protiviti®
Global Business Consulting

GUIDE TO

Technology Modernisation & Transformation

Face the Future with Confidence®

Contents

Introduction

In today's rapidly evolving business world, the lines between technology and business have blurred. Organisations need to modernise and transform their technology in order to compete successfully.

One of the most significant long-term challenges organisations are addressing today is modernising technology and transforming their enterprises — from infrastructure to the use of cloud, to addressing and elevating their security measures, to enabling their workforce to operate on a mobile basis from anywhere possible. These challenges and the many changes underway in organisations worldwide are the basis of a recent blog series Protiviti published, titled the "Guide to Technology Modernisation and Transformation."

CIOs play a critical role in transforming the world of work using automation and technology — but they can't do it alone. Collaboration among the C-suite is critical. In this book, we offer a compilation of these blogs, each of which contains informative insights and practical tips that CIOs, CISOs, and other technology and C-suite leaders can leverage to initiate, implement and complete technology modernisation and transformation programs in their organisations.

Protiviti
September 2021

Future-Proof: Technology Solves for Business Value

At a Glance

Where technology was once a tool, it is now the path forward. Understanding the capabilities of technology such that it builds business value is key to business longevity. But endurance is not enough. Organisations must grow, but those that know how to sway with the evolution of technology while navigating its potholes can increase business value. To future-proof business growth, organisations should:

- Pivot and transform technology so that technology supports business growth
- Anticipate customer needs through agility, efficacy and efficiency
- Leapfrog to transform from outdated models to more effective approaches
- Implement new technology for enterprise transformation with an understanding of the associated responsibilities of data governance, ownership and validity
- Lean on CIOs as technology stewards to support growth while mitigating disruption

---

Business and technology were once seen as separate or distinct, but today they are deeply intertwined. In fact, the days of task-driven technology have vanished. Instead, using technology as a vehicle for business growth is the future. IT departments are no longer a separate function of a business; they are a way of doing business. Organisations must leverage technology to solve for business value or understand that business longevity will suffer.

While enterprise transformation is driven by customer and business needs, technology can be the catalyst for large transformational change.

Look up, frequently

Pivoting and transforming the organisation to remain relevant is a continuous mission for C-suite executives. Along that transformation journey, they must navigate:

- Competitive pressures
- Evolving customer and workforce expectations that force businesses to operate at faster speeds
- Disruptive crises such as global pandemics
- Dynamic regulatory demands

Today's business environment commands that business leaders continually look up from their daily business demands and ask, "How has the world changed — *today*? What will the next transformation require?"

For an organisation to remain viable, its opportunities and challenges must be met with an intimate partnership between business and technology.

Change demands agility, efficacy and efficiency

Previous IT planning asked, "What is an organisation's five-year IT roadmap?" Today's IT planning asks, "What is an organisation's five-day IT roadmap?" — a clear evolution of the rapid pace of business today, particularly given the business requirements created by the COVID-19 pandemic. However, while the pandemic has been and still is massively disruptive, it did not necessarily change the trajectory of today's business climate. It only accelerated it.

Customers want touchless interaction. They want speed and they want businesses to anticipate their needs. They do not want to search for products and services. Like Uber, consumers want to open an app, hit a button, and have a car show up. These heightened customer expectations pervade into all companies, whether or not a company can move at that pace or has anything to do with Uber. This is the new reality and expectation of an end-customer or employee.

Technology is constantly evolving and advancing. With the availability of low-code and no-code technology, some business units are moving away from relying on IT and are hiring contractors or implementing their own systems without involving IT. CIOs must create partnerships rather than acting as gatekeepers and must assume the role of transformation agent so they are proactively addressing business challenges — not just technology issues.

From disruption to leapfrog

Disruption offers organisations the opportunity to leapfrog — to transform from an outdated model to an approach that is more effective.

For example, the pandemic precluded employees from being physically present at customer sites. How did organisations respond to hybrid and remote working arrangements? Did they continue to provide customers with the experience they expected? Or were customers left searching for a more valuable experience — with another provider?

While organisations have an opportunity to leapfrog to remote or hybrid workplaces during disruption, they must also look to practical implementation:

- Can employees be provided with efficient and effective tools to interact?
- How will training, mentoring and managing employees be deployed? Can new approaches be effective?
- Can staff be retooled? If not, how can new teams (in various time zones) be efficiently sourced and built?

Effective leaders pivot and deploy the right technologies to solve for business needs. They focus on the things that offer collaboration and agility, such as online voting technology and collaboration tools for data visualisation, in addition to augmented reality capabilities like Microsoft HoloLens. They not only make up ground that was lost by being remote, but they advance it forward. They leapfrog.

For business leaders to tap into technological capability, CIOs must have direct visibility into the business problem or the opportunity and share the art of the possible with business executives. On the flip side, business leaders must provide CIOs with a seat at the "business opportunities and challenges table." Doing so enables CIOs to create solutions that offer competitive advantages and solutions for enterprise growth.

The benefits of enterprise transformation

The benefits that organisations can expect to receive from leveraging technology for enterprise transformation include:

- Increased revenue and enterprise value
- Increased market share and heightened market presence
- Environmental, social and corporate governance goodwill — customers want to do business with organisations that align with their values
- Geographically diverse employees with different perspectives that enrich the customer experience
- Health and safety improvements such as using predictive analytics to prevent accidents or employing Internet of Things (IoT)-based technology to improve workplace sanitation

Transformation brings responsibility

Implementing new technology for enterprise transformation brings increased responsibility to ensure the organisation and its customers are protected from emerging risks associated with that new technology. For example, while IoT devices offer advantages, many do not have built-in security and privacy features. Therefore, the organisation is burdened with ensuring that data collected from such devices is being used, shared and protected properly. Data governance, ownership and validity issues rise to the surface and must be addressed.

Similarly, organisations have a responsibility to their shareholders to allocate and expend capital wisely so as not to overbudget, underutilise or suboptimise technology.

Enterprise transformation frequently requires behavioural change. Organisations are responsible for creating the space for change in order to generate such behaviour. While training is important to transformation, it is only a facet of the transformation journey. Proper communication and messaging are also critical.

To be effective, it is important that companies implement transformation governance and enablement, and perhaps devote resources to forming a transformation function that manages the complexities of enterprise transformation, including:

- Upskilling the workforce or customers for modernised technology
- Securing proper talent
- Ensuring that all change-makers are incentivised in a way that is aligned with a shared goal
- Leveraging the expertise of internal audit to manage transformation risk

The way forward

Technology can be a double-edged sword. Organisations must use it to improve business value or risk having it used against them by their competitors. CIOs are instrumental stewards of technology — they are in a prime position to influence growth and mitigate disruption by ensuring that business and technology intersect effectively. Accordingly, they must act as agents of enterprise transformation rather than merely implementers of technology.

The emphasis on the interconnectivity of technology and business cannot be overstated. Deep interconnectivity drives growth by enriching the customer experience. How important is the customer experience? According to this article in Forbes, "Brands with superior customer experience bring in 5.7 times more revenue than competitors that lag in customer experience." Improving customer experience across the enterprise requires transformation, and the collaboration between business and technology is a key success factor.

AUTHORS

JASON BRUCKER, Managing Director, Technology Strategy and Operations, Denver
SCOTT LALIBERTE, Managing Director, Global Leader, Emerging Technology Solutions, Philadelphia
JOAN SMITH, Managing Director, Digital Solutions, Phoenix

Implement Balanced Governance to Reduce Risk of Enterprise Transformation Failure

At a Glance

All organisations must transform digitally or face irrelevance. While enterprise transformation can bring growth, it can result in failure if improperly implemented. Spiraling costs, diminished employee morale and unmet goals become reality. Businesses must focus on the factors that can make or break their transformation efforts. To increase the chances for a successful transformation, companies should:

- Ensure that governance accommodates a feedback loop into decision-making for changes in risk
- Implement an effective governance structure that creates alignment back to what the business needs
- Align the right resources and establish a structure of clear roles and responsibilities, with accountability
- Align individual project team goals with the benefits of overall transformation
- Define a clear path for actionable, effective decision-making with performance that is measured and managed
- Ensure that both the budget and planning have adequate focus on evaluating and measuring end results to ensure that planned benefits and KPIs have been achieved

More than half of companies undergoing a transformation project ***fail in the initial phase.*** *And with this failure, organisations only partially achieve the value that should come from transformation — and they can experience overwhelming frustration that transcends the organisation.*

For a company to be successful, it must implement a governance program that is aligned with business goals — with a laser-like focus on achieving value while balancing risk. Ultimately, a governance command center — the central nervous system of enterprise transformation — is integral to arriving at targeted value.

Defining value but ignoring risk is disastrous governance

Dynamic governance is on a value and risk continuum. Transformation management offices (TMOs) can be more successful by having open conversations about risk. Risk does not simply go away if ignored; on the contrary, risk grows and permeates and causes even more damage over time. TMOs with a governance structure that

accommodates a feedback loop into decision-making for changes in risk can overcome and minimise impact to the value the enterprise transformation is meant to deliver. Additionally, executive leadership must recognise the role of Enterprise Risk and Internal Audit in assessing risk independently and providing effective challenge for balanced governance.

To begin, organisations must:

- Understand and define the value of transformation and the associated risks
- Understand the impact to transformation value if not remediated
- Drive risk mitigation
- Measure performance against value criteria and risk appetite to ensure transformation is being achieved

Go beyond basic — implement next-level governance

An effective governance structure creates alignment back to enterprise stakeholders' and customers' needs. There must be purposeful focus and organisation-wide alignment on achieving the benefits of transformation, finding the union of different executives to align on vision, value and managing risk, and tying it all back to cross-functional alignment. This eliminates silos by focusing on how the value is delivered across the organisation's functional boundaries.

Experienced TMOs go beyond the basics of developing project plans and tracking progress — however, they must fulfill these responsibilities too. They implement next-level governance, owning the desired results, balanced with evaluating associated risks. How do organisations arrive at next-level governance? Creating good project- and program-level plans and mapping a critical path to transformation is not enough; these are not the decisive factors for success. Executive meetings must go from information-sharing and status presentations to driving decisions, committing to actions and enforcing accountability.

To have next-level governance, it is important to think differently about governance and understand that it's not just about control. Governance is about *tying it all together.* It is about value, decisions, guidance, risk and understanding resourcing. It is about plan completeness and understanding dependencies — and the methodologies at play. For instance, regardless of whether Agile, waterfall or hybrid approaches are used, there will be complex dependencies. It is critical that the stage gates are defined and certain criteria are addressed. TMOs have an opportunity to rise above the transformation dust by understanding how all pieces fit together to provide a critical path that is transparent and comprehensive — one that establishes effective and efficient workflow to achieve goals regardless of approach.

When complex dependencies are not sufficiently addressed, completeness, accuracy, velocity and effectiveness suffer. For example, a transformation program team that pushes out the end date of development can create an overlap with validation phases like system, integration and user acceptance testing (SIT and UAT). If development is ongoing during these validation phases, the overlap will make it much more challenging to ensure the completeness and accuracy of the testing due to potential changes in the underlying technology. That's not to say you can't be somewhat flexible — rigidity with either waterfall or Agile reveals weakness in the program management and governance approach. But ongoing analysis of phase-gating criteria paired with focused discussions of risks as part of the ongoing governance approach can help organisations make better informed and intentional decisions on the balance between flexibility and adverse business outcomes.

Many factors to resource sufficiency

A key element to effective governance is having a TMO that establishes clear roles and responsibilities, along with accountability. Roles and responsibilities should be inclusive of all key stakeholders on the program, from the TMO and core project team members to key business and technology owners, vendors and system integration partners — and last, but no less important, leadership comprising the program governance functions. Questions to consider include whether the organisation has:

- Aligned the right resources and skills to be successful
- Determined the risks and impacts to achieving defined value
- Created a transformation command center equipped to establish the reality of the transformation in a way that is aligned across various project teams while solving for capacity and resource constraints (people, time and budget)
- Identified all program tasks and dependencies to ensure comprehensive management; while this is not directly resource-oriented, if we miss an upstream effort and fail to engage that team (and hold them to account), the project is at risk

See the forest through the trees

Successful TMOs align individual project team goals with the benefits of overall transformation. For instance, a scenario where the system integrator believes their team is on par — while the business has serious resource shortfalls and unaddressed dependencies — does not have transformation alignment.

While teams engaged on complex programs can be effective at individually managing themselves, the crossroads are determined by how the teams intersect on an aggregate approach. TMOs solve for this challenge. There is a recognition that while it is one thing to manage a team of six, 10 or 20 people, it is another thing entirely to manage a team of hundreds who must all achieve a common goal, thus requiring elevated program management and governance.

Team dependencies, as well as activities and goals of each program team, must be knitted together and aligned with transformation value. The TMO must ensure that decision-making at the team level is not decreasing the value proposition of the overall program.

Performance management

Successful governance structures have a clear path for actionable, effective decision-making, born from performance that is properly measured and managed. For each objective, the right metrics and basis for measurement should be developed for each work stream. Regular, transparent updates on performance and the delivery of value should be presented throughout the project life cycle to provide insight into the progression of that work vs. targets. A few examples include:

- **Data Conversion** — should measure conversion-specific metrics for each data object being converted (e.g., time to convert, fallout/error percentages, etc.)
- **SIT** — should measure testing progression against functional requirement points, as well as incidence of issues by severity
- **UAT** — should measure testing progression against end-to-end business process scenario outcomes, not just the same functional points as SIT (e.g., order initiated through cash received as a transaction scenario), as well as incidence of issues by severity

Reap — and measure — the benefits

One of the most overlooked aspects from a governance perspective is the realisation and measurement of results and value, which are often tracked with overall transformation KPIs. Transformation teams often focus on planning and setting budgets around the transformation project itself, without allowing for the review and measurement of end results. It's not uncommon for transformation teams, once the project is completed, to hand over delivery to the functional or technology stakeholders and either leave the organisation or return to their business-as-usual roles. Planning — and budget — to measure the end results is often overlooked. A successful governance program should ensure that there is adequate focus on evaluating and measuring the end results to ensure that the planned benefits and KPIs have been achieved.

Transformation value is achieved by successfully managing the execution of the program across all workstreams and effectively managing against risk and value criteria, recognising that risk mitigation is a key enabler activity to unlocking transformation value. Over time, balanced governance evolves and adapts by leveraging on a transformation command center. Effective governance helps enable this critical balance. Starting with governance in mind and adapting throughout the transformation will enable the program to be a success.

AUTHORS

SAM BASSETT, Managing Director, Technology Consulting, Singapore
JASON BRUCKER, Managing Director, Technology Strategy and Operations, Denver
TOM MCKERNAN, Associate Director, Technology Strategy and Operations, Chicago

Lasting Transformation Requires Solution Design Disciplines

At a Glance

To achieve truly transformative impacts, organisations and IT executives must embrace Solution Design disciplines to:

- Align technology decision-making with strategic business vision
- Listen and respond to the voice of the external customer to shape transformation priorities
- Enlist internal customers to drive operational improvements
- Conduct a regular and candid evaluation of systems, skill sets and service providers
- Establish an architecture review board to maintain a comprehensive solution design

In the same way that marathons require rigorous preparation to reach the finish line, technological transformations will not yield lasting rewards without vision, planning, dedicated resources and unwavering determination. When organisations do not embrace digital transformation, failure ensues — enterprise value suffers, employee fatigue becomes rampant, customer experience is negatively impacted, and time is lost. To remain relevant, organisations must regularly reevaluate and optimise technology solutions to relentlessly pursue current business outcomes and enterprise value.

