the very top of your risk management list. That mapping exercise takes weeks to do right. Unfortunately, today's attackers don't need weeks to find your weak points.

Pete's take

"If an investment firm's clients can't view their accounts, or a hospital can't pull up patient records, that's not just downtime, that could be an extinction-level event. Identify these 'heartbeat' processes first and put your resources there."

Pete Renneker, Managing Director, Risk & Financial Advisory, Deloitte & Touche LLP



Modernize how you *triage risk*

1

The threat landscape is moving at machine speed, driven by the rapid rise of frontier AI. Historically, cybercrime had natural limits. Pulling off a sophisticated hack required elite coding skills and weeks of manual research. This “friction” gave businesses a comfortable window of time to react.

Frontier AI has significantly reduced that friction, presenting private companies with a dual threat:

1. The automated bug hunt:

Attackers use AI to instantly scan the internet, locate unpatched systems, and launch automated attacks at scale in minutes, not weeks.

2. Autonomous threats:

Frontier AI models can now find software flaws and write working exploits entirely on their own, with zero human direction.

AI has fundamentally challenged our traditional way of triaging software bugs. In the past, companies tended to focus on patching important vulnerabilities, leaving “medium” bugs on a list to deal with later.

Today, frontier AI can chain together two or three of those minor, overlooked vulnerabilities to create an exploit with devastating impact on an important vulnerable system or database. The old priority list no longer reflects the real risk.

The good news: The same technology attackers use can work for you too. AI-driven tools can now prioritize patches based on real-world exploitability rather than static severity scores and flag anomalous activity at a speed no human team could match alone. Today’s defense doesn’t have to move slower than the attack.

For a private company with a small IT team, defensive AI is a massive force multiplier. Some companies are now deploying agentic security operations centers (SOCs). These are teams of AI digital analysts designed to handle specific, highly repetitive workflows, like tier 1 alert triage, threat intelligence and tool engineering. Working alongside human teams, these AI agents can instantly analyze traffic, flag anomalies, and isolate compromised devices in seconds.

Step
3

Pete’s take

“AI-discovered vulnerabilities are real; that part isn’t hype. But for a private company, the bigger problem is often velocity, not novelty. You’re still working through known vulnerabilities while attackers have sped up on every front. The novel attacks and the known threats now move at a speed you’ve never had to defend against.”

Pete Renneker, Managing Director, Risk & Financial Advisory, Deloitte & Touche LLP

4

5

1

2

3

Step
4

5

Close your *access gaps*

Controls like multifactor authentication (MFA) are table stakes at this point but implementing them in silos leaves organizations with a false sense of security. Private companies often deploy MFA on corporate email while leaving legacy servers, remote portals, and service accounts exposed.

Organizations should also curb access sprawl. In growing private companies

where people wear multiple hats, permissions quietly accumulate and rarely get revoked. While executives rarely hold IT admin passwords, their daily accounts often carry broad access to sensitive financial records, intellectual property (IP), and client data. Executive leaders should ask themselves: ***Do I really want to carry a target of that size in my pocket every day?*** The answer is likely “No.”

Scott's take

“In fast-growing private companies, people accumulate excessive permissions over time. Executive accounts in particular become targets simply because they hold broad access to data and IP they rarely need day to day. Implementing a least-privilege model alongside privileged access management (PAM) ensures that even if credentials are compromised, the attacker's blast radius is contained.”

Scott Staiton, Senior Manager, Strategy, Growth & Transformation, Deloitte & Touche LLP

1

2

3

4

Step
5

Practice makes *prudence*

Exercising is the most effective tool at your disposal. Gather your executive team and pressure test your response to a simulated crisis. These rehearsals expose operational gaps no software purchase could fix—because the failure point usually isn't your tech, it's your decision-making under pressure.

A wargaming session forces an executive team to work through these important decisions before a live adversary forces your hand. It surfaces the exact calls that tend to paralyze a business mid-breach, like who has explicit authority to shut down a revenue-generating platform to stop a virus from spreading.

Finally, be realistic about the clock. A severe attack isn't a 48-hour IT outage. Recovery routinely takes weeks, sometimes months, as you rebuild systems and verify your data is clean. Your business continuity plans should assume a disruption on that longer timescale, not a

best-case one. This is also where backups earn their keep, but only if you've tested them. A backup you've never restored from is a guess, not a plan.

For your most important systems, go beyond standard backups. Keep a clean, separate copy of your heartbeat data somewhere completely walled off from your main network, often called a cyber vault. That way, even if attackers get into everything else, that copy stays untouched. Rehearsal tells you who makes the calls during a breach. A tested vault and recovery plan tell you how fast you get back to business.

The five steps above are about changing how leadership thinks about resiliency. But strategy doesn't stick without action. Use the following list as your first-week homework. It features concrete tasks you can hand off and check off, no new budget required.

Scott's take

"Crisis response often fails at the most fundamental level: communication. If enterprise networks go down, your digital address book goes offline. Without preestablished alternative channels to connect important executives, legal counsel and partners, an organization's response can be paralyzed before it even begins."

Scott Staiton, Senior Manager, Strategy, Growth & Transformation, Deloitte & Touche LLP

The Monday morning *game plan*

Executive team

Draft a risk tolerance statement. Bring the executive team together to write a clear, one-page risk tolerance statement explicitly defining the level of operational disruption the business can afford to carry.

Chief operating officer

Map the heartbeat (MVC). Run a 90-minute session with finance, ops, sales and legal. Identify the two to three services required for basic survival and revenue generation and map the tech that supports them.

Operations lead

Elevate important suppliers. Identify which third-party vendors are connected to your mapped MVC services. Place those vendors at the very top of your security review list.

Executive team + IT lead

Audit executive access. Audit sensitive access and enforce least privilege. Identify who has access to high-value financial, customer and strategic data. Implement privileged access management (PAM) and data loss prevention (DLP) controls to restrict unnecessary exposure and contain the blast radius of any breach.

IT lead

Hunt for gaps. Locate any remote access portals, legacy databases, or service accounts that currently bypass your company's security policies. Set a strict 30-day deadline to close those gaps.

Operations lead

Develop crisis simulations. Design, schedule and lead tabletop exercises to rehearse and stress-test response plans.

IT lead

Test your backups. Confirm your company's most important data has a clean, isolated copy, not just a standard backup on the same network. Demand a restoration test to prove systems can be rebuilt and document the recovery timeline.

Completing these tasks can help position cyber resilience as a demonstrable business asset, one some organizations use to strengthen their standing in vendor, partner, or deal-related discussions—while supporting the durability of security posture over time.

Explore how to build structural cyber and operational resiliency within your private enterprise by reaching out to Tiffany, Pete or Scott, on the following page.

Endnotes

1. [Deloitte Private Family Business Cybersecurity Report](#), Deloitte Global / Deloitte Private, January 29, 2026, p. 4. Data based on a global survey of private and family enterprise leaders assessing cyber incident prevalence, operational disruption, and cyber maturity.

Contacts



Tiffany Kleemann

Managing Director, Cyber &
Strategy Risk Leader
Deloitte & Touche LLP
tkleemann@deloitte.com



Pete Renneker

Managing Director, Risk &
Financial Advisory
Deloitte & Touche LLP
prenneker@deloitte.com



Scott Staiton

Senior Manager, Strategy,
Growth & Transformation
Deloitte & Touche LLP
sstaiton@deloitte.com

Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (DTTL), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.