IS 460: Enterprise Cloud Computing

Cloud Computing and Enterprise Digital Transformation

Final Research Paper

Yi-Ching Tsai
Simran Singh
Ricardo Sanchez Ralph
Monroe
Teresa George

Contents

Introduction

Cloud computing has revolutionized the way organizations operate by providing easy access to servers, storage, databases, and applications over the internet, allowing them to pay only for what they actually use. This approach accelerates project launches, enables businesses to scale their resources up or down as needed, and helps save money on unused hardware. In this report, our team explores the basics of cloud services and how they can transform businesses. We also tackle real- world challenges like security vulnerabilities, Ata privacy concerns, and compliance issues. To wrap things up, we present a straightforward, step-by-step guide to identifying and addressing these risks, empowering organizations to embrace the cloud with confidence.

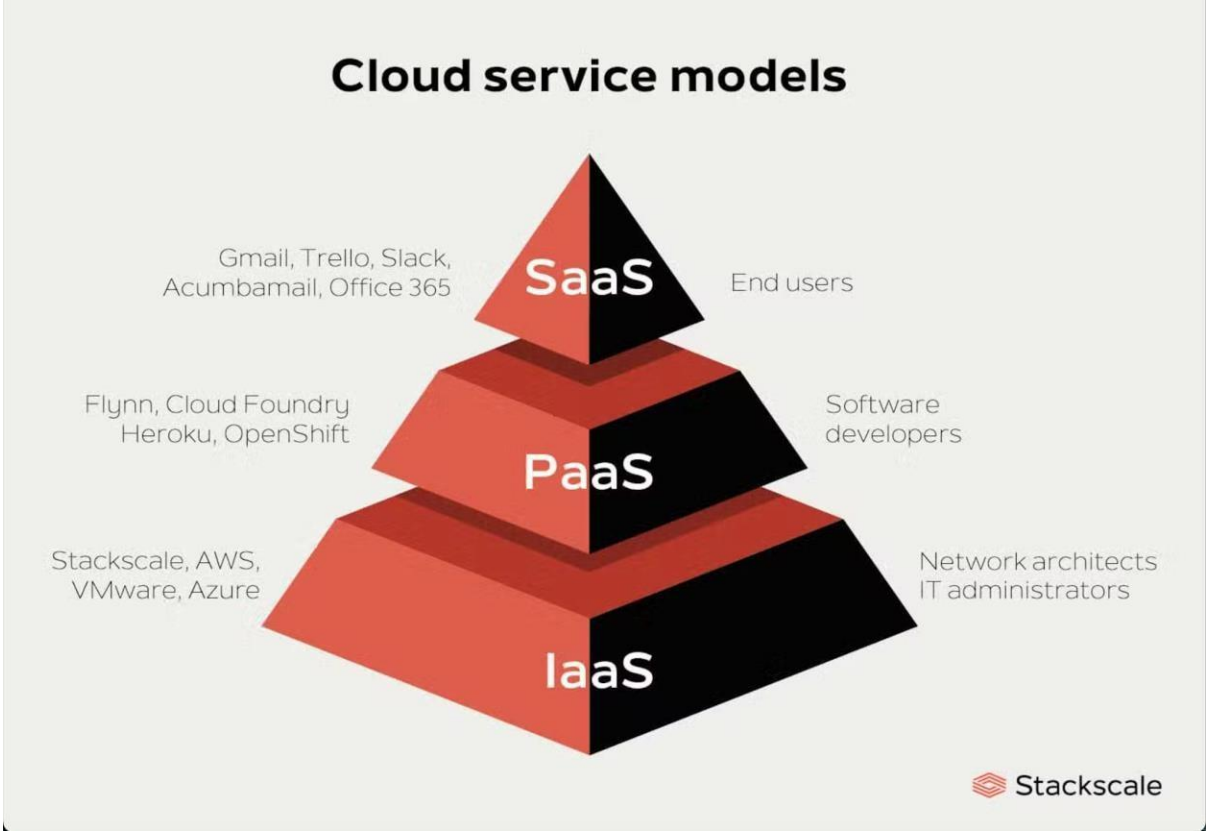
Cloud computing has changed the game for enterprises by offering on-demand access to computing power, storage, databases, networking, and applications through a pay-as-you-go model. This means companies can avoid hefty upfront costs for physical infrastructure and can quickly scale their resources to meet shifting business needs. Consequently, businesses can roll out new features more rapidly, provide a consistent platform for a global workforce, and transition their tech budgets from fixed capital expenses to more flexible operating costs.

But it's not just about saving money; adopting the cloud strategy fosters innovation by allowing IT teams to concentrate on strategic projects instead of getting bogged down with hardware upkeep. Key cloud architectures—like micro-segmentation, container orchestration, and serverless computing—facilitate quick iterations and continuous delivery. Plus, the extensive network of data centers run by cloud providers guarantees high availability and low latency for users. On top of that, advanced services such as machine-learning APIs, serverless event processing, and edge computing are easily accessible, giving organizations of all sizes the chance to experiment with cutting-edge technologies without the need for specialized infrastructure.