Strategic vision must drive decision-making

Transformation requires decision-making that is firmly anchored in the organisation's strategic vision. Successful chief information officers (CIOs) and chief technology officers (CTOs) align technology solutions with the organisation's business plan. They consistently lean on updated three- to five-year strategic vision plans to guide data and technology choices that maximise value and support business objectives. Their decision-making considers the status of the organisation's strategic vision, including whether the organisation is focused on:

- Aggressive growth
- Cost reduction and efficiency
- Employee morale and engagement

To have a strong pulse on business plans, technology executives must have a prominent role at the C-suite table. Next-level business leaders ensure the IT executive's voice is respected and leveraged in defining corporate vision. On the flip side, savvy CIOs and CTOs understand the opportunities and challenges within other C-suite functions. Smart IT departments do not function in an operational silo nor dictate technical strategy to the organisation — rather they enlighten and inspire business leaders about technology to encourage adaptability to the potential of emerging technology. When executives are regularly engaged and informed, they become true partners in a digital transformation focused on a unified vision.

External customer experience is paramount

Revenue drives valuations — and the external customer experience is at the helm of sales growth, particularly in our modern hyperconnected world. Technology has become an essential ingredient in influencing customer perceptions of product value and interactions with the organisation. However, there are so many potential areas of focus and so many technologies that could be brought to bear that prioritisation of limited investments is essential. The voice of the external customer and the key moments that matter in an experience should be a driving force in determining modernisation and transformation priorities.

Organisations must seek out and understand their customers' expectations, as well as the desired experience for interacting with the organisation. Additionally, organisations should prioritise investments in technology based on data-driven insights into threats and opportunities that align with current strategic customer goals (i.e., market share, revenue per customer, brand awareness). Organisations should work toward near real-time analytics for metrics such as transaction speed, order size and repeat customers in order to enable accurate decision-making around potential experience friction points. These may proactively indicate circumstances of perceived inefficient customer service or a lower degree of product choice compared to competitors, or conversely may highlight pockets of strength to expand. Hindrances must be identified, analysed for root cause and potentially solutioned through technology optimisation or acquisition.

Internal customers should drive operational transformations

While external customers drive revenue, internal customers drive operations and ultimately profitability — so they are equally integral. IT should likewise solicit candid and regular feedback from internal customers, including sales, finance, human resources and the supply chain regarding insight into the obstacles or inefficiencies that impede operations. Treating other departments as customers of IT enables a partnership that is synergistic and collaborative — and seeks to illuminate opportunities for departments to perform their jobs in ways that they never thought possible. Often there are cases where repetitive tasks can be automated through tools, enhancing quality and efficiency.

But the real opportunity is for IT to change the game for internal customers. IT can approach users with a message of, "I understand that is the process you've been following — but what if you don't have to handle that piece in the future? What if we implement a new feature or integration or cloud product that can eliminate that step altogether so you can focus on higher-level work?" A laundry list of possibilities will start to emerge that can be prioritised based on time and/or expenditures saved weighed against investment.

To know the path forward, take inventory

Successful technology executives regularly scan external trends and technology advances as well as external and internal customer voices to formulate plans to add value to the organisation and its strategic goals. These opportunities should be weighed in the context of the

current inventory of technology. With the proliferation of cloud-based applications readily sourced by any department with funding, it is helpful to conduct a routine technology inventory and assessment. Ideally this can be performed across the enterprise with a candid evaluation to confirm whether the organisation has the best portfolio of solutions, skill sets and service providers to transform.

Assessing the company's inventory of technology involves looking at the current managed application portfolio combined with a survey or review of external technology providers for completeness. Each technology should be evaluated for its fit for current needs, overlap or duplication, licensing sizing, dependencies on other systems, vendor roadmap and sunset plans. This exercise creates a conversation that reconfirms fit, considers upgrades or enhancements, identifies third-party risks and integrates planning towards the transformation goals of the company.

Solution Architecture Review Boards offer connected transformation

Harmonising the varied and constantly changing technology elements in an organisation requires a holistic perspective and guiding principles to maintain focus on the core vision and key priorities. One method to ensure that technology components and investments are compatible with the strategy-driven transformation environment is to form an Architecture Review Board (ARB). Designating business-minded technology architects who regularly engage with executives to evaluate new technology decisions enables the continual advancement of a connected and comprehensive solution design and avoidance of disruptive or distracting technology. This focus is more important than ever with the proliferation of distributed data, applications, channels and integrations that must work together. To promote comprehensive, communicative, and transparent transformations, ARBs can:

- Serve as the connective tissue that brings diverse and heterogeneous products into a common overarching solution design
- Ensure that all technology components and communication channels are integrating in a way that provides external and internal customers with a seamless experience
- Connect technology in a way that offers accurate data that is void of duplication and inconsistencies
- Prioritise investments towards business value
- Consider implications of risk, compliance and regulatory burdens

All drivers — including customer, process, technical and risk — must be considered in maintaining a high-performing organisation's solution design. The portfolio of systems must be regularly tuned for maximum value while also advancing the organisation's strategic vision. Ultimately, organisations must continually adapt and solve for business problems and opportunities by incorporating the right technology at the right time and in the right way.

AUTHOR

JOHN HARRISON, Managing Director, Enterprise Application Solutions, Houston

Leverage the Cloud to Modernise Your Technology and Enable Business Goals

At a Glance

Organisations undergoing technology modernisation can leverage the cloud to attain business goals. Solving for business value requires organisations to optimise cloud infrastructure and apply the following key actions:

- Transform data processes
- Address people considerations
- Build compliance along each step of the transformation journey
- Optimise costs
- Streamline complexity

Is your organisation modernising its technology by leveraging the cloud to gain new sources of revenue, optimise supply chains, reduce costs and increase market share? Successful organisations do not merely move traditional data to cloud platforms to have better data access — they shift to the cloud by thinking differently, using the cloud as a tool to achieve business goals by implementing a strong cloud infrastructure.

Cloud has evolved to become a key enabler for organisations to develop, grow and compete in today's marketplace. Executives should collaborate and communicate to enable a different, more valuable version of the enterprise and understand how cloud underpins this vision. Cloud can bring speed, agility, resilience and visibility. But taking on too much at once or not following a tried and tested model with clear foundations for successful consumption of cloud can result in analysis paralysis and questions from the business on whether cloud is a true enabler. Organisations may find it helpful to execute a multi-stage migration rather than undertaking a comprehensive re-architecture. An incremental approach to cloud adoption affords a company time to refine the approach and effectively demonstrate progress and benefits.

Shed what no longer propels you

Transforming data processes is critical to capitalising on technology modernisation. Organisations should not rely on old tools, such as using Excel spreadsheets for change management, when there are many highly effective cloud-based tools that enable a more efficient, effective and consistent way forward. Existing processes must be abandoned to the extent they are holding the company back from achieving grander goals.

Take your people along on the ride

Enterprise transformation demands change management and navigating skillset considerations such as training so that employees can operate with confidence and evolve with your business. Companies should ensure they are bringing their people along on the transformation journey. As processes and technology change, employees should be trained so skillsets align with new approaches. To maximise ROI, organisations must think innovatively by adopting new practices like Agile for work effort management and DevOps for rapid provisioning of business solutions into the cloud.

Compliance is not an afterthought

Compliance and security should be built by design and integrated into cloud solutions to enable better and safer consumption and to leverage the innovative nature of cloud services within your organisation. Automation affords different approaches to achieving compliance. Cloud deployment can be automatically driven, with entities spinning up numerous new systems while incorporating security and compliance along the way. Cloud-native paradigms such as DevSecOps can simultaneously incorporate compliance into deployments. In comparison, traditional controls scan for vulnerabilities and apply patches at endpoints in time. This can put organisations at risk during patch deployment and leave them blind with no insight — unless they automate compliance controls.

Watch costs

It is easy to acquire technology that exceeds needs or requirements — and it is even easier to forget to turn technology off when it is underutilised. Insufficient control on technology expanse results in excessive and unnecessary costs, so it is important to ensure that costs are well-managed and substantiated. Cloud, finance and procurement teams should work together to weigh cloud costs against benefits. FinOps can bring financial accountability to the variable costs of cloud infrastructure, helping organisations have a pulse on the financial health of their cloud environment.

Complexity can crush clarity

Uncontrolled complexity causes chaos. An in-depth understanding of the current cloud environment is essential as it facilitates subsequent modernisation later down the line — as compared to the complexity of trying to understand the data environment along the journey. Companies should not overcomplicate deployment simply to use new cloud technologies. Working with the Cloud Service Provider (CSP) and partners, organisations should aim to use the consumption of cloud to reduce complexity and define this as a target of transformation.

Have a 360° C-suite

Effective cloud that aligns with business strategies comes from C-suite executives who communicate early and collaborate often. C-suite executives who understand how cloud infrastructure enables their business goals have a greater likelihood of achieving those goals. All members of the team must come with an understanding and alignment towards a common business case. It is then that all aspects of cloud are addressed, including cost, security, complexity, people and process. For example, having CFO buy-in early to support upfront investment is essential. Likewise, ensuring the chief data officer (CDO) and chief marketing officer (CMO) collaborate on how the cloud infrastructure supports the business case is critical to achieving revenue results. When communication and collaboration are lacking, conflicting scenarios develop — although revenue may increase, risk also may be higher. A growing concern among clients is the movement of more production workloads to the cloud. Production workloads with sensitive data require having compliance in place, now more important than ever.

Engaging the C-suite about departmental challenges and opportunities uncovers gems of insight that can be used to improve efficiency or increase value in departments outside of IT. Effective CIOs continuously ask, "How can I be a better partner?" While communicating early and often is key for all members of the C-suite, there are some issues that are important for certain executives to be aware of, including:

- **Chief financial officer (CFO)** — While consuming the cloud is easier across the organisation, a lack of control can allow costs to spiral. Implementing controls ahead of time can save money and provide greater oversight. The impact of infrastructure changing from CapEx to a consumption-driven OpEx model should be analysed and understood.
- **Chief risk officer (CRO)/chief compliance officer (CCO)** — Understanding the differences in how CROs and CCOs control risk is important due to the shift from interim approvals to DevOps automation. A combination of learning and incorporating appropriate checks into automation processes is important.
- **Chief audit executive (CAE)** — With the automation that cloud infrastructure brings, controls become codified where they were previously in easy-to-comprehend word documents. To address codification, auditors must acquire the proper training to understand and read code and provide assurance on the proper design and operation of automation.
- **Chief data officer (CDO)** — Knowing data location and cost is key. Having newer and more effective tools brings a need to understand associated risks. As data size grows, risk complexity increases, making it more important to manage the volume of data and the controls and compliance around that data.
- **Chief marketing officer (CMO)** — Cloud can enable a holistic user experience across end points so that services integrate with call centers, mobile apps, home assistant devices and other access points. This affords richer data to elevate enterprise offerings that are delivered to consumers.

Last but not least, business leaders and employees are the beneficiaries of a solid cloud infrastructure, as the end result is increased speed and delivery from enterprise to client.

Where do companies go from here?

An organisation's phase in its transformation journey determines next steps. Entities at the beginning of their cloud adoption journey should plan, analyse their current environment, assess their workforce and determine and augment skillsets. Entities further along in the cloud journey should look for ongoing optimisation opportunities and continuous improvement. Lastly, enterprises approaching completion of cloud transformation should solidify benefits in accordance with those defined in the cloud transformation business plan.

AUTHORS

RANDY ARMKNECHT, Managing Director, Cloud Solutions, Chicago
DAVID KISSANE, Managing Director, Technology Consulting, Sydney
JAMES FOX, Director, Cloud Solutions, West End (UK)

Emerging Technologies: Creating New Ways to Solve Business Problems

At a Glance

Emerging technology can enable enterprise goals — but only if properly implemented. To achieve smart implementation, companies should:

- Automate processes
- Enrich data
- Visualise data and analytics
- Innovate to reach new capabilities
- Ensure early and frequent collaboration between the CIO and the C-suite

In today's transformative business environment, emerging technology has a decisive role to play in an organisation's innovations, customer experience and overall success. On one hand, business leaders have the greatest insight about the organisation's needs and objectives, and likely have new ideas on how to achieve those objectives. On the other hand, the CIO has the greatest knowledge of what is possible — along with an understanding of emerging technologies and how they can be used.

Emerging technologies such as artificial intelligence (AI), machine learning (ML), augmented reality (AR) and Internet of Things (IoT) can help organisations scale on demand, improve resiliency, minimise infrastructure investments, and deploy solutions rapidly and securely. Potentially disruptive emerging technologies such as quantum computing threaten to revolutionise many industries, as well as pose significant risks businesses must manage in the coming years. More importantly, these technologies can help companies create powerful transformations within the organisation that can drive additional revenue and set it apart from the competition.

Combining the insights of the business leaders with the technical knowledge and expertise of the CIO leads to synergistic decision-making that differentiates organisations and brings prized marketplace disruption.

CIOs must learn to think differently by applying technology solutions to solve *business* challenges. However, they must be enabled by organisational cultures that support innovation and governance functions that facilitate the partnership between the CIO and business executives.

Investment in emerging technology is not just a risk/reward assessment — it is an investment/return

decision. This is because some ROI may not be directly quantifiable, such as increases in goodwill or brand recognition. Companies that quickly uplifted their technology in response to the COVID-19 pandemic were far more resilient than others, specifically in the form of an enabled workforce and more efficient customer experience through digital channels. Soliciting input from all members of the C-suite is important for a holistic, comprehensive business case. In addition, it is important that organisations recognise ROI may be a long-term play, as short-term ROI may not reflect the full potential a technology brings. However, whether short- or long-term, emerging technology brings risks that must be identified and mitigated. Companies should focus on value creation and risk mitigation in equal measure.

Automate where possible

Existing processes should be assessed to determine current building blocks. Then, to the extent financially feasible, organisations should identify repeatable processes that are performed often, as they are ideal candidates for hyperautomation, which applies advanced technologies such as artificial intelligence (AI) and machine learning (ML) with robotic process automation (RPA) to increasingly automate processes. Mundane tasks that do not result in skills growth and are not rewarding to employees can be performed by machines so that staff can focus on higher-level, more rewarding tasks. For example, machine learning can be applied to automate tasks that are repetitive, labour-intensive, and require numerous hours to perform. By using data to implement and improve data processes, organisations can take advantage of the rapidly evolving field of machine learning to gain significant ROI.

Enrich to empower

Business decisions should be powered by enriched data. It is important that organisations understand the data that is available to them — and they must filter and organise it in formats that can be used for further analytics. Strong data analytics enables smarter business decisions.

Data is growing exponentially. By 2026, one trillion Internet of Things (IoT) devices will be in use. Each device generates endless data on demographics, purchasing decisions and profiles. To take advantage of the flood of data, organisations that harness data and enrich it to make smart business decisions can gain competitive advantage through improved operations and personalised customer experiences. Those that do not may face competitive pressures that pose threats to continuing operations.

Visualise for value

Visualisation technology makes data more meaningful to businesses by allowing for more profound ways of presenting data and ideating strategies. For example, augmented reality (AR) can help improve decision-making by bridging physical and logical worlds and has the potential to revolutionise different industries and functions. Organisations can level-up data visualisation by applying AR to make data visually available in near real-time while AR provides real-time feedback to staff who must make difficult, instant decisions based on the information they have on hand. For example, a field technician working on a piece of equipment in a tight, remote space could have instructions or diagrams in their view while working on the equipment with both hands.

Innovation may require long-term investment

The capacity for innovation is contingent on foresight. CIOs have the potential to expand the realm of the possible for their organisations. They must think of new ways to leverage emerging technology for efficiency, competitive advantage or market share. However, there must be a recognition among C-suite members that while CIOs can implement life- and business-changing technologies, some tools require long-term investment.

For example, in the next three to five years, quantum computing is going to begin having an astounding impact on business processes and will require businesses to think differently about challenges and how they can go about solving them. Quantum computing will enable organisations to have exponential increases in computing capability and will make it possible to solve problems that cannot be solved today. But, just as with other emerging technologies, long-term planning and workforce training are required.

Collaborate early and often

CIOs must collaborate early and often with all constituents inside and outside the C-suite. Each C-suite member must freely bring a unique skillset to form a high-functioning team with accountability. While all C-suite members work toward common business goals, there will be issues that are of particular importance to each, including:

- **Chief financial officer (CFO)** — Emerging technology presents difficult investment decisions that can result in runaway costs. Preemptively implementing controls can save money by reining in expenses.
- **Chief risk officer (CRO)** — Emerging technology brings new risks. It is critical that CROs identify and mitigate new risks to minimise impact on ROI.
- **Chief audit executive (CAE)** — New technology requires updated skillsets. Staff with the requisite training is essential to auditing new technology and ensuring it is operating as intended. CAEs should also realise the importance of refreshing the risk profile regularly — along with internal audit plans —to cover emerging technology risks. For example, companies with RPA should conduct an internal audit on the process taken to govern, implement and control RPA.
- **Chief data officer (CDO)** — Enabling emerging technology for the organisation is largely dependent on the CDO. Close collaboration and alignment between the CDO and CIO are key.
- **Chief marketing officer (CMO)** — Ensuring that the CIO and CDO have a strong understanding of the customer experience is critical to the value brought by emerging technology. CMOs enable this understanding.

Where do companies go from here?

While emerging technology surfaces many factors to consider, it is important that organisations ensure the following actions are taken in their technology enablement journeys:

- Leverage existing assets by assessing current technology and using current building blocks such as data sources, technology and talent
- Set a foundational understanding among the C-suite about how the business will transform and how it will get there
- Have a framework that facilitates engagement between the CIO and business leaders so that CIOs understand business goals and the desired customer experience
- Develop a culture fostered around change enablement so that employees are open to change. Forward-thinking organisations embrace employee empowerment and develop training programs to provide new skills for more rewarding careers as the organisation modernises, helping employees feel safe from the real or perceived job security threat from automation
- Swiftly qualify what is of value to the organisation and what is a fad

When properly implemented, emerging technologies can be powerful in helping companies solve business problems, scale on demand, improve resiliency and deploy technology solutions rapidly and securely. Companies should conduct a digital maturity assessment and determine areas where emerging technology could provide the greatest value or enable the organisation to deliver on its strategies with greater certainty or at a faster pace. It's also critical to have effective change management during the transition, otherwise any technology program will never truly reap the intended benefits. The most successful CIOs of the future will be those who seamlessly provide optimal customer and employee experiences while enabling business innovation.

AUTHORS

GHISLAINE ENTWISLE, Managing Director, Technology Consulting, Melbourne (AU)
SCOTT LALIBERTE, Managing Director, Global Leader, Emerging Technology Solutions, Philadelphia

Bolster Application Security and Internal Controls Compliance with Design-In Processes and Automation

At a Glance

Security and control compliance can safeguard an entity's digital assets during enterprise transformation. To achieve success, companies should:

- Use a process-oriented approach that is end-to-end
- Engage with business leaders and applying change management strategies
- Align security with business goals
- Have the right resources in place
- Collaborate with business leaders and essential stakeholders
- Approach security holistically

Business process controls and application security are not just valuable for organisations looking to transform to a modernised state — they are critical. As technology becomes increasingly pervasive, the complexity of the information technology (IT) and digital landscape is growing exponentially. Regulatory requirements and the constant news regarding the latest security and data breach of a high-profile company are increasing the pressure on IT resources to provide evidence of security measures taken during large transformation initiatives. And, as a result, many executives are now adopting, more than ever before, a design-in approach to application security and internal controls.

Today's technologies for application security and internal controls optimisation allow for deeper automation of testing processes while being fully integrated across the technology environment. Manual controls may no longer be effective or sustainable. Automating security brings return on investment (ROI) by protecting digital assets while increasing efficiency and reducing the burden on IT departments. Effective CIOs heighten ROI by defining the parameters for success while considering and mitigating risk to avoid penalties and prevent fraud or other repercussions. They apply a forward-thinking approach to avert unnecessary costs and complications, and they partner with business leaders to accomplish their goals rather than using a siloed implementation approach.

Experienced CIOs incorporate controls and security *along* the transformation and modernisation journey rather than tacking it on the back end of the program. Why? Because a *design-in* approach improves ROI. It addresses all necessary controls by focusing on automation and incorporating continuous controls monitoring and assessments. Incorporating a design-in approach to technology modernisation projects lowers remediation costs

after systems are live. It brings peace of mind to external auditors and facilitates the company's ability to maintain and sustain secure systems. While design-in costs may be higher in the short term, the costs of remediating poor security and compliance concerns far outweigh the near-term investment of a design-in approach.

Use a process-oriented approach

Process-oriented approaches offer end-to-end attention while bringing automation, efficiency and more comprehensive security. Leveraging tools that elevate access monitoring (such as segregation of duties and sensitive access) as well as IT process automation (including user provisioning and annual recertifications) facilitates the efficiency organisations need. Technology transformation is more successful when tools are used to address compliance and IT process automation. Artificial intelligence (AI) and machine learning (ML) technologies allow companies to create and implement complex use cases that can make it possible to detect fraud scenarios. And intelligent process automation (IPA) solutions allow companies to automate legacy technologies with relatively low effort. Far from being one-use-case assets, these tools transform inefficient activities across core IT processes through continuous monitoring and automation.

Adopt engagement and change management strategies

Experienced CIOs recognise that transformation projects are not purely technical. They know that engaging with business leaders early and throughout deployment leads to effective implementation and user adoption. Key players such as audit, risk and compliance groups who have a seat at the IT think-tank table are particularly important to the adoption of security and controls compliance.

Change management and enablement can compound adoption success. IT can enable change management initiatives by working across the organisation to help address risk ownership, training, behaviour and culture.

Bolster security with vested stakeholders

CIOs must go beyond involving business leaders in the transformation. They must collaborate with other essential stakeholders regardless of level. Collaboration builds buy-in and facilitates engagement in the preparation and execution of testing and signoffs. Vested stakeholders validate that data is complete and accurate from a business perspective. Engaging stakeholders is paramount regardless of the transformation strategy.

Dedicate resources — it is a must, not a luxury

Having a dedicated workstream is core to the ownership of security and compliance efforts. Where it was previously an afterthought, it is now a necessity. Rather than addressing issues after the fact and after damage has been done, forward-thinking CIOs are preemptively and formally dedicating resources to security and controls workstreams.

Collaborative understanding brings results

When addressing security and controls compliance integration, successful CIOs:

- Have an effective steering committee
- Apply a clear understanding of the audit committee's priorities
- Outline KPIs as part of the governance process
- Evaluate business leader requirements for success
- Apply reporting and analytics as tools to achieve goals

Approach security and controls holistically

Addressing security *holistically* is fundamental. CIOs must consider the complete portfolio of security and controls when tackling enterprise transformations. In fact, a holistic approach to security might have mitigated the damage suffered by companies who fell victim to more than 281,000 data breaches since the GDPR legislation went into effect in mid-2018.

However, enterprise transformation cannot be successful using a one-size-fits-all approach — rather, it involves thoughtful consideration of security issues beyond common topics. It needs more than siloed consideration of identity access management and cyber breaches. It requires comprehensive consideration of the complete portfolio of security and controls. A holistic approach may include questions such as:

- What broader security measures must be taken across all layers of the digital landscape (e.g., databases, servers and operating systems, networks and storage, backups and disaster recovery operations, etc.)?
- What is the impact to data security and privacy during transformation deployment?
- Where does personal information reside in the future state?
- How are regulatory requirements being handled to prevent breach-related fines?
- What are the automation opportunities related to controls compliance and business process optimisation?

Impact on the C-suite

CIOs have the opportunity to serve as digital enablers and thought leaders. They understand how security and controls can support business goals to build value. The right involvement of key C-suite leaders and global process owners is essential to achieving technology alignment with organisational goals. Certain unique issues relevant to the C-suite as they pertain to security and internal controls compliance include:

- **Chief financial officer (CFO) and business leaders** — Alignment with business priorities is paramount, therefore collaboration with C-suite leaders for input on IT efforts is essential. Business leaders must consider the entirety of what the modernisation will require, including shared services and centralised master data functions.
- **Chief audit executive (CAE), chief compliance officer (CCO) and chief risk officer (CRO)** — Involvement and consultation with the compliance, controls and security workstream is essential to ensuring that industry and regulatory requirements are being addressed. Additionally, the CRO and CAE are instrumental in offering guidance for a design-in approach that aligns with risk objectives.
- **Chief data officer (CDO) and chief marketing officer (CMO)** — Security, controls and compliance have an impact on data governance objectives. Collaboration with the CDO and CMO on prevention and mitigation of data breaches is fundamental.

Across the C-suite, executives must have full understanding and insight into how their business processes truly intersect, along with deviations from standard and manual work arounds. A technology like process mining enables quantitative analysis on improvement areas and bottlenecks, which enables executives to implement real-time predictive analysis on a single process, providing more effective services to the customer.

Where do companies go from here?

As organisations undertake technology transformation initiatives, high-stakes considerations include:

- Applying a design-in approach for process and compliance automation and efficiency

- Using an agile approach to meeting objectives in a dynamic digital environment
- Determining the parameters for success, including KPIs, change management initiatives and strategic business goals
- Integrating security programs into the organisation's culture
- Ensuring user adoption through two-way communication plans that incorporate feedback
- Having a dedicated security and controls workstream with consultation from the audit function

Ensuring sound security and controls compliance practices is essential to maintaining and supporting the value of technology transformation. The ultimate outcome is increased efficiency and improved quality of security and business processes, along with reduced costs and fewer error-prone manual controls, enabling transformation to continuous monitoring.

AUTHORS

TONI LASTELLA, Managing Director, Enterprise Application Solutions, New York
JOHN LIVINGOOD, Managing Director, Enterprise Application Solutions, San Francisco
MARCO GEISENBERGER, Director, Technology Consulting, Munich

People: A Forgotten Element of Technology Transformation

At a Glance

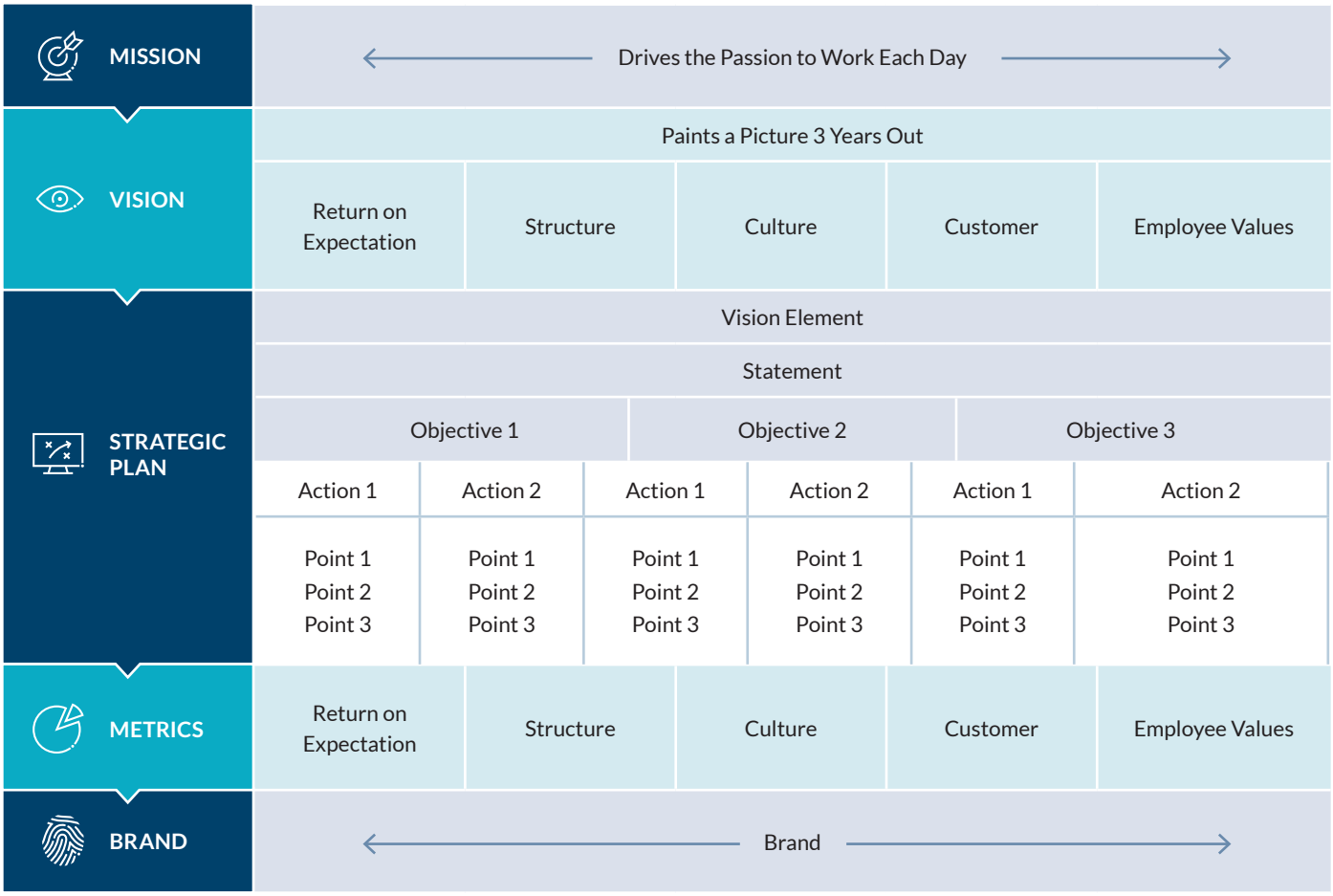
Human capital issues are a significant determinant of enterprise transformation success. Strong change enablement programs can elevate success for organisations that:

- Ensure the executive team is committed to transformation
- Establish a strong vision
- Align strategy with vision
- Set up a transformation management office

Enterprise transformation demands technology to work and people to adopt it. The "people" component of enterprise transformation can make or break digital transformation. If people within the organisation are given the right tools and are enabled and empowered to use them, they can achieve the desired intent of technology transformations. CIOs enable adoption by championing comprehensive change enablement programs that focus on ***people****. When people receive the consideration they deserve, they are more apt to bring innovative ideas forward. Organisations that do not sufficiently budget for change enablement fail at enterprise transformation because people do not adopt the new technology. Instead, they revert to previous processes or find alternatives.*

While strong ROI is compelling, so is the fact that people issues are one of the top enterprise risks. In 2020, the SEC introduced, and the International Organisation for Standardisation supported, the first regulatory standard (ISO 30414) that prescribes employee experience as a part of enterprise value. ISO 30414 reflects the enterprise risks of neglecting the people aspect of corporate activities, and it shines a light on the contributions of an organisation's human capital.