While the benefits of cloud transformation are clear, achieving success in this area demands thoughtful planning and execution. In this paper, our team sets out to identify the main factors that drive companies to shift from on-premises systems to cloud solutions. These factors include competitive pressures, goals for operational efficiency, and the need for global scalability. We also take a close look at the various challenges that can arise during migration and ongoing operations, such as security vulnerabilities, data privacy issues, and regulatory compliance. To provide practical

insights, we draw on detailed case studies from the finance, healthcare, and retail sectors, helping organizations navigate their journey toward a secure, resilient, and efficient cloud transformation.

To tackle these questions, we employed a two-pronged research strategy. First, we systematically compared different cloud service models—like infrastructure as a service, platform as a service, and software as a service—alongside various deployment architectures, including public, private, and hybrid. This analysis, based on vendor documentation and market research, gave us valuable insights into the trade-offs related to cost, control, and scalability. At the same time, we delved into real-world migration stories found in white papers, technical blogs, and conference presentations to pinpoint common success factors, pitfalls, and emerging technology trends. By combining model comparisons with practical case studies, our approach offers both clear concepts and actionable advice for enterprises looking to embrace the cloud.



Source: (Stackscale, 2023)

Cloud Computing: Concepts, Models, and Technologies

Cloud computing is one of the most talked-about innovations in the IT world today and for good reason. At its core, cloud computing refers to computing services offered by third-party providers that are available on demand and can be scaled dynamically based on user needs

(Rosenberg & Mateos, 2011, p. 1). Instead of building, managing, and maintaining their own IT systems, organizations can now access services like data storage, networking, and computing power over the internet.

The change in how we use and deliver computing resources has major advantages. Economically, cloud computing can significantly reduce infrastructure costs. It also allows companies to be more flexible and agile by giving them the ability to quickly adjust their resources as needed (Rosenberg & Mateos, 2011, p. 3). Five core principles that define cloud computing are shared computing resources among users, virtualization, which makes better use of hardware by running multiple systems on the same physical machine. Elastic scaling, which allows resources to grow or lessen with demand.
Automations, so that virtual machines can be created or removed without manual setup and lastly, pay-as-you-go billing, where users are only charged for the resources they actually use (Rosenberg & Mateos, 2011, p. 3).

Page 8 in our textbook discusses the importance of cloud computing in modern IT infrastructure. It talks about how cloud computing has become a key part of today's IT systems, not just for convenience and scalability, but also for security (Rosenberg & Mateos, 2011, p. 8). Cloud providers
often offer stronger security than traditional, in-house data centers. However, companies still need to weigh the pros and cons carefully, considering factors like performance, reliability, and their specific needs. But with the right planning, the cloud can offer powerful benefits.

Cloud computing services are offered through different models, each offering varying levels of control, flexibility, and convenience. The three main services models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

IaaS provides computing resources like virtual machines, storage, and bandwidth. An example is Amazon EC2, which allows users to choose virtual machine images based on different operating systems. With IaaS, users are billed based on consumption, such as how long a virtual machine is running, how much data is stored, and the bandwidth used for data going in and out. While this model does offer a lot of flexibility, it also requires more work from developers to configure and manage the environment (Rosenberg & Mateos, 2011, pp. 15-16).

PaaS takes things a step further by taking care of most of the infrastructure work for you, so developers can focus on building their application. Unlike IaaS, you don't have to deal directly with operating systems. Platforms such as Google App Engine and Microsoft Azure handle that part,

allowing you to simply write and deploy your code. Even though PaaS makes development easier, it can also come with some limitations. For example, you may need to use certain programming languages or tools supported by the specific program (Rosenberg & Mateos, 2011, pp. 15-16).

SaaS delivers fully developed applications over the internet on demand. These services are ready to use and don't require installation or maintenance by the end user. An example is salesforce.com, which provides tools for sales, customer relationship management, and more. Users typically pay a subscription fee or license to use the software (Rosenberg & Mateos, 2011, pp. 15-16).

Cloud deployment models define how cloud services are made available to users. The primary models are Public Cloud, Private Cloud, and Hybrid Cloud, each offering its own advantages and differences. A post from Aztech IT Solutions (2023) talks about the main differences between these models which I will be discussing.

The public cloud is a model where services like storage, computing power, and networking are delivered over the internet by third-party providers. These services are shared among multiple users. Public cloud platforms are commonly used due to their cost efficiency and flexibility. According to Aztech IT Solutions (2023), some benefits of public cloud are lower costs, greater flexibility and agility, easy scalability, built-in security features, and minimal maintenance. Public clouds are mostly more budget-friendly. Businesses only pay for what they use, and they avoid large upfront costs for hardware or software. With public clouds, it's simple to increase or reduce computing resources based on demand, this is especially helpful for businesses with fluctuating workloads.