How do organisations begin addressing people issues as part of enterprise transformation? To avoid failure by underestimating the people component, change enablement should start at the very beginning — at project identification. Stakeholders must be in initial conversations about technology transformation. They bring value as they offer viewpoints on impact to job functions, which opens a dialogue on guided support and remediation.



To bring the benefits of enterprise transformation, organisations that want strong change enablement must establish a shared-risk, shared-gain approach.

Start with a commitment for change at the top

If there is a pinnacle to change enablement, it is having an executive leadership team that is committed to the transformation at the outset. The words and actions of the CEO and C-suite members must continuously resonate a commitment to transformation. Sharing progress toward achieving KPIs and metrics reinforces commitment. The organisation's human capital must be made to feel that they are significant players in the rewards and risks of transformation. CEOs who constantly communicate about the difference that people make and their impact on brand or the customer experience move the needle towards adoption and increased ROI.

Creating opportunities to talk about the digital transformation, and frequently, is a must. Executives must *constantly* reinforce their commitment to the transformation through town hall meetings and frequent interoffice communications that illustrate metrics to prove progress and impact.

Establish a North Star

To enable change, organisations must have a very strong *vision* — a mind's eye picture of their desired future state, what the change will accomplish and how

it impacts the organisation. Having a vision is the North Star that informs direction. The key elements of vision that companies should work toward include:

- **Return on expectation** — Includes a focus on financial transformation, metrics and results of the desired state, based on investment and impact to the business
- **Structure** — Encompasses the operational transformation structure and the organisation's aspirations for a future state
- **Culture** — Identifies people's initial perceptions of an organisation
- **Customer** — Defines the customer experience and why customers choose to do business with the organisation
- **Employee values** — Highlights organisational value and the human capital management required for the strongest employee experience

Without a defined vision, there is lack of human adoption.

Align strategy with vision

It is essential to ensure that the organisation's strategic objectives align with its vision. Strategic objectives enable vison to become actionable so results can be achieved. Strategic objectives must permeate to front-line employees and stakeholders. Analysing metrics and KPIs along the transformation journey helps guide decision-making towards the stated strategy. When the cascade of vision, strategic objectives and metrics align, organisations are well-positioned for optimised ROI.

A dashboard of KPIs and metrics to demonstrate progress and people's efforts in making a difference supports vision. Dashboards can offer transparency. They are tangible tools that demonstrate and track progress, guiding the transformation toward buy-in and success. Dashboards can be leveraged to explain the reasons for detours or modifications to the transformation journey, bringing understanding so people remain committed to the transformation.

Create a transformation management office at the outset

Setting up a transformation management office helps align the people aspect of the transformation in step with the other elements of change. Implementing change enablement at the very beginning of a transformation is essential. Introducing change enablement late in the journey, such as during implementation, causes people to disengage and not feel a sense of ownership. As a result, implementation often fails, budget overruns impact ROI and the benefits of transformation are diminished. Comprehensive transformation processes should focus on activities and deliverables that:

- Identify and align
- Document and map
- Design and develop
- Implement and adopt
- Facilitate feedback and improvement

The transformation office consists of a change enablement team with roles to ensure the most impactful implementation possible. Ownership and responsibilities are defined with team members working in unison from a single plan for the highest level of engagement, ownership and adoption of the change. Roles in the transformation office may include change lead, change agent, change champion team member, training coordinator, training developer, communication coordinator and communication developer.

The collaborative role of the C-suite

CIOs must have a direct seat at the C-suite decision table, rather than indirectly reporting through another executive. Establishing a collaboration framework that supports strategy and fosters knowledge sharing is optimal. CIOs must pay particular attention to going beyond technology by focusing on the *business* aspect of change enablement. They must speak the language of the business by focusing on the "why" of change and tying it to the business need.

The C-suite and other leaders must be role models of change, and C-suite members must be aligned with the CEO. People are watching and absorbing even if they are not vocalising their thoughts. The C-suite should watch for signs of disengagement and adjust accordingly to maintain people's interest and ensure they feel seen and heard.

To boost buy-in, leaders should demonstrate resilience, energy, support, patience, ethics, courage and trust. Leaders and change-enablers must be approachable to receive feedback. Executive leaders must attain individual buy-in to attain adoption by staying focused on the individual and using a shared-reward, shared-risk approach. Executives must also ensure that their communications are consistent with their actions and that it all ties back to strategic objectives, vision and corporate values.

What should companies do now?

Implementing change enablement *with adequate funding* at the start of enterprise transformation is essential. It allows for increased human capital buy-in and heightened ROI. As importantly, aligning activities and deliverables with the organisation's vision, strategic objectives and metrics positions companies for successful enterprise transformation. To move forward, organisations must know where they have been. For that reason, organisations should evaluate past change initiatives to assess past "people" approaches and make adjustments accordingly.

AUTHORS

GHISLAINE ENTWISLE, Managing Director, Technology Consulting, Melbourne (AU)
KATHIE TOPEL, Director, Business Performance Improvement, Chicago

Effective Cybersecurity is Essential as Cyber Threats Expected to Continue Over Next Decade

At a Glance

Cybersecurity is recognised as a top enterprise risk. For organisations to harness the power of effective cybersecurity frameworks, they should:

- Understand the latest technologies and approaches shaping security programs
- Build resilience into the framework
- Monitor, detect and respond to cyber incidents with agility and speed
- Collaborate effectively across the C-suite

Cyber threats are among the top ten highest-rated critical risks of organisations today and for 2030, according to Protiviti's Executive Perspectives on Top Risks for 2021 and 2030. The constantly changing risk environment requires companies to be agile in how they adapt and address cyber risks. CIOs and CTOs often transform business solutions to enable the business using tools such as artificial intelligence (AI) and Internet of Things (IoT). But with these tools comes new or increased cybersecurity and technology risks.

Without clear communication of the business risks and threats to business success, actions taken to manage cyber risks can create inherent conflict within organisations, increase competition for funding and resources, and create a perception that runs counter to business enablement. Having an effective change management program, initiated and sponsored by senior leadership, changes the tone at the top and can promote acceptance of the processes and policies put in place to manage cyber threats.

Moving off legacy platforms into more agile technology environments such as Microsoft Azure (and other cloud providers) enables organisations to safely benefit from the opportunities that such tools bring. When approached in a thoughtful and disciplined manner, organisations can accomplish their transformational objectives while, at the same time, taking notable steps to improve their security posture.

As organisations continue to modernise their technology platforms, key cybersecurity disciplines and approaches need to be considered.

New approaches to data protection

One of the key technology shifts that has shaped cybersecurity programs is the move to cloud (i.e., XaaS). This has drastically impacted the efficacy of traditional cybersecurity technologies, thus forcing organisations to evolve and update their cybersecurity architectures. It also has led to a de-emphasis of perimeter-based controls wrapped around the corporate network as the focus shifts more to identity and data-centric approaches. Capabilities such as micro-segmentation, Secure Access Services Edge (SASE) and software-defined perimeters are now needed to securely enable employees and conduct business with customers. These new approaches have proven especially effective as many organisations pivoted their operations to remote work environments. While endpoint devices such as laptops and mobile devices will play a role in organisations for a long time to come, these new architectures are required to extend traditional controls out and away from the protection of corporate networks to any location around the world. As organisations introduce new technologies during the course of transformation, it's important for the CIO to understand potential risks and plan for the right management of these risks.

Resilience as a foundation

Resilience is another key to success within cybersecurity programs. Modernisation of an organisation's technology platforms represents a significant opportunity to build resilience into the key applications and infrastructure that support core business services.

When no longer constrained by legacy platforms and outdated technologies, organisations can leverage a variety of new and evolving technologies like the cloud to significantly decrease the likelihood of a sustained outage with business impact. From high-availability architectures to enhanced workload and service management, CIOs must take a thoughtful and intentional approach to capitalise on the opportunity and build resiliency into the go-forward architecture. Speed, funding and pandemic-supporting operations, however, are preventing these changes from happening quickly. The IP that exists in outdated technologies remain in place and serve as the basis for many company operations. It is also important to note that some areas of a business, such as assembly lines (some of which are FDA certified) are unable to legally move quickly to adopt cloud and replace legacy applications.

Visibility, speed and agility

Much has been written about the zero-trust architecture, and while there is no shortage of opinions on the topic, one aspect that many cybersecurity practitioners tend to agree on is that experiencing a security incident is not a matter or "if," but "when." Zero trust as a security model has started to catch on because one of its core philosophies is to always assume that adversaries are in an organisation's environment. This is a significant mind shift from how programs have historically been built. This shift not only impacts how a program is designed, but where and how budget is applied. An "assume breach" philosophy will push an organisation to turn from heavy investment in preventative controls to a more balanced portfolio that includes an emphasis on visibility and response.

Organisations can minimise cyber risk exposure and incident impact to business operations through enhanced monitoring, detecting and response capabilities that feed an organisation's agility and speed, support resiliency, and potentially reduce adversary dwell time. CIOs should plan ahead for transformation to create more resilient services that enable business operations.

Engage with the C-suite

Cybersecurity has implications that ripple across the entire organisation. All C-suite members must understand their roles in the company's cybersecurity risks and ensure appropriate cybersecurity oversight in their respective operations and transformation projects. CIOs

who collaborate with their executive counterparts recognise that while CIOs drive many cybersecurity decisions, joining forces with the rest of the organisation's leadership team helps solidify technology implementation and change management while boosting ROI. Each C-suite member is uniquely impacted by cyber technology:

- **Chief information security officer (CISO)** — There is a significant reliance on IT and cybersecurity working closely together to monitor, detect and respond to cyber incidents. As large-scale attacks progress and elevate risk profiles, it is imperative that CIOs prioritise cybersecurity in step with CISOs.
- **Chief risk officer (CRO)** — Difficult investment decisions are made by CFOs. CROs must help uphold the ROI on such decisions by placing IT and security risk on a par with other enterprise risks.
- **Chief audit executive (CAE)** — To the extent cybersecurity impacts internal controls, auditors must have the proper training to audit controls in a cloud environment.
- **Chief marketing officer (CMO)** — CMOs must be well-positioned to produce a secure enablement of the customer journey, including securing customer identity and access management (CIAM).
- **Business leaders** — To build resilient businesses, leaders must take an active role in enabling IT with a strong understanding of business goals and services. Accordingly, business leaders must help contribute to recovery from adverse cybersecurity incidents.
- **Employees** — Employee buy-in through proper training and change management strategies is instrumental to cybersecurity transformation and modernisation projects.

Where do companies go from here?

Cybersecurity demands agility and resilience. As organisations move through their enterprise transformation journeys, it is important that they consider the following issues to optimise ROI:

- Proper cyber "hygiene" is foundational to managing security risks and maintaining resilience of business services.
- Organisations should have a clear maturity assessment of their current cybersecurity protection, with the target maturity level agreed on by both the CIO/CISO and top executives or the board. This will allow the CIO/CISO to plan for future improvement.
- Companies must mitigate cybersecurity risk without slowing down enterprise transformation and should search for opportunities to boost enterprise value with novel tools such as Greenfield cloud environments.
- CIOs and CISOs should evaluate the extent of cybersecurity implementations with an eye on enterprise transformation, carefully determining the measures required for minimally viable products or services and adding greater cybersecurity complexity where needed.
- With cyber threats expected to be among the top ten risks for organisations across the next decade, CIOs must ensure that their organisations have effective cybersecurity programming to mitigate risk and protect their company's valuable assets during and after digital transformation.

AUTHORS

MICHAEL PANG, Managing Director, Technology Consulting, Hong Kong
NICK PUETZ, Managing Director, Security and Privacy, St. Louis
ANDREW RETRUM, Managing Director, Security and Privacy, Chicago

Balancing Identity and Access Management for Risk versus Speed

At a Glance

Identity access management is the cornerstone of security. To arrive at programs that balance speed, risk and usability, CIOs must collaborate with the C-suite to:

- Target incremental progress over perfection
- Aim for infrastructure with governance
- Gain visibility into customer profiles
- Choose smart partners and effective products
- Address pain points to gain buy-in

Identity and access management (IAM) is the cornerstone of security. As such, it is important to balance IAM to ensure maximum speed of user access while managing risk. Proper IAM enables legitimate internal and external users to access the right data at the right time from the right devices. While IAM may seem like a check box in the journey to technology transformation, its role is much larger.

IAM is — quite literally — a key to a desired, secure and modernised state. Identity and access issues such as duplicate and stale user accounts, excessive user access and suboptimal automation can slow user access and erode security and should be resolved. Technology transformation is an opportune time to clean up old habits. "Lifting and shifting" obsolete identity and access processes to modernised technology is equivalent to using a defunct motor in a new Ferrari. Solid IAM programs clean up data, increase speed for a wide range of internal and external users, and look to reengineer and automate processes within the framework of a governance and policy program.

CIOs identify and focus on current strengths and weaknesses to arrive at a best-of-breed IAM solution that is structurally sound and integrates well in the organisational technology ecosystem. They implement IAM programs that enable efficiency and trim duplicative or overlapping technologies so that organisations are not over-licensed for capabilities that will not be utilised.

IAM brings value

IAM must be balanced for three things — speed, risk, and usability. IAM can enable enterprise transformation projects through automation that enables quicker access. It allows for movement of workloads into the cloud seamlessly and enables companies to externalise applications that are on-premises. However, speed must be balanced with each organisation's unique risks. While the right IAM structure can reduce risk, insufficient IAM can increase risk.

Usability is also an important factor in an IAM program. Whether the solution is single sign-on or multifactor, a simplified, well-designed solution that is easy to use and understand can improve the user experience, make employee onboarding seamless and reduce help-desk calls. Conversely, a poorly designed solution can create friction in a user's experience depending on what choices are made in the technologies and processes that are put in place, and can negatively impact user adoption.

With far-reaching implications *across* the organisation, it is crucial that CIOs are exceedingly thoughtful about their IAM strategy.

It takes time to build the right identity infrastructure. Upfront investment costs with an eye toward scalability are essential as the organisation grows in people, processes, data, performance and cloud capability. Once a robust IAM foundation is established, organisations can move faster into future states.

Target incremental progress over perfection

It is critical to understand that IAM is not a project — it is an ongoing program that must span and align with the life of the organisation. CIOs should aim for incremental progress over delayed perfection. IAM must be maintained, keeping pace with growth and dynamic business needs. IAM cannot be an afterthought of technology transformation, as afterthoughts lead to failure and newsworthy security breach disasters.

Aim for infrastructure with governance

Beyond choosing the right technology, strong IAM requires a solid infrastructure, with a strategy and a roadmap. CIOs should build out a strong IAM infrastructure with ongoing maintenance and improvement that aligns with business needs. Maintaining IAM is a never-ending marathon because once the infrastructure is rolled out, there are additional capabilities, integrations and (sometimes) business units that impact IAM programs.

While a strategy and a roadmap are instrumental, they must be accompanied by a governance model led by a steering committee that champions the voice of the customer. The steering committee serves to inform C-suite decision-making with an empowered understanding of business pain points, risks and security challenges. It is then that informed decisions about trained staff can be made to ensure that the organisation's crawl-walk-run strategy leads to the stated vision.

Gain visibility into all identity profile types

An effective IAM program creates a consolidated record for each person as one identity. For a comprehensive view of each user's accessibility and associated risk, IAM must be able to form a single identity for each user. While many organisations are focused on employees (e.g., segregation of duties), client identities across the various business units are just as important, particularly in the case of corporate mergers and acquisitions, where a customer might have access across several business units. A strong IAM program addresses disparate identity issues by developing a consolidated profile for each person across a unified user experience when they interact with the organisation.

Robust IAM demands smart partners and effective products

Put bluntly, effective IAM is not a do-it-yourself program. To prevent user access breach disasters, CIOs must recognise that they need smart partners and best-in-class products. IT departments that attempt to build and maintain their own IAM program are left with failed frameworks, or they crash along the transformation journey. Experienced IAM partners enable flexible frameworks that control risk while leveraging customised technology such as intelligent process automation (IPA) and artificial intelligence (AI).

Address pain points to gain buy-in

IAM touches every aspect of the organisation, making implementation and adoption very challenging. When new controls are implemented, users often find a way around them. To gain user buy-in, CIOs must collaborate with other C-suite leaders to solve for user pain points such as automating tedious functions. Offering value propositions to C-suite members is key to effective implementation and acceptance. The sooner users are vested in the controls, the more successful the program will be. Issues unique to C-suite members include:

- **Chief risk officer (CRO) and chief administrative officer (CAO)** — Access governance models, monitoring, prevention and remediation strategies and identity risk scores (of internal and external users, including vendors) are top concerns. It is important to demonstrate value by providing traceability for faster, more accurate audits. Implementing IAM controls to address access and permission for risk reduction offers value propositions to CROs and CAOs.
- **Chief financial officer (CFO)** — Preventing and mitigating data breaches, protecting assets, and demonstrating return on investment are critical to CFOs. They look for increased production, efficiency and value, while protecting sensitive assets with privileged access management programs.
- **Chief data officer (CDO)** — Protecting data from hackers is the critical task of CDOs. IAM offers the data protection, monitoring, privacy policies and classifications that CDOs want while also applying analytics for enriched, contextualised data from protected data lakes. A collaborative partnership between the CIO and CDO is crucial for building an IAM strategy that considers the who, when, why and how of data access.
- **Chief marketing officer (CMO)** — CMOs are interested in privileged user management, which is the activity of users who have privileged access. They are concerned with controlling proper usage of social media accounts and other external-facing communications to secure brand value. And they appreciate the ability to rapidly capture customer information, protect customer identity and enable quick authentication.

Where do companies go from here?

IAM brings significant ROI to enterprise transformation by:

- Supporting compliance
- Elevating security
- Increasing operational efficiency

While the most significant benefits of IAM cannot be numerically quantified, the value of an effective IAM program is undeniable, because access breaches come with severe consequences and intolerable monetary and reputational costs.

To acquire the greatest benefit from IAM during enterprise transformation, companies should undertake the following, with each step centered on IAM:

- Understand the organisation's current processes, users and technologies
- Know the organisation's transformation infrastructure goals
- Understand the drivers for transformation
- Assess how IAM fits into enterprise transformation
- Lay out an IAM strategy with subject matter experts
- Evaluate gaps and opportunities and discuss pain points with business centers
- Create a roadmap that delivers iterative and consistent improvements to security, risk reduction and the user experience

Identity and access management is difficult and ongoing. CIOs should aim for progress over perfection. IAM programs that scale for growth are essential to bringing a future IAM state endowed with security, speed and visibility.

AUTHORS

ASHRAF MOTIWALA, Managing Director, Security and Privacy, Dallas
DUSTY ANDERSON, Director, Security and Privacy, Phoenix
CHAD WOLCOTT, Director, Security and Privacy, Boston

*Managing Director **ENRICO FERRETTI**, Milan, also contributed to this article.*

Enable Rapid Response to Changing Business Needs with Agile and DevOps

At a Glance

Agile and DevOps bring rapid agility. To reap the benefits, organisations must:

- Ensure strong leadership support of Agile and DevOps enablement
- Scale an enterprise mindset
- Promote a culture of change and learning — and enable it
- Modernise methodically

Successful companies today are lean, agile organisations with executives who have a vision and a mindset that empowers collaboration so employees can achieve that vision. These organisations must be agile because rapidly responding to dynamic market demands without compromising quality is required for survival. Achieving business transformation and agility requires commitment from leadership at the very top of an organisation, including C-suite, business and technology leaders. Each must be committed to the agile/digital transformation and must communicate that support clearly throughout the transformation journey.

Agile and DevOps are disrupters of the conventional software development life cycle. Combining Agile and DevOps with elements such as cloud, testing, security, risk management and compliance creates a modernised technology delivery approach that can help an organisation achieve greater speed, reduced risk, and enhanced quality and experience. Agile accelerates and shortens the software development life cycle by focusing on smaller, incremental builds and continuous iteration, while DevOps underpins the Agile release cycle through a standardised, automated and well-governed process. CIOs bring value to business agility by championing an Agile and DevOps framework for a quick, adaptive response to market conditions and competitive pressures. They build and maintain a value-driven, cross-functional infrastructure using the right technology, people and processes.

Like a strong, stable foundation, forming and maintaining an Agile and DevOps enterprise architecture brings the built-in flexibility needed to transition from the status quo to new capabilities for pivoting on demand. This contributes to accelerated development and enhanced defect detection and correction, resulting in improved quality. DevOps stresses transparency, increased communication and cross-functional collaboration. In terms of relative significance, software development, testing and

implementation are all considered equal. Agile enables an elastic way of working through technical platforms so employees can quickly and flexibly deliver innovation and greater value to the market. Meanwhile, DevOps maintains modernisation momentum by driving ongoing transformation.

Agile and DevOps lean on a mindset shift from traditional approaches to empowered self-organised teams, incremental builds with fast learning cycles, and continuous improvement. These are all tied to an enterprise architecture that includes the business vision and capabilities within the business architecture with clear buy-in from top leadership. CIOs are instrumental in helping to permeate an Agile, lean mindset throughout the C-suite and the organisation. They must demonstrate to stakeholders that Agile delivers steady value sooner as compared to waterfall approaches where value is released at program completion.

An Agile tone at the top is crucial

Successful enablement of Agile and DevOps requires full support of business leadership from the top down. Without this support, the transition will not succeed. Business and technology leaders must be committed to the Agile/digital transformation and must communicate this support clearly and continually throughout the transformation process. CIOs must provide guidance through clear definitions of the vision, strategy, goals, objectives and metrics for employees to adopt, including KPIs (Key Performance Indicators) and objectives and key results (OKRs). It is critical that employees and other stakeholders align with the stated vision and goals. Communication and employee engagement builds commitment, so organisations should ensure that status updates on the transformation are shared with employees through town hall meetings, video updates and other communications.

Leaders must be forward-thinking and go beyond walking the walk; they must provide steadfast, active support. Successful CIOs and business leaders understand that business agility, which includes Agile and DevOps enablement, does not come easily. To bring value, a culture that is creative and innovative must be built. The concept that no idea is a bad idea should be the standard. To avoid stifling creativity, organisations should clearly define the vision and then unleash its human capital to figure out the details of achieving the stated vision.

However, experienced CIOs recognise that — rather than being risk-averse — there are smart ways to take risks. While teams should be encouraged toward innovation, a "fail early/fail fast" approach should be adopted. Rapid testing, learning from failure, pivoting and moving forward with other innovative ideas is core to Agile and DevOps enablement.

Scale an enterprise mindset

For effective response to market demands, the organisation must have an enterprise mindset toward digital transformation, as opposed to a siloed approach. Where market demands prompt a business to pivot, the entire organisation must be uniformly responsive. To enable all functions of the organisation to work towards the same vision and objectives, incentives and motivations across the enterprise must all support and align with a singular vision. To gain commitment, leveraging a collaborative approach rather than a hierarchical one is more effective.

Promote a culture of change — and enable it

Every stakeholder must accept forthcoming change. Building an Agile Center of Excellence (ACE) enables the necessary changes to achieve corporate vision. An ACE promotes the transformation and ensures that people are in alignment with vision, strategy, goals and objectives.

Likewise, the leadership team and the CIO must keep a strong pulse on employee pain points. Conducting roundtable discussions and performing surveys provide insight on areas requiring improvement. To assess how employees are feeling and to support engagement, open communication is a must. It informs how and when to provide necessary support, including training and coaching, so everyone can keep working toward enabling the corporate vision.

Modernisation is a journey, not a mission

Organisations should upgrade, replace or substitute technology incrementally and as feasible. They should not attempt to modernise every aspect of the business in one avalanche. To the extent there are capabilities that have become obsolete or are no longer bringing value, it may be best to return to square one — go to the whiteboard and start from scratch on a particular process or technology.

Collaborate comprehensively

Digital modernisation is a time for having a collaborative, enterprise mindset. Silos must be broken down and the concept of looking for individual benefits should be stricken. To enable collaboration and transparency, frequent and proactive communication is essential.

Having a governance structure for the transformation that is inclusive of key players is a must. It is paramount to include the CIO and other innovative leaders at the executive roundtable. Business executives and technology leaders alike, including CIOs and CDOs, all must have a voice in high-level decision-making, and it is essential that their input is considered. Doing so supports a governance structure that enables business leaders to inform IT and, likewise, enables IT executives to inform business decision-making.

All hands on deck

The domino effect of change and adaptation requires that all functions of the business respond by transforming — in unison. A failure to respond in one or more of the organisation's functions will cause the enterprise transformation to topple. For that reason, to keep pace, everyone in the organisation from marketing and sales to audit, risk and compliance must adopt an Agile, lean mindset. Leveraging Agile and DevOps enables rapid response and fulfillment of market demands.

C-suite support is integral to the ability of each function to pivot and respond to the changes needed for agile reaction. For example, chief data officers (CDOs) rely on real-time intelligence by collecting user information. Organisations must shift away from periodic reporting to real-time analytics to feed the Agile and DevOps process and quickly respond to market changes. Middle management must be fully committed to the transformation and aligned with the business's vision as they are the boots-on-the-ground agents of change. They promote and ensure employees are achieving goals and supporting the business vision. Anything short of commitment and full alignment of business vision results in delayed transformation at best — or failure at worst.

What should organisations do now?

Transformation is challenging and requires adjustments over time. However, it is imperative for organisations to choose a starting point. When assessing current status and establishing Agile and DevOps readiness, organisations should:

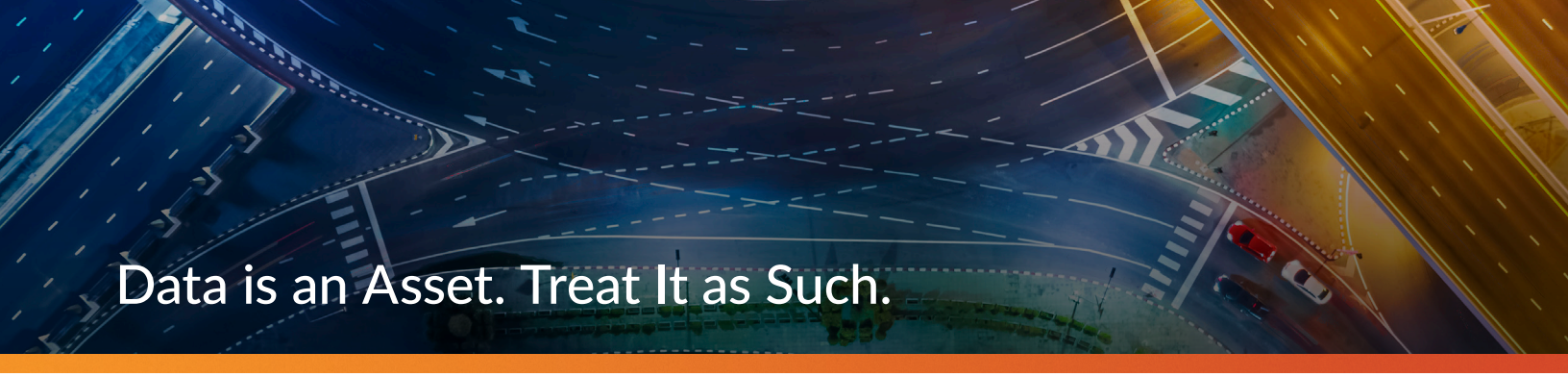
- Establish the business vision, roadmap and transformation impacts
- Understand the reason for the transformation and analyse the benefits gained
- Understand the roadblocks to short-term and long-term transformation
- Understand the organisation's challenges for a clearer view on the appropriateness of an Agile or digital transformation
- Establish and define metrics — KPIs and OKRs

Agile and DevOps enables technical agility for organisations. Keeping pace demands that organisations pivot rapidly to meet and exceed expectations. To win at enterprise transformation, a business must leverage Agile and DevOps uniformly across the organisation, for a chain is only as strong as its weakest link.

AUTHORS

JEFF STRAIN, Managing Director, Technology Strategy and Operations, Charlotte
SOFIA HANSEN, Associate Director, Technology Strategy and Operations, New York

*Managing Director **SCOTT GRACYALNY**, Chicago, also contributed to this post.*



Data is an Asset. Treat It as Such.

At a Glance

Data is an asset when it is built to bring value. Digital transformations that champion data meet and exceed ROI expectations. Smart CIOs treat data as they would treat their careers — with diligence, sustainability and effort. Organisations must solve for digital transformation by understanding and maintaining their greatest asset — their data. To maintain the value of data during enterprise transformation, organisations must:

- Understand the organisational strategies for driving value from data
- Implement a data workstream
- Understand the past to arrive at a desired future state
- Focus on people to extract legacy information
- Brainstorm new ways of working

Data is the building block of business. If a company loses its data or if its data is compromised, it could significantly damage the business in terms of financial performance, brand reputation or loss of customers. Executives understand that data is an asset when it is transformed to bring value. Whether an organisation leverages data to fundamentally run its business, the data is a byproduct of conducting day-to-day operations, or the business sells the data assets as a unique product, data must be managed, protected, traced and updated. The importance of valuable data is even more amplified as an enterprise undergoes digital transformation.

CIOs must be deeply involved in unlocking and protecting the organisation's data to gain its full value as an asset. Data that is not properly integrated will cause enterprise transformation to fail. CIOs who want to modernise their application architecture or any other architecture must have a data structure, know where their data originates, and understand its lineage and how it interacts with operational flows.

Fragmented and uncontrolled data impede technology modernisation. Thus, fundamental data challenges must be addressed to enable full value. When an organisation's data is scattered, vague and unmanaged, time and money must be spent correcting these deficiencies prior to technology modernisation. While many organisations have access to sufficient technology, they do not have a process, discipline and the fundamentals to leverage data as an asset, and therefore aren't getting the anticipated return on investment.