Even though the public cloud has these benefits, they also have some limitations such as security risks, downtime and availability, and cost management. Even though public cloud is affordable, the costs can add up overtime, especially when moving large systems or handling complicated setups. Public cloud services can experience outages due to issues like server crashes or internet disruptions and although providers offer strong security tools, the fact that public cloud resources are accessible from anywhere makes them a potential target for cyberattacks. Some examples of public cloud providers are Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, and many more.

A private cloud is a type of cloud environment that is for a single organization. Unlike public clouds, which are shared by many users, a private cloud is either managed internally by a company or hosted by a third-party provider but still used by only one organization. This gives businesses more control over their systems while still providing the flexibility and scalability of cloud computing.

According to Aztech IT Solutions (2023), some benefits of private cloud are stronger security, faster performance, and better flexibility. Since private clouds are isolated from public access, they provide a safer space for storing sensitive data. Companies can have extra protection like encryption, two-factor authentication, and more. Since everything is kept together in one private system, data can be accessed more quickly, which helps make things run smoother. Because private cloud has better flexibility, businesses can adjust their computing resources such as storage, memory, and processing power, without investing in new hardware.

There are also some limitations when it comes to private cloud. Such as higher costs upfront, limited scalability, and less flexibility. Setting up a private cloud can be expensive, this involves costs in hardware, software tools, and qualified IT staff. Unlike public clouds that can expand resources instantly, private cloud scalability may be limited by the physical infrastructure in place. Also, businesses using private clouds are often with a specific provider or internal system, which can limit what services they can use or how much they can customize their setup. Some examples of private cloud services are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

A hybrid cloud combines both public and private cloud environments, allowing organizations to run their workloads in their own secure systems while taking advantage of the scalability and flexibility of public cloud services. It gives businesses the best of both worlds, control and security where needed, and cost-effective, on-demand access to resources when required. Hybrid companies manage operations more efficiently while keeping critical data safe.

Some benefits of hybrid cloud are cost efficiency, improved security, and high availability. Hybrid cloud helps businesses save money by balancing resources between private infrastructure and cost- effective public services. Companies can purchase only what they need and use public cloud resources to scale when necessary. With hybrid cloud, businesses can keep their most sensitive data and operations on a private network while using public cloud services for less critical tasks. And by spreading applications across multiple environments, hybrid cloud reduces the risk of downtown caused by disasters. According to Aztech IT Solutions (2023), some examples of hybrid cloud use are multi-cloud strategies and public-private cloud split.

Security challenges, increased complexity, and higher maintenance costs are some of the limitations of hybrid cloud. Since hybrid cloud involves multiple platforms, it increases the number of access points that must be protected. Managing a hybrid cloud can be complicated. It requires coordinating

different technologies, vendors, and environments while making sure they all work well together. Even though hybrid cloud can reduce costs in some areas, maintaining both public and private systems can add up. According to Aztech IT Solutions (2023), some examples of hybrid cloud use are multi-cloud strategies and public-private cloud split.

Serverless computing is a cloud model that lets developers deploy and run code without managing servers or infrastructures. The cloud provider takes care of everything behind the scenes so developers can focus only on building their application (Cloudflare, n.d).

One of the biggest benefits of serverless computing is its on-demand pricing model. Businesses are only charged for the actual time their code runs, which results in major cost savings, especially for applications with unpredictable workloads (Cloudflare, n.d).

Serverless also enables quick scalability and faster development cycles. Since the infrastructure scales automatically with demand, developers don't need to worry about setting up backend systems. It's a great fit for services that need to scale quickly and deploy fast, though it may not be ideal for every type of web application (Cloudflare, n.d)..

Edge computing is a growing trend in cloud technology that focuses on processing data as close as possible to where it is created. Instead of sending all information to a distant cloud server, edge computing handles many tasks on devices like smartphones or nearby edge servers (Cloudflare, n.d). This approach helps reduce delays and cuts down on the amount of data being sent across long distances.

By keeping more processes at the “edge” of the network, businesses can get faster responses and reduce their dependence on centralized cloud infrastructure. This is especially useful for time- sensitive applications like self-driving cars and IoT devices that need real-time decision making.

An article from *Oracle* talks about the roles and benefits of AI in Cloud Computing. Artificial intelligence (AI) and cloud computing are closely connected. In large-scale data centers, AI plays a critical role in completing tasks like scaling resources, identifying system errors, monitoring for cyber threats, and spotting potential fraud (Erickson, 2024). This helps providers manage a large infrastructure more efficiently and also supports millions of users at once.

Today, the cloud has also become the main way businesses integrate AI into their own operations. Many software-as-a-service (SaaS) platforms now come with built-in AI features. Some companies even use cloud-based platforms to build and train their own AI tools (Erickson, 2024).

AI is important to cloud computing because AI helps cloud companies deliver fast, reliable services at a lower cost from managing resources and performing system maintenance to delivering SaaS applications. At the same time, as more businesses start to use AI, cloud computing is becoming the simplest and most effective way to access the technologies. AI also depends heavily on cloud computing. Training AI models requires a lot of computing power, which many organizations can't afford to build in-house (Erickson, 2024).

Enterprise Digital Transformation: Drivers and Frameworks

Cloud computing is a part of the current digital transformation. Digital transformation is a strategic decision an organization makes to implement technical solutions across all areas of their business. Some drivers for which digital transformation is moved forward include organizational, technological, and customers. Not only are there drivers pushing forward transformation, but frameworks have been created to help businesses highlight their gaps and their digital transformation progression.

This current trend takes into consideration a business' process, products and services, operations and technical infrastructure. The purpose for why an organization moves forward with digital transformation is because they believe it will drive business growth by meeting market expectations.

Not only is the bottom line impacted, but digital transformation targets change in how a business operates, reforming its processes, user experience, and employee experience. It is essentially ensuring an organization is keeping up with current advancements and not getting lost in the rapid changing society. Otherwise companies risk falling behind competitors or losing customers.

Moreover, in the current society, people are used to having the convenience of technology at their fingertips. This has shaped the expectations of the consumer. The ability to perform their work responsibilities and live their lives is made efficient with the latest technology. Thus, digital transformation is a must for companies to attract and retain customers, hire skilled workers, and grow its value in the market.

Digital Transformation Key Drivers

A key driver of digital transformation is the culture from within the organization. It is bolstered by business leaders who have a mindset that embraces change. Change is inevitable, especially when it comes to technology. So, having leaders who fosters a culture of collaboration, tech adoption, and a customer-centric approach helps drive an organization's digital transformation.
Furthermore, a culture that's data-informed has a good foundation for change. This is because data reveals behaviors and patterns, thus providing decision makers with insight into trends. With a culture that is data-informed, it can be easier to agree to make a digital advancement, if the data analysis is revealing that is what needs to be done.

Lastly regarding culture, a business that embraces the agile methodology can be flexible and more dynamic with change. For example, an agile culture can navigate a seamless digital transformation because the process will be broken down into short phases for sprints. No matter how much things change, one of the main drivers for digital transformation takes place internally.

If a business has not fostered a culture of agility, being data-centric, and collaborative, they will have a difficult time with transformation.Another driver in digital transformation is technology. Technologies such as cloud computing, and now AI has accelerated digital transformation. Each new technological advancement brings efficiency that businesses can take advantage of to increase its value.

First off, if we focus on cloud computing we see the strategic opportunities cloud computing provides such as cost efficiency, scalability, increased security, and flexibility for a business. Cloud computing is cost efficient because the annual overhead cost of hardware, which is an operational cost, can be reduced with cloud computing. Instead of paying for its own hardware and maintenance upkeep, businesses can now pay for only what they need.

The purpose of any business is to make money, but more importantly increase its profit margin. As such, business leaders are attracted to products or services that will help lower their operational costs without decreasing the value of their own products or services.

This leads to another opportunity for businesses, which is scalability and flexibility. Ever since the Covid-19 pandemic business, organizations, and governments were forced to innovate. Peter Drucker says there are seven specific sources for innovation: unexpected occurrences, incongruities, process

needs, industry and market changes, demographic changes, changes in perception, and new knowledge. So, like a cascading effect, these seven sources were impacted on a global scale, and it highlighted the need for businesses to be flexible and scalable.

Cloud computing allows a business to be scalable by providing services that can grow or scale down depending on the needs of the business. For example, a small business may have virtual desktops on the cloud and increase or decrease the amount based on growth or reduction. Furthermore, the flexibility of cloud computing is another strategic opportunity because employees can access applications remotely from the cloud. Thus, cloud computing broadens an enterprise's ability to bring in high-end talent remotely.

Along with having remote workers, a business who uses cloud computing has the advantage of having a virtual "office". In November of 2024, Gallup released data showing an increasing trend that 75% of U.S. employees with remote-capable jobs would prefer either remote or hybrid work. With this increasing rise a business needs to ensure their remote employees can access what they need and collaborate seamlessly. Cloud computing's infrastructure enables co-workers to access and work on the same data and files.

Another important opportunity cloud computing provides is increased security, such as automated regulatory compliance, increased resiliency, and continuous visibility. With cloud computing businesses can save time and resources by setting up compliance policies that automatically update to regulations within their industry. Another benefit to cloud security is ensuring data is continuously protected because the worry of a physical server failing is gone. Lastly, according to St. Bonaventure, having continuous visibility allows teams to better examine threats and find ways to improve security.

Machine learning and AI are technologies that companies are leveraging and concurrently driving digital transformation. Businesses are using AI to drive strategies by adopting predictive analytics which can help automate processes, reduce cost, and personalize the customer's experience.