Understand the organisational strategies for deriving value from data

The purpose behind collecting and retaining data is to meet business objectives. A key for driving and treating data as an asset is to first value that asset by understanding how it is used within the organisation. IT professionals must fully understand the business strategy and then provide guidance for how to collect, store and protect the data assets needed to drive to that strategy. In any digital transformation, data is essential, so clearly this alignment must occur.

Implement a data workstream

It is important that data not be an afterthought in technology modernisation efforts. On the contrary, organisations must understand the origins and characteristics of their data, including whether it contains personally identifiable information (PII), as well as the requirements to manage it. Organisations should develop and implement a dedicated data workstream, including integrating and harmonising data from different systems and addressing data timing, including real-time, near real-time and batch data. Organisations that do not develop data as a workstream will reap subpar results — at best — from their modernisation efforts.

Understand the past to arrive at a desired future state

CIOs must understand their organisation's legacy architecture and desired future state, and they must bridge the gap between the two. Technology environments are layered with multiple years of various technologies. As an organisation implements new technology year after year, a mixture of techniques and programming are deployed, each of which pose unique data challenges. Disassembling old data structures and reassembling them for a future state requires unique skill sets, including a strong understanding of legacy systems.

Focus on people to extract legacy information

The talent shortage of workers with experience in legacy systems is a real and prominent challenge for many organisations. As an ageing workforce looks toward retirement, organisations risk losing valuable information about their legacy systems, and will be challenged to find replacement candidates who can understand why legacy systems were built the way they were (many decisions were made for good reasons but caused complexity). To proactively address this problem, CIOs should implement focused programs to gather institutional knowledge and legacy systems information from internal subject matter experts while they can, and then should use data governance techniques to persist this knowledge. This will ensure the organisation is in a good position to implement new technologies.

Brainstorm new ways of working

The old way of working, now obsolete or becoming obsolete, applied a siloed resources method where various resources (data analyst, mapper, architect, ETL resource and API developer, etc.) were used to perform tasks. Today's organisations are looking for new ways of working and are engaging full-stack developers and engineers who can perform a broad range of technology skills. Companies want a single team that can build and have security overlays and operations — without calling in specialised resources at every turn. This makes it possible to continuously develop and build applications while incorporating security and operational aspects throughout.

Companies can adopt new ways of working by addressing remote working arrangements and building best-of-breed technologies into their models. Companies should also seek out resources with the right skill sets in the right locations and for the right price to address data DevSecOps or continuous development, continuous security, continuous improvement and continuous operations.

Holistic collaboration brings company-wide modernisation

Collaboration *across* the enterprise is essential to optimising the modernisation of the organisation. Addressing only one function or department's transformation may be detrimental if consideration is not given to other functions or departments. Therefore, a holistic collaboration brings company-wide transformation, as opposed to only partial transformation.

C-suite members each have unique concerns about the integrity of data and the extent to which it impacts their respective functions:

- **Chief risk officer (CRO)** — The integrity of the data being applied in risk models is of utmost importance to the CRO because if the data is not reliable, true risk cannot be properly determined.
- **Chief financial officer (CFO)** — Financial reports, including audited financial statements for public companies, are based on data in the general ledger. To the extent the data is not reliable, there could be severe consequences, including financial statement restatements and inaccurate valuations.
- **Chief audit executive (CAE) and chief data officer (CDO)** — A collaboration triangle should be formed among the CIO, CAE and CDO. Their communications support the organisation's audit activities as the CDO (for public companies) ensures that all controls are performing as intended (especially for compliance purposes), the CAE ensures controls are properly defined and the CIO supports the technical aspects of the audit function.
- **Chief compliance officer (CCO)** — Confirming that the right people have the right access to the right data is of utmost importance to the CCO for compliance purposes. Therefore, understanding and securing the parameters and permissions for access to data is paramount.

What should companies do now?

To gain full value of their data, organisations must ensure that it is understood, tracked, optimised and controlled. As they move through their transformation efforts, companies should:

- Understand their data ecosystem, including where the data resides and how it is transformed and leveraged
- Understand the relative value of data within the data pipeline and eliminate data sources that are not needed for business purposes
- Know what data is being acquired from outside vendors and how it is being used internally.
- Don't buy, keep or ask for more data than the organisation needs
- Eliminate irrelevant, erroneous and duplicative data from the environment, depending on the organisation's industry and the level of its environment control
- Create a golden source of data across the data ecosystem to ensure accuracy and consistency

CIOs must work with leadership across the entire organisation to resolve fundamental data challenges if they are to achieve a successful technology transformation. A focus on correcting deficiencies and developing a process and discipline for managing and protecting data through proper governance will ensure the organisation transforms and leverages its data for maximum value.

AUTHOR

PETER MOTTRAM, Managing Director, Enterprise Data and Analytics, New York

Data and Analytics Drives Strategic Decision Making

At a Glance

Business analytics and reporting can empower enterprise transformation. To modernise data for reporting and analytics, organisations should:

- Implement self-service to generate efficiency
- Use data governance to empower analytics
- Minimise silos and use a flexible architecture for knowledge workers

As data becomes more complex and explodes in volume, end-users' expectations for quick access to reliable data remains robust. To meet business needs, companies must harness and use information in a way that propels business goals. Reporting and analytics are, therefore, critical priorities for CIOs because they structure and optimise information to guide businesses in strategic decision making, which can bring a competitive advantage. Each plays a key role in enterprise transformation, the success of which largely depends on whether an organisation plans for the use and analysis of data and implements the technical infrastructure to support it.

End users must have the ability to easily access accurate, relevant data when and where they need it, and leverage that information in a way that enables business. While data access is a must, it should be balanced with governance to ensure the data is trustworthy, compliant and secure. Users also must be able to engage in *collaborative* analytics — a key modernisation capability that supports *enterprise-level* discussions — as opposed to simplistic individual views that lead to tunnel-vision decisions.

Self-service generates efficiency

CIOs aiming for strong reporting and analytics must focus on self-service. They should shift to data automation so end users can access information when they need it without waiting for IT to provide it to them. Business-driven CIOs are implementing self-service by modernising and using the cloud for rapid data access. CIOs are moving data and applications to flexible cloud platforms that offer greater accessibility, support reporting requirements, and execute on data-sharing and platform demands.

Cloud services bring a scalable solution that accommodates increasing demands and provide a flexible system that empowers the organisation in ways that an on-premises environment cannot. They also enable self-service by automating data access, discovery, analysis, preparation and presentation.

Strong data governance empowers analytics

Data *governance* is a top consideration in enterprise transformation. Organisations that do not govern their data do not have quality data from which to ensure regulatory compliance or to make solid business decisions. Bad data can lead to faulty decision making that results in decreased customer satisfaction, loss in revenue and damage to the brand. It can also lower efficiency and productivity, as one seemingly minor data error can have a snowball effect, especially when not caught early in the process.

CIOs who want to support strong analytics must implement data governance that brings

- Streamlined operations
- Analytics grounded in reliable data
- Effective regulatory compliance

Minimise silos and implement a flexible architecture for knowledge workers

Information silos are real — and they are disabling to knowledge workers. To modernise, CIOs must minimise information silos to have a single source of truth. Organisations should evaluate whether or not they are minimising data silos by leveraging an open, flexible platform that supports data-sharing and reporting needs.

During modernisation, organisations often struggle with how different platforms will integrate with various apps, and they likely will be using an even greater number of apps in the future. Building a flexible data architecture accommodates unique business needs, including the nuances of various applications. The idea of a "one-architecture-fits-all" approach is not effective. Having a platform that is founded in flexibility enables integration and allows for the efficient flow of reporting.

Collaboration should center around governance

CIOs should collaborate with C-suite members on the parameters of data governance, including the:

- Value of data being stored
- Use, organisation and governance of data
- Accessibility of data

A transformation "center of excellence" can help define roles and responsibilities while enabling enterprise transformation change management initiatives and communications among C-suite members.

C-suite members are uniquely impacted by reporting and analytics:

- **Chief risk officer (CRO)** — In today's environment, data is a key component in the risk environment. CROs should be data-driven and remain alert to risks associated with data breaches. A data-driven CRO will proactively manage risk by understanding how the organisation's data can be strategically used to protect against threats to the company's data sources.
- **Chief financial officer (CFO)** — CFOs must understand the value that data governance brings to reporting and analytics. CFOs will value the ability to access information that is more accurate, detailed and timely to support financial reporting.
- **Chief data officer (CDO)** — Enterprise data strategy is at the core of CDO priorities and directly tied to the outputs of reporting and analytics. The CIO and CDO must collaborate on how data strategy can serve reporting and analytics in a way that bolsters enterprise transformation.
- **Chief marketing officer (CMO)** — Rigid data environments negatively impact marketing efforts. Strong data governance enables more effective marketing activities and the ability to assess the value of marketing campaigns. CMOs can easily leverage modern data assets to make better, more informed decisions.

- **Chief audit executive (CAE)** — Data automation brings immense value to a historically manually-driven internal audit function. Data sampling can become more efficient, population samples will be broader for effective risk identification, and self-service accessibility can enable internal audit analytics.
- **Chief compliance officer (CCO)** — Reporting and analytics provides the ability to manage the controls environment and test the effectiveness, completeness and accuracy of controls. It also provides the ability to assess gaps in compliance and enables gap assessments to be done in a more proactive fashion.
- **Business leaders and employees** — Organisations do not transform overnight. Sustainable modernisation requires time. Strong reporting and analytics enable business leaders and employees to make sustainable incremental improvements. Organisations will benefit from broad-based, incremental performance improvements by having the right data at the right time for better decision-making.

What should companies do now?

Organisations should consider conducting an enterprise data readiness assessment by evaluating their organisational maturity level for various aspects of data reporting and analytics. Accordingly, they should determine modernisation readiness, data quality and governance capabilities, data maturity status, modernisation goals and the requirements to achieve them. Next-level organisations should evaluate and consider:

- The impact that modernising will have on their reporting and analytics
- How they want to analyse data and use it as an asset
- The benefits that modernising will have on analytics and whether it will enable data analysis in the manner needed
- Investments in technologies and solutions needed to share, profit from or differentiate data

Tomorrow's CIO is continuously evaluating whether they have the right systems in place to support the organisation's modernisation efforts. CIOs must plan for the future — in the present — to enable reporting and analytics that propel decision-making and transform organisations.

AUTHORS

STEVE FREEMAN, Managing Director, Enterprise Applications Solutions, Atlanta
BRIAN JORDAN, Managing Director, Enterprise Applications Solutions, Boston
RISH DUA, Director, Enterprise Data and Analytics, Chicago

Data Governance Shapes Enterprise Transformation

At a Glance

Data is the substance and sustenance of digital enterprise transformation. Organisations must enhance data through governance programs that:

- Build sustainable data governance programs
- Enable compliance through data automation and flexibility
- Align data with business objectives
- Ensure ethical use of data assets

If enterprise transformation represents a universe, data is at the center. Data is like clay that must be shaped and molded to build a transformation that brings business value. As Carly Fiorina, former CEO of Hewlett-Packard, once said, "The goal is to turn data into information, and information into insights." Data conversion and governance helps transform data into information that can be used for making insightful decisions.

Data must be governed, controlled and protected so that its quality is enhanced, it is well understood, and it is fit for purpose to support end-user demands. Because data is a critical asset, organisations should design in governance from the ground up on all major projects and business objectives. Data governance consists of a collection of controls designed to increase an organisation's knowledge of the data assets, protect the fidelity and quality of these assets, and provide controls over the use of these assets. As such, data governance is an enabling competency for the rest of the organisation, requiring coordination from many different areas of the business to enable and support the required controls.

While data governance is a critical enabler, experienced CIOs understand that it is not a one-time activity.

Dynamic business needs and regulatory demands require that data is continuously maintained and governed. To optimise data governance for enterprise transformation, CIOs should:

- Build sustainable data governance programs by embedding processes into the upfront collection, maintenance, use and destruction of data
- Support compliance through automation and flexibility
- Align data with business objectives and understand the value or risk of the data elements
- Capture information to ensure data uses are ethical and align to company values as well as regulatory, contractual and compliance needs

Build sustainable data governance programs

The need to understand data fully and protect usage only increases as organisations rely more on data assets for artificial intelligence, automated decisioning and other key business processes. To ensure the ability to deliver this value, data governance must be built in from the start, not as a project but rather a sustained process. Sustainable data governance helps digital transformation efforts thrive on a continuous basis through automated discovery of data definitions, compliance, and governance and management activities. One major barrier to data governance is the creation and management of data dictionaries. Once established, data definitions require continuous maintenance because they change over time, with people using them in different ways and enriching and enhancing those definitions. Data definitions must evolve with the demands of the business.

CIOs must build an evergreen data governance process to avoid repetitive, iterative, expensive and time-consuming data rediscovery processes. For example, when data is not defined, the composition of the data is not understood; organisations will not know where it belongs and how it is being used. Every time data is moved to a new location, the process of discussing it with business users to understand how they are using it and redocumenting the definition must start over again. This becomes a frustrating and expensive cycle stuck on repeat between IT and business units. In contrast, building in processes to support evergreen data dictionaries enables end users to understand the data they are using from the start, propagating down the definitions into new data sources and warehouses as they are created.

Enable compliance through automation and flexibility

Historically, compliance with data regulations has relied on a reactive approach, waiting for emerging requirements before implementing solutions.

Forward-thinking CIOs anticipate compliance needs and apply built-in intelligence upfront in their data governance programs. Much of the foundation for data governance starts through understanding the definitions of an organisation's data, where it is housed, and how the business uses it. This knowledge can be pivoted to support any number of future compliance needs by enriching our fundamental knowledge of the asset itself. With security and privacy regulatory expectations constantly increasing, the more the risks associated with data can be understood and classified preemptively, the less reactive — and more proactive — organisations can be. To proactively address compliance issues, CIOs must have a seat at the C-suite table so they are aware of and understand upcoming business issues and regulatory challenges that may be on the horizon and can incorporate that understanding proactively as data safeguards are developed. As new compliance initiatives surface, CIOs can preemptively:

- Ensure there is an evergreen Enterprise Data Dictionary or catalogue to describe data assets across the organisation
- Gain an understanding of how the data could impact, drive or prevent compliance issues
- Assess how the data can be applied to the compliance initiative
- Proactively anticipate the next compliance initiative rather than performing repetitive, full discovery exercises that drain time and money

With cloud services, organisations can gain fluidity as rules are built into data for increased flexibility. To take advantage of this inherent flexibility, fully understanding the data definitions and other metadata is a must. When properly enabled through this foundational knowledge, organisations can go on the offensive with their data governance program as opposed to remaining in the reactive, defensive stance.

Align data governance with business objectives

CIOs must align with the business to understand what data is most important. Data is a business asset, but it is safeguarded, provisioned and otherwise controlled with technology assets. The data asset itself must align with the business objectives and demands to drive value. While technology provides a storage place for data, it is business leaders who must help define and inform data and assign value to it. When data governance programs are developed, it is critical for the CIO to get involvement and commitment from across the business, as governance often involves time and resource commitments from across the entire organisation. The CIO drives this mandate while giving a clear definition of how long it will take, what involvement will be needed across the organisation, and what eventual value will be delivered by governance.