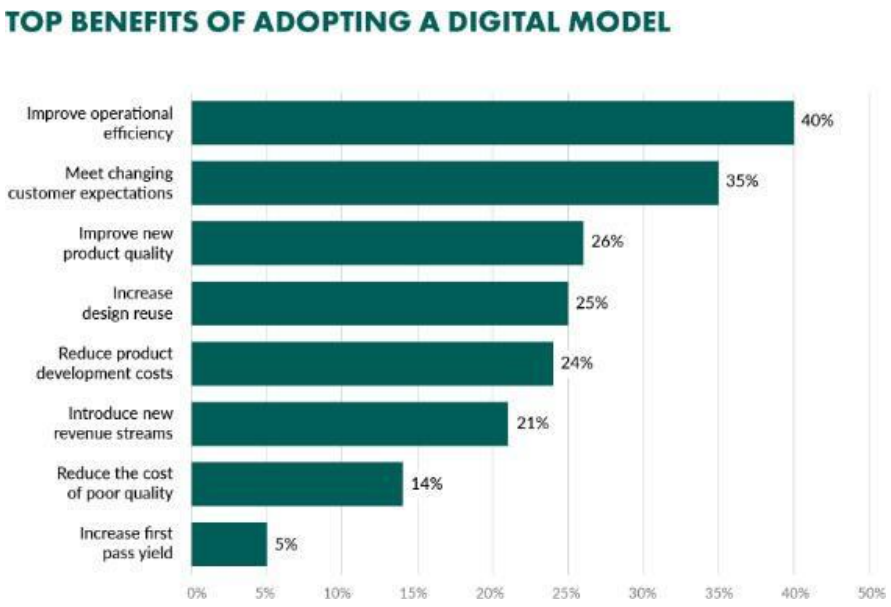
Along with the heavy use of data for machine learning and AI, organizations must seek how they will manage, organize and control its data, also known as data governance. This employs a whole new set of risk management, policies and processes. Without data governance, companies can face the

consequences of security vulnerabilities, ethical missteps and operational inefficiencies. Machine learning and AI are driving digital transformation, not only because it enhances the customers experience, but it upgrades the employee's experience. A business can integrate AI within its systems architecture, allowing AI to understand the organizations systems, networks and applications. This will allow employees to utilize a resource with the capacity to provide data or information that's needed in a seamless way.

Lastly, AI is a technology that's driving digital transformation because of its profitability. For example, a company who has a team of developers, can utilize AI to help them catch bugs or solve errors in their code faster than if a human was examining the code alone. This helps reduce time while providing value, thus helping in the profitability of the company.

One of the most important drivers for digital transformation are the customers themselves. Without customers to buy or use the product or service from a business, then that business would cease to exist. The customer who becomes a consumer validates the value of a business. It is the customers who are dictating the strategy of the business and overall they are the ones driving digital transformation.

To keep us with the "always-connected" customers, the business must embrace technology to deliver an unmatched customer experience. This quote highlights how today's customer is essentially attached to their device and are used to having everything they need in the palm of their hand. So, they will expect nothing less when they engage with a business. The data backs up the driving force behind the customer being the catalyst for digital transformation. Also, 35% of business executives say that digital transformation for their companies happened to meet the changing customer expectations. (SuperOffice, 2025)



(SuperOffice, 2025)

When companies embrace digital tools and systems, they position themselves to meet customer needs more effectively. Surveyed data from Deloitte show that organizations with higher digital maturity saw a 45% increase in revenue. These same organizations also reported stronger performance in growth, innovation (29%), and sales and marketing (41%).

What this tells us is that customers are shaping the direction of digital change. Businesses that listen and adapt to those needs tend to thrive. A McKinsey study reinforces this, noting that companies that digitize their supply chain can increase annual earnings by as much as 3.2%. When companies use digital transformation to stay aligned with customer behavior, it not only boosts performance, it can build trust and loyalty over time.

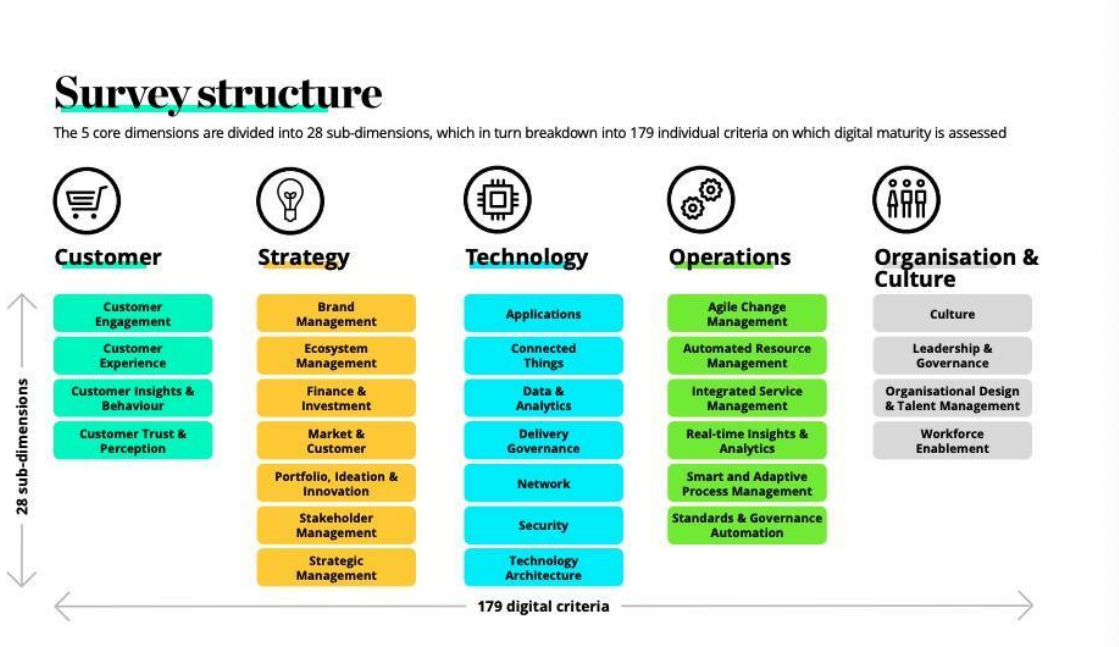
Digital Transformation Frameworks

How does a business know it's ready to undertake a digital transformation? A comprehensive assessment needs to be done to highlight how a company can improve its digital prowess. The digital maturity model is a framework that helps ensure a business is ready for a digital transformation. The Deloitte Digital Maturity Model and McKinsey Digital Quotient are quite similar, but have some differing focuses.

Digital Transformation Framework Comparisons		
Entity	Deloitte's Digital Maturity Model	McKinsey Digital Quotient
Examines	Business strategy, organization, capabilities, insights and customer experience.	strategy, capabilities, organization, and culture
Purpose	Seeks to align digital initiatives with business objectives and foster a culture of innovation.	Highlights the importance of leadership, talent management, and digital mindset to drive successful digital transformation.

Deloitte was excited to be the first industry-standard digital maturity assessment tool. Launched on May 16th 2017, this new framework was designed to empower business along each part of their transformation. Deloitte thought that there was no clear industry-oriented roadmap and thus with no clarity, it hindered the progress for digital transformation. By collaborating with global businesses, Deloitte's model is the first pan-organization digital maturity model. (Deloitte, 2017)

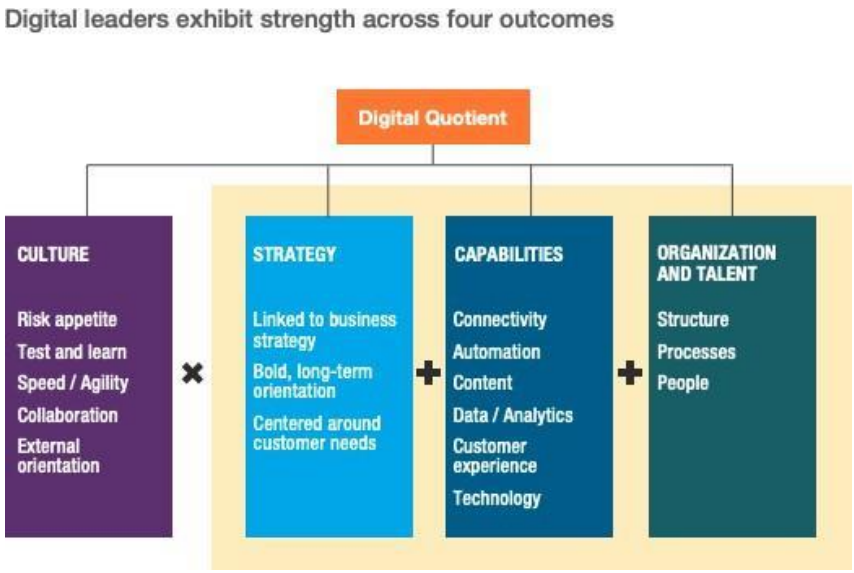
This model focuses on five business dimensions: the customer, strategy, technology, operations, and organisation and culture. Each of those dimensions are then broken down into 28 sub-dimensions. Using this model, a business must assess its current technologies and identify new digital opportunities for the future. Then it takes the potential opportunities and refines them down to a micro level to fully assess its impact within every business aspect. Finally a plan is created to test the new digital concept before full implementation takes place.



(Deloitte, 2018)

Another framework is McKinsey's Digital Quotient, which focuses on ensuring companies have specific attributes and management practices to lead to digital and financial success. Based on their analysis, McKinsey found that a company having expertise in technology or the newest tech is not the barometer for digital maturity. What they found is that digital maturity is truly impacted by the behaviors of the management team and culture.

Within the Digital Quotient the first point of order is culture. The Digital Quotient seeks to understand the business culture and their appetite for risk, ability to learn, speed and agility, collaboration and external orientation. The next component is strategy aims to understand business strategy, more specifically its digital strategy. The third component, capabilities, looks for gaps within the company asking questions such as, are they making data-informed decisions?, do the leaders embrace technologies?, and is there a focus on automation? Lastly the Digital Quotient focuses on an organization's people, processes and structure. An assessment is made to see if there are digital champions among the talent, and is there communication regarding digital key performance indicators. (Catlin, Segev, & Singer, 2015).