To enable the business's investment in data, CIOs must work with other business leaders to evaluate:

- The real business problem being solved by the data, which helps to define the value or risk of the data
- How the organisation will be better off tomorrow than today as a result of governance
- The cost of data problems, both in opportunity costs (not being able to pursue something) as well as real monetary costs
- How the data governance program can be aligned with business objectives with a smaller spend that produces quick value

Ensure ethical use of data assets

An emerging concern for CIOs is how data assets are being used and if those uses are ethical. Definitions of social and cultural norms for ethical behaviour may deviate slightly across different areas, but a great rule of thumb is for the CIO to consider what reactions might result from the organisation's specific data uses being published on the front page of The Wall Street Journal. Unfortunately, more CIOs are learning this lesson the hard way, with the repercussions including overall loss of shareholder value and confidence.

Ethical data use should consider the value of the particular or planned data use case, as compared to the potential harm or downside. Organisations are increasingly creating Data Ethics panels to review new innovations or data products to help steer clear of some of these ethical issues. These committees are often asked fundamental questions, such as:

- Can we use our data assets for the planned purpose based on our commitments to our clients and contractual, legal and compliance restrictions on the data?
- Should we use the data for these purposes? Will it drive value?
- Will we use the data in this way if the value of the use outweighs the overall risks, which is a decision ultimately made by management?

Obtain buy-in to fulfill business needs

CIOs need to collaborate and obtain buy-in from business leaders using value propositions like enhancing data to increase efficiency or reduce costs for the C-suite. While it is challenging to start a data governance program, implementing policy-based behaviour is achieved through either reward or enforcement.

The manner in which each C-suite member is uniquely impacted by data governance includes:

- **Chief operating officer (COO), chief marketing officer (CMO) and chief financial officer (CFO)** — First-line members must provide buy-in so that departmental resources can be leveraged. Their human capital enables an understanding of how data is used, as well as performing data documentation.

- **Chief risk officer (CRO) and chief compliance officer (CCO)** — Second-line members enforce that people are performing the requests of first-line members, such as publishing policies.
- **Chief audit executive (CAE)** — Third-line members validate that data governance programs are working as intended.
- **Business leaders and their employees** — IT will request certain data-driven tasks, such as maintaining data definitions. This requires employees to be more data-driven and alters their day-to-day responsibilities.

What should companies do now?

Organisations should assess and understand their maturity in data governance and clearly articulate its value proposition, which includes risk reduction, optimisation and reduced rework. Organisations that are mature in their technology transformation journey focus on continuously knowing their data, especially as new datasets are gained. However, for all organisations, it is key that they establish a strong master and transactional data governance program that is responsive and adaptive and, most importantly, properly defines the roles and responsibilities for the data. To achieve strong governance, organisations should:

- Establish a governance strategy by defining policies and procedures for data maintenance, backed by data profiling to uncover areas of improvement and prioritisation for the governance road map
- Develop master data governance with a focus on process interactions and validations of key attributes for optimal performance of business operations across the enterprise
- Understand the roles that technology will play in the implementation of data governance
- Measure data quality metrics across master and transactional datasets and suggest corrective actions where needed

The better organisations know and understand their data, the more valuable that knowledge can be used for governance, security, privacy, identity access management, change management and transformation.

AUTHOR

MATT MCGIVERN, Managing Director, Data and Analytics, Atlanta

Project Resourcing Untangles the Who, What, When, Where of the Transformation Journey

At a Glance

Resource considerations for organisations undergoing enterprise transformation can be dizzying. To tap into the solutions that project resourcing brings, forward-thinking CIOs:

- Define clear roles, responsibilities, reporting and decision-making authority
- Govern for a clearer path forward
- Champion organisational change management to quell anxiety
- Align project resourcing and methodology
- Optimise offshoring efforts

As organisations digitally transform, they must determine who will do what, when and where. Meanwhile, fundamental business activities must continue while new processes, tools and skills are onboarded during digital overhaul. Clear and transparent alignment between transformation strategy and placing people and partners in the right roles is critical.

Smart project resourcing keeps the organisation's business operating effectively while equipping it with the right people and partners to enable it to succeed in its transformation journey. It enables the CIO to ensure necessary skills and experience are available to focus on transformation efforts while maintaining business as usual (BAU) and provides an opportunity to identify and fill gaps. Effective project resourcing looks beyond cost and considers resource needs after the transformation effort is complete. To this end, CIOs must think ahead and plan for the knowledge they need to retain to sustain BAU post-transformation.

Through all of this, CIOs must keep their mind on the goal of the enterprise transformation strategy.

Define roles, responsibilities and decision-making authority

Building and maintaining an optimal resource mix for transformation efforts is critical for success. Defining roles, responsibilities and decision-making authority at the outset provides transparency and measurability. CIOs must identify the right skills, individuals and partners to achieve the vision while maximising budget dollars. With these components identified, they can determine fixed and variable components of the labour pool, including temporary resources needed only during transformation efforts.

As team skill sets and composition are evaluated and onshore or offshore third parties are brought in, team

dynamics change. Subject matter experts may need to be pulled from their day-to-day job responsibilities to focus on the transformation effort, creating gaps in coverage that may need to be backfilled. Accordingly, new or revised team structures will be built.

Govern for a clearer path forward

While a business can outsource work, it cannot outsource risk or responsibility, so building a strong governance structure upfront is paramount. CIOs must identify stakeholders and key players, and ensure a strong understanding and vested involvement for a governance structure that helps the organisation:

- Stay on track and in lockstep with strategy
- Execute on different workstreams by providing the appropriate skills for the transformation
- Clear organisational barriers
- Account for the expected outputs of each function

From technology vendors to internal team members, organisations should take an "assume nothing" approach to governance so people clearly understand expectations from the start.

Champion organisational change management to quell anxiety

Transformational change initiates a ripple effect as some impacts are not apparent on the surface. Anticipating the impact of change for both internal resources and external third parties and implementing organisational change management plans that positively address the impact should be important initial objectives for CIOs to ensure buy in and quell anxiety.

Fear of the unknown and possible job elimination can significantly hinder productivity if transformation ambiguity causes attrition. Creating transition plans to ease job security fears can save an enterprise transformation. Candid discussions and communicating frequently about changes to responsibilities and job functions offers employees reassurance, helping keep key resources where companies need them to achieve transformation goals.

Align project resourcing and methodology

CIOs should establish a methodology such as Agile or Waterfall to conduct the transformation, and determine KPIs to track progress, establish the team's skill set and align project resourcing with all aspects of the methodology. Everything from timeline, budgets and costs to roles and responsibilities is aligned to the methodology. Defined levels of reporting are set through tools such as a RACI matrix, leaving no room for ambiguity in decision making. The methodology sets the structure for the transformation and reduces inconsistent processes. Successful transformation requires the CIO to implement the right quality measures and quality control, to communicate early and often, and to structure project resourcing to mitigate against "cliffhanger" deadlines.

Optimise offshoring efforts

Repeatable components of transformation that have clear inputs and outputs lend themselves to offshoring. However, offshoring has its own benefits and challenges. CIOs must understand their team's skill sets to make ideal offshoring decisions that fill resource gaps and offer cost benefit. When offshoring, organisations should define expectations for:

- Roles and responsibilities, including quality standards and relationship owners
- Communication protocols, including time zone differences and methods for communicating
- Service-level agreements, so progress and quality can be tracked and deadlines met

Well-defined offshoring responsibilities mitigate ambiguity and prevent tasks from falling through the cracks.

Collaborate to gain an understanding of people impact

CIOs should collaborate with the C-suite and listen with the goal of understanding the "people" impact on each area. Team member involvement, impact to operations and planning for backfill resourcing should each be considered as they relate to the unique parameters of each C-suite member:

- **Chief compliance officer (CCO), chief risk officer (CRO) and chief audit executive (CAE)** — Ensure access is appropriately controlled as responsibilities and permissions are allocated to people or teams that would not normally have access. Resources must be appropriately educated on compliance and controls-related requirements.
- **Chief data officer (CDO)** — Changes to critical data models and data governance will be impacted. The CIO should collaborate with the CDO to secure data and incorporate any impacts to the data strategy in the plan.
- **Chief marketing officer (CMO)** — Digital transformation may alter the way a business's customers interact with the organisation. If an organisation is not equipped to provide the necessary support for the new interactions, there may be poor user experiences. Ensuring the marketing plan is aligned with the transformation is key.

What should companies do now?

While every organisation's transformation journey is unique, there are common features for how project resourcing boosts successful transformation, including:

- **Defined vision and expected value** — Organisations must go beyond meeting timelines and reaching a transformation "end" point. They must strive to improve efficiency, reduce spending, increase automation and eliminate manual errors. They must ensure that project resourcing is aligned with goals and strategy and establish ways of measuring KPIs at the outset.
- **Stakeholder mapping and engagement** — For successful project resourcing, companies must know their stakeholders. They use methods like Design Thinking to gain comprehensive stakeholder inclusion and employ a holistic ecosystem view of project resourcing.
- **Optimal training** — Team members and partners should have clearly defined goals and receive appropriate training so they can understand how they support the transformation and can conform to an established governance structure that serves the corporate strategy.

Unfortunately, project resourcing is not without limits. To balance the trade-off between costs and budget limitations and achieving transformation goals, CIOs must assess resourcing beyond the transformation. Having a game plan for how resourcing will transition into the company's steady state after the transformation will help set strategy and expectations early, ensuring success.

AUTHORS

SAMIR DATT, Managing Director, Technology Strategy and Operations, Houston
MATT DAVIS, Managing Director, Technology Strategy and Operations, Dallas

Strong Business Continuity Management Brings Resilience

At a Glance

Business continuity management (BCM) brings resilience to organisations as they transform digitally. For the greatest ROI from efforts towards resilience, CIOs should:

- Champion business requirements
- Consider the cloud as a way to build resilience
- Obtain buy-in from business leaders and steering committees
- Implement more disciplined validation and testing

Business disruptions happen every day and can cause companies to lose millions of dollars and suffer reputational damage. But these losses can be minimised. When astute executives, including CIOs, cheat disruption by focusing on business continuity management (BCM) programs that build resilience, interruption is conquered so that enterprise transformation can prosper.

CIOs should apply a business lens that informs how the business could be impacted (operationally, financially, legally, etc.) in the event of a disruption, and design solutions to minimise the impact. They must build resilience by analysing the core operations driving the business and identifying critical business services. Understanding business requirements across the organisation as they relate to resilience and remaining dynamic when business conditions change is key. As importantly, CIOs must account for the criticality and timing of each business process, from front-office processes such as sales and customer services to back-office processes such as human resources and finance.

Next-level organisations go a step further and use business continuity and resilience as a *competitive advantage*. Customers want to do business with organisations that do not miss a beat. Customers do not want to wait — they want what they want, when they want it, and that "when" is now. Companies that showcase resilience and build it into their value proposition gain a competitive advantage. But the issue of operational resilience expands beyond businesses. Supervisory authorities such as those in the financial services industry are bringing operational resilience into the limelight with discussion papers and proposals to enhance resilience.

Champion core business requirements

The CIO's customer is the business itself. As such, the business's needs must be understood. This is key to solution design. Proactivity also is a must. Asking the right questions for an understanding of the business's strategy and implementing architecture today that supports the technology of the future is fundamental. Similarly, CIOs and CISOs must anticipate technology needs to build an IT infrastructure that defends against cyberattacks. No longer a risk of tomorrow, cyberattacks are a real threat that BCM and IT leaders must be prepared for now. Understanding business requirements, from technology recovery requirements to data loss tolerance, enables a dynamic technology strategy that morphs with the changing needs of the business. To gain a strong business understanding, CIOs should evaluate:

- **Recovery time objective (RTO)** — The length of time a business process can be without key technology (e.g., business applications, data sets, devices)
- **Recovery point objective (RPO)** — The amount of critical data a process can afford to lose before there is intolerable impact — also known as data loss tolerance

Conducting a business impact analysis (BIA) is critical to identifying business requirements. BIAs enable an understanding of business activities and their outputs to position RTOs and RPOs as inputs into the transformation effort. However, completing a BIA is not enough — it must be maintained over time to allow for continued resilience as the environment changes.

Leverage cloud as a means to build resilience

The availability of robust, secure cloud solutions for disaster recovery represents a fundamental shift in disaster recovery planning. Cloud solutions can be more secure and provide better failover capabilities than businesses can accommodate with their own on-premise environments. For organisations that employ cloud technology for their production environments, resiliency and recovery are intrinsic to the platform, and disaster recovery capabilities are easily added. It is essential for these organisations to possess the expertise to govern and manage cloud implementations, keeping requirements of business process owners in the forefront. When businesses attend to these concerns, configuration of disaster recovery features in the cloud is reasonably straightforward.

Obtain buy-in from business leaders

The business continuity and resilience function cannot be performed in a silo. The CIO must ensure that technology solutions are designed and implemented with input and buy in from leaders across the enterprise, including C-level executives, operations, finance, legal, communications and HR, among others. Organisations should establish a steering committee composed of leaders across the organisation who frequently collaborate on all issues related to BCM and resilience. Business leaders who are invested devote the time, people and resources needed for a successful BCM program.

Implement more disciplined validation and testing

CIOs must test against what could happen and stay disciplined in their validation and testing approach. A more disciplined methodology to validation and testing is essential to sidestepping shortfalls in meeting business expectations. If business leaders expect only 12 hours of downtime from a business interruption but technology workarounds require 48 hours, devastating consequences could ensue, including increased costs, reputational damage and other downstream effects. Testing and validation that back up technology assertions depended upon by stakeholders are elemental.

Collaboration is an all-way street

While technology is a driver for business resilience, it is not the *only* driver. People, processes and other factors must be considered. CIOs must understand the driving factors of C-suite members and, likewise, C-suite members must understand the driving factors of the CIO. Modern CIOs proactively collaborate to understand needs, and they ask questions that inform how IT staff can assist and what technology must do to fulfill business demands.

Impact on the C-suite

While the impact that disruption brings to each C-suite member can be industry specific, there are key considerations across all organisations regarding resilience.

- **Chief financial officer (CFO)** — Transaction processing delays cripple the CFO and the finance function by impeding the processing of financial information. With disruption, unplanned costs arise, most of which are the CFO's responsibility. Engaging the CFO and collaborating on planning for cost minimisation are key.
- **Chief risk officer (CRO)** — Complying with regulatory guidelines may be challenging during times of disruption, especially in heavily regulated industries. Penalties for noncompliance — in addition to having to report such deficiencies to the organisation's leadership — can be damaging. Designing resilient technology solutions enables compliance with regulatory requirements while also mitigating secondary fallout. Commercial insurance is another critical risk-mitigation tool used to reduce operational risks. Organisations may acquire insurance to protect the tangible assets (e.g., workers, equipment and buildings) of the organisation and/or to defray the cost of unexpected liabilities (e.g., civil lawsuits, regulatory investigations).
- **Chief information security officer (CISO)** — The CISO develops the cybersecurity program for an organisation and drives the IT security strategy and implementation while protecting the organisation from cyber hacking and security threats. To ensure there are no gaps in IT and the cyber control environment, the CIO and CISO need to work closely together.
- **Chief audit executive (CAE)** — To optimise risk management, the CAE and the BCM function should work in unison to leverage technology for assessing and mitigating risk. BCM, enterprise risk management and internal audit must work together and apply uniform principles to their respective areas of responsibility.
- **Chief marketing officer (CMO)** — Understanding the impact of disruption — from viral pandemics to product delays — is key to a strong BCM program. Involving marketing in resilience efforts is extremely important to understanding which procedures are in place, how to supplement them and how to respond to a disruption event.
- **Chief operating officer (COO)** — Because COOs are responsible for operations that drive the organisation, it is important to design technology solutions that can minimise disruption to those processes, which can vary by industry. Collaboration between the CIO and COO supports operational resilience by applying technology solutions that can minimise disruption and the subsequent impact to the organisation.

What should companies do now?

A complete and deep understanding of the business is critical to mitigating disruption. To design solutions that minimise the impact of a business disruption, companies should assess their current BCM status. CIOs should inventory current efforts to maintain resilience

and determine a desired BCM state and what they need to do to achieve it. It is important to eliminate or modify iterative technology to cut costs. However, while determinable costs are central, soft costs are just as important to mitigate. Idle personnel, employee morale and reputation costs that are not easily definable in dollars can bring down a business.

Organisations can optimise BCM ROI by continually understanding business requirements and designing complementary business and technology solutions that satisfy business objectives during enterprise transformation, inclusive of the following:

- Governance over resiliency efforts should be directed by a steering committee to assess and supplement policy standards, obtain C-suite buy-in and secure resources
- Key processes must be understood via the business-driven BIA, and the potential impacts of disruption must be addressed
- A strategic plan leveraging a BIA to minimise impact and plan for disruption is critical
- Implementing a disciplined methodology to validation and testing so that shortfalls in meeting business expectations can be avoided is imperative

Last, resilience is not a goal that is achieved. It is an ongoing effort earned over time. CIOs who cheat disruption by addressing resilience holistically support an organisation's efforts to come back stronger in the face of adversity.

AUTHORS

MATT WATSON, Managing Director, Technology Strategy and Operations, Washington D.C.
DUGAN KRWAWICZ, Associate Director, Technology Strategy and Operations, Dallas
HIRUN TANTIRIGAMA, Director, Sydney

An Ecosystem Approach Expands Business Potential

At a Glance

Busy CIOs may have an opportunity to tap into an unexplored gem to boost transformational growth. CIOs can leverage an ecosystem business model (EBM) approach to support technology transformation if they:

- Determine modernisation goals and objectives
- Evaluate current capabilities
- Fill gaps by exploring the ecosystem of solution providers

For companies undergoing a technology modernisation and transformation effort, considering an ecosystem business model (EBM) is key to success. Busy CIOs consumed with never-ending technology demands may be missing massive growth potential and opportunities unless they are nurturing an ecosystem business model. Ecosystems can drive dramatic change within an organisation and enable rapid innovation as companies within the ecosystem co-evolve their capabilities and work together to develop superior solutions that can disrupt markets.

CIOs should continuously evaluate the innovation potential of technologies across their EBM to transform and modernise their organisation. Doing so creates awareness of the organisation's specific business needs and enables the organisation to achieve critical objectives.

Determine modernisation goals and objectives

From a bird's eye view, enterprise transformation requires several critical components to effectively evaluate the enterprise's architecture, establish a modernisation strategy and address data security and privacy issues.

However, the key to building a strong EBM is in gaining a deep understanding of the organisation's modernisation goals and objectives, which may include educating clients, reaching new customers, building new products or services, or operating more efficiently and cost-effectively. Corporate goals inform which capabilities need to be explored further for transformation.

Evaluate current capabilities

CIOs must inventory their organisation's current capabilities, both in technology and in people with the skills to adopt and implement the technology successfully. In many cases, the business lacks the skill sets to implement or optimise, so having a service

partner to assist is important. Evaluating the current state of the company's ecosystem and mapping it to current capabilities is critical for an EBM to enable transformation. A current state assessment should include an inventory of technologies used throughout the organisation, capabilities of tools and platforms, current licencing and a holistic view of vendor roadmaps that can address any gaps. Not doing so may delay or stall transformation initiatives, impacting the agile delivery of potential value to the business.

Case in point: a multinational technology corporation assessed vendor capabilities in their current environment to develop technologies for the modern workplace. They wanted to roll out technology in a more digital-savvy way versus using the heavy coding and longer cycles needed for developing an application. An ecosystem vendor within their global EBM already had such a capability. Evaluating the company's current capabilities, along with the vendor's roadmap and how it linked to the goals and objectives, enabled transformation goals in an accelerated manner.

Fill gaps by exploring the ecosystem of solution and service providers

Companies must work strategically with ecosystem partners and understand the full capabilities of each partner's technology or service and what it can bring to the organisation. Tools such as a market analysis can help determine vendor capabilities, which then enable an organisation to map the vendor's capabilities to various areas in the organisation with current needs. CIOs then leverage the capabilities of ecosystem vendors to fill gaps in the company's own abilities. A strong partnership enables a 360-degree feedback loop between the organisation and vendor or service provider. Organisations can provide input about areas where gaps can be filled, driving change or development on the vendor or service partner's roadmap. The vendor partner then can deliver the capability in the next product development round. The partnership influences the partner's roadmap to introduce particular services, features or enhancements, and the organisation's gaps are closed. Having regular product roadmap sessions with a vendor enables continuous collaboration to enhance innovation in applications.

As an example, a major farm equipment manufacturer leveraged its EBM to modernise the way customers used its equipment, ultimately disrupting a highly commoditised industry. The company embedded its ecosystem partner's devices into farm equipment, capturing critical data, and then opened that data to application developers. A new digital application was created that allowed customers to transform their entire business, operating equipment remotely and monitoring their crops, including soil and water levels, using their mobile phones or tablets. This enabled the organisation's customers to increase efficiency and improve outcomes and enabled the equipment manufacturer to differentiate itself in the market.

Collaboration leads to continuous enhancement

EBMs lean on collaboration to open the doors of unlimited possibilities and enhance areas of the organisation. Generating different ideas and perspectives elevates and expands product offerings and services. It enables viewpoints for solving problems through a diverse lens and widens the business' vision to include solutions it may not have considered otherwise.

Permeate EBM value throughout the C-suite

Business ecosystems can have pervasive impact. To access EBM value that permeates the organisation, relevant roadmap information and EBM strategies should be shared with C-suite members and other leaders so they can access partner technologies. Steering committees can help communicate regularly with the organisation's decision-makers to give everyone a voice, share information and proactively

share ecosystem strategies. CIOs should understand that functional areas across the organisation can benefit from an EBM, but working with or bringing a new ecosystem partner onboard can impact the work of other C-suite leaders.

- **Chief innovation officer** — The chief innovation officer has unlimited opportunity to collaborate across emerging technologies and tools. They create value by bringing new IP to market through joint collaboration for solutions that are only achievable by combining experts from both companies.
- **Chief financial officer (CFO) and chief audit executive (CAE)** — The CFO and CAE have a unique opportunity to leverage advanced analytics strategies for financial reporting. Doing so enables a more efficient EBM.
- **Chief sales officer (CSO)** — An organisation's EBM can be propelled by CSOs who open doors to diverse revenue streams and go-to-market opportunities through reselling, referrals, joint IP creation and solutioning. Likewise, they enhance margins and expand market share by broadening sales reach through alliance referrals.
- **Chief risk officer (CRO) and chief compliance officer (CCO)** — To assess third-party risk, the CRO and CCO must optimise risk and compliance across the organisation's ecosystem by leveraging frameworks, tools and technologies.
- **Chief diversity officer (CDO)** — CDOs are well-positioned to encourage and facilitate external collaboration with companies, leaders, activists and subject matter experts for a resource-rich, diverse ecosystem with an abundance of ideas, innovation and growth.
- **Chief marketing officer (CMO)** — To bolster EBMs, progressive CMOs increase marketing opportunities through external exposure with alliance companies, including logo promotion, conferences, webinars and social media. They elevate the organisation's brand through association with companies of similar values and culture. CMOs can enhance organisational efficiencies, drive revenue and cut costs by leveraging advanced analytics and AI machine learning across big data lakes.

What should companies do now?

Ultimately, companies should develop a capabilities map across key relationships. Capabilities mapping should be aligned with the organisation's goals and objectives and transformation strategy — with the fallout being the gaps that must be addressed. Once gaps are identified, organisations should conduct the proper market research and market scanning to see how other vendors can fill such gaps. Cooperation and collaboration are key to successful transformation efforts that leverage the EBM holistically because they leverage the diverse thinking that drives innovation.

As organisations enrich their EBMs, they should plan to deliver value incrementally — and they should begin early in the transformation process. Transformation programs have long-term timelines. When stakeholders do not see consistent, incremental value being delivered, their enthusiasm drops. EBM results should be consistently communicated to shareholders, stakeholders, customers and suppliers as well, as it substantiates their investment in the EBM. Keeping an ecosystem approach top of mind supports the value that is manifested across the ecosystem.

AUTHORS

CLAUDIA KUZMA, Managing Director, Ecosystems, Chicago
CATHERINE ALPETER, Manager, Operations, Chicago

Amplify Customer Experience to Propel Next-Level Growth

At a Glance

CIOs are challenged with connecting technology to customer experience. They can leverage enterprise transformation and modernisation to improve customer experience if they:

- Anchor to brand purpose
- Use insights to improve customer experience
- Design for customer trust
- Implement change enablement
- Ensure comprehensive input

Customer experience (CX) plays a critical role in organisational success. Customers today are buying based on their experience with a company and whether a product or service aligns with their personal values, including access, inclusivity, sustainability and trust. Customer experience should play the starring role in decision-making and should be woven into technology initiatives.

To optimise technology for CX, CIOs must connect technology to customer value. They should think of technology in terms of customer experience rather than customer process.

Anchor to brand purpose

A company's brand purpose represents the reason a company exists beyond making money. It defines the company's mission and, often, how the company plans to improve the world for the better — and it is a powerful contributor to customer experience and loyalty. Organisations should understand their brand purpose and invest in the technologies that enable, align to and help project that purpose.

Customers can often have multiple varied experiences with an organisation; negative ones can lead to customer attrition. Organisations should gather insights and map the customer journey to understand customer expectations so they can better identify which experiences are the most important and impactful. These journey maps can then inform technology investments and capabilities while building an ecosystem and technology portfolio that links back to customer and brand experience.

Companies that do not anchor to brand purpose run the risk of spending millions of dollars on technologies that do not align to what customers care about. When customers perceive poor experiences, they take their

dollars to the competition. CIOs who demand mapping customer experience to brand purpose support more than technology — they champion business longevity.

Use customer insights

CIOs who are continuously building a better customer experience know the importance of listening to the voice of customers. Customer insights come from many different sources, but data is the strongest foundation for critical decision-making. Organisations should use customer data feedback loops to improve CX.

To extract value from customer insights, CIOs should:

- Make technology decisions using customer experience insights as inputs
- Connect to the voice of the customer to understand customer experiences that matter
- Use data to glean a line of sight for investing in technologies that heighten CX

Design for customer trust

Today's business environment is overwhelmingly dynamic. CIOs and the C-suite must constantly navigate new regulatory demands, customer expectations and disruptive competition. Companies who can respond to change by implementing seamless technology gain an advantage by avoiding disruption to the customer experience and enabling customer trust.

CIOs should design technologies with customer trust in mind, thinking ahead and anticipating future changes as technology is built or designed so the customer experience is as seamless as possible. Organisations should incorporate as much flexibility into the design process as possible. Otherwise, organisations risk lags in response time, a shortfall in anticipating customer needs, a reduction in customer trust and damage to the CX.

Implement change enablement

Employees are an organisation's most effective brand ambassadors, and they are the organisation's internal customers. The more employees are equipped for and transitioned to new technology, the better the internal and external customer experience, making change enablement essential. A strong, comprehensive change enablement program brings a welcome shift in roles and responsibilities as new technology frees employees to perform higher-level tasks. Redeployments may enable critical resources to perform higher-priority tasks so other challenges can be addressed.

Change enablement programs transition employees to using new technology in the way it is intended. Innovative organisations understand that automation is not necessarily digital if it is being used in an analogue manner. Using new technology in an outdated or obsolete way does not support digital transformation. Real automation requires a transition from a waterfall mindset to an Agile approach. When change enablement is implemented using an Agile mindset of experimenting, failing quickly, wire-prototyping, etc., efficiencies can be realised.

C-suite partnerships bring synergistic value

Successful collaboration requires technology and business leaders to work together. With the whole of the C-suite being greater than the sum of its members, each member should focus on applying unique value while working synergistically with the other members and departments of the organisation.

The full scope of stakeholders should have a seat at the design table. Working closely as strategic partners, CIOs and C-suite members should promote collaborative planning norms and ensure all stakeholder voices are heard. Having the organisation's business executives, compliance leadership and CISO at the decision-making table enables an organisation to make appropriate, customer-connected decisions that are focused on outcomes.

A C-suite that understands the art of the possible builds an ecosystem that leverages capabilities, technologies and digital elements to push the organisation towards continuous CX improvement. Each member of the team provides a unique contribution:

- **Chief marketing officer (CMO)** — The CMO works in partnership with the CIO and CDO to enable a seamless online and offline customer experience by leveraging technology through new digital products and services.
- **Chief customer officer (CCO) and chief experience officer (CXO)** — CCOs and CXOs work across the entire enterprise to champion the CX, leading the charge for innovation, reimagination and end-to-end improvement of customer experiences.
- **Chief digital officer (CDO)** — The CDO focuses on end-to-end automation and developing innovative or disruptive digital products and services that bring value to customers.
- **Chief risk officer (CRO)** — Ensuring that the customer experience is aligned with the organisation's risk appetite is a critical role of the CRO, who also must help deliver experiences that protect the customer while aligning with industry requirements, standards and regulations — without adversely impacting the CX.
- **Chief financial officer (CFO)** — CFOs aim for customer growth, bringing CX value and prioritising the organisation's investment in the customer experience capabilities that will have the most significant impact.

What should companies do now to gain the greatest ROI?

To optimise ROI from enterprise transformation and elevate the customer experience, companies should:

- Align efforts across the organisation and its budgets and priorities with a focus on value to the customer and the customer's end-to-end journey. CIOs should enable the optimal customer experience by building a technology road map that considers more than just the systems, incorporating data, privacy and regulatory compliance elements as well
- Ensure the CIO's team understands feedback related to the "voice of the customer" and leverages this feedback to empower investments in the highest-impact strategic initiatives that connect to the experience enhancements that customers value most
- Embrace and apply an Agile mindset to updating software development life cycles, budgetary processes, stage-gating and DevOps. Doing so enables organisations to optimally meet market, customer and employee needs for pace and speed for the most valued features and functions

CIOs and their organisations can have a significant effect to boost their customer experience, as they are uniquely positioned to implement innovative technologies that enable ongoing enhancements to the dynamic expectations of customers.

AUTHORS

BRYAN COMITE, Managing Director, Operations Improvement, New York
JOAN SMITH, Managing Director, Digital Solutions, Phoenix

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

For more information, please contact us at TechnologyConsulting@protiviti.com.

THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA *
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®