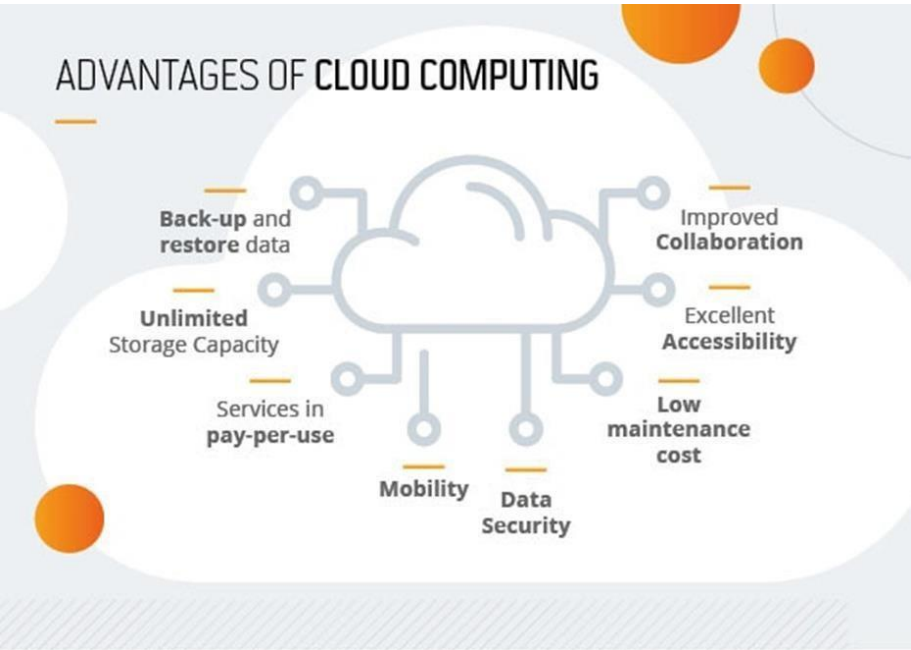
(Catlin et al., 2015)

All in all, the frameworks for digital transformation must be comprehensive. One can argue that determining an organization's digital readiness for transformation is less about technology and more about its leaders, the people, the culture, and processes. Each company must decide which framework or model that is best suited for them and their digital transformation goals. No matter which framework is chosen, the extent of successful digital transformation can be determined based on how honest and comprehensive the assessment is, analyzing the results and developing a thorough roadmap.

Cloud & Digital Transformation Intersection

We live in a world today where technology is always evolving and these enterprises are turning to cloud computing at a higher rate as their way of conducting digital transformation strategies. When looking at the benefits of cloud it comes with the flexibility in their operations, allows them to innovate at a faster pace, and also allows them to change with the demands of the market as they see fit. When looking at cloud computing as a whole it is evolving and now integrating the use of Artificial Intelligence, Business Intelligence, and even Big Data Analytics. With the use of these technologies it allows them to run their business a lot more efficiently and also speed up the pace they operate at. It has been seen across many industries that when adapting cloud technology to support their digital transformation strategies they have all seen the benefits provided by cloud.

Cloud Transformation Support



Flexibility and scalability are one of the main advantages that enterprises see when they are looking to implement cloud technology. This is a huge advantage as it allows an enterprise to scale up and down at will which only helps the operations of the enterprise. When looking at the demand an enterprise may receive they are able to scale up or down with ease and can meet the demands of the market.

Because they can meet demands from the market this allows them to use and allocate their resources wisely. " Migrating to the cloud allows organizations to buy as much storage space and computing capacity as they need, which is ideal for rapidly growing enterprises" (Tanner, 2024). This is an example of what these enterprises are able to do with cloud technology as they are able to have any amount of storage space and computer capacity readily available for them to use and help innovate the company. Another benefit for the company is that when they move onto cloud there are cost benefits and efficiency benefits as well. One of the ways that these enterprises can achieve these benefits is by using the pay-as-you-go model which allows the enterprise to only pay for the resources that they need to operate. By using the pay-as-you-go model the enterprise can lower maintenance costs as they will be on the provider to keep the service running and the enterprise only has to worry about paying for the service and using it to the benefit of the company. The use of cloud computing can also increase the compliance and security abilities of the enterprise. When looking at the cloud providers and what they provide for the enterprise it is seen that in their security systems they offer features like encryption, identity management, and threat detection which are some features that will help protect the enterprise and its data making sure it also follows any compliance rules.

Technology Integration

Cloud is also constantly integrating new forms of technology which help keep its software up to date to make sure it is the most optimal software. In this new age of technology data-driven decision making has become an essential part of success for any enterprise seeking to be successful. Big Data and Analytics is a huge reason companies want to integrate cloud in their enterprise. By using cloud-based analytic tools companies can take in a large amount of data and be able to process it and turn it into advanced insights and information that will turn it into decisions that will be more accurate and beneficial to the company. One of the tools used by these companies is Google Cloud Platform which facilitates the process of gathering and storing data and analyzing the data for the best results possible. Another benefit that cloud computing offers these enterprises is the ability to process data in real time. This allows companies to gather data and analyze it almost instantly and it gives them the ability to make real time decisions that are accurate. This feature is used when a company is looking to follow emerging trends and stay ahead of them ensuring success. Overall Business Intelligence tools are a huge part of cloud computing and help ensure company success and competitiveness in their field.

Artificial Intelligence is one of the new and emerging forms of technologies that is finding its way into cloud computing. The use of Artificial Intelligence and Machine Learning is currently changing the cloud computing industry. Cloud computing platforms allow these enterprises to use the computing power and storage they need to be able to implement these new Artificial Intelligence and Machine Learning Models. One example of this being used is in Microsoft Azure. Microsoft Azure now has integrated Artificial Intelligence models like ChatGPT into its service which helps them better the experience of their users and also optimizing their product. Another big cloud platform is AWS which is widely used by enterprises to enhance their Artificial Intelligence Capabilities. Since Cloud is easily scalable and flexible it makes it easier to integrate artificial intelligence and machine learning making for an advanced and innovative enterprise.

As an enterprise integrates cloud services the cybersecurity and identity become a lot more complex and harder to manage. Using Cloud security frameworks like the zero-trust model can alleviate some of the stress of protecting sensitive data and can also ensure the compliance of the data. When looking at the zero trust models they operate differently from other models as it operates in a “never trust, always verify.” This model makes it a necessity to continuously authenticate and authorize every user and device that attempts to access any of the resources of the enterprise. This

prevents cyber security attacks and creates a much safer environment for the enterprise using the cloud. When it comes to digital identities Unified Access Management solutions have emerged. This provides secure access to multiple devices and applications and this is all done on cloud-based computing.

Case Studies and Discussion

Introduction

Cloud computing has become a cornerstone technology that enables organizations to scale, innovate, and provide rapid response to the demands of fluctuating markets. The shift from traditional on-premises systems to cloud-based infrastructure offers the promise of agility, economies of scale, and decision making that is driven by data.

The path leading towards digital transformation via cloud computing is riddled with both opportunities and risks that each organization must evaluate fully before undertaking the decision to embark upon migration. While there are several enterprises that have reported significant benefits from cloud adoption, several have encountered costly failures. (Rosenberg, 2011). In this section we will discuss the background cloud migration efforts and outcomes for three different organizations: Netflix, Target Canada, and Nanaimo Regional General Hospital.

Table 1: Cloud Computing in Practice - A Comparative Summary Chart

Organization	Netflix (Success)	Target Canada (missed opportunity)	Nanaimo Regional Hospital (Failure)
Industry	Entertainment/Streaming	Retail	Healthcare
Cloud Strategy	Full migration to AWS microservices, DevOps	Could have used cloud for scalable ERP, analytics, inventory and POS	Cloud-based Cerner EHR system (iHealth) via private infrastructure
Goal	Improve scalability, resilience, and global delivery	Rapid and flexible expansion into Canadian market	Streamline clinical data access, improve safety and workflows
Outcomes	Highly scalable, reliable, globally salable platform	System failures, data issues, and failed launch in 2 years	Clinician resistance, workflow disruptions, system suspension
Key Success/Failure Factors	Phased deployment, automation and monitoring, strong DevOps culture	Inventory inaccuracy, lack of scalability, poor data handling	Poor Change management, lack of clinician input, training gaps
Cloud Benefits Realized/Needed	Elastic compute, Global CDN, Real time analytics	Scalable infrastructure, real-time inventory, analytics	Centralized records (attempted), potential for better access

Lessons Learned	Invest in engineering, plan migration carefully, automate for resilience	Cloud enables agility and accuracy, test and scale gradually	Engage end users early, train thoroughly, pilot before rollout

Netflix: A Success Story

Background

Netflix is a global leader in streaming video content, serving over 260 million subscribers in more than 190 countries (Netflix, 2016; Wikipedia contributors, n.d.). Founded in 1997 by Marc Randolph and Reed Hastings, Netflix is an American company that began as DVD-by-mail movie rental service (Wikipedia contributors, n.d.). The company eventually built two data centres in close proximity to meet the demands of their growing subscribers for their video-on-demand service, an on- demand digital streaming service. While they were able to maintain a degree of success and growth prior to cloud migration, it was clear that the case for cloud was becoming stronger. Various realizations began to emerge. One such example was that new features were frequently available for end users on cloud first or exclusively on cloud basis. Integrations were also easier on the cloud platform, faster upgrade speeds, as well as a need to be on cutting edge of features releases, new and cloud- only features.

In 2008 Netflix experienced a major database corruption which resulted in the company being forced into shut down for three entire days. This was perhaps the major inciting event that led the company to a fork in the road: Whether to continue forward in the same momentum, putting more investments into building their data centers, or adopting the cloud. Netflix's decision was driven primarily by a need for increased innovation, reliability, speed, and increased availability for their subscribers (TechRepublic, 2018).

Figure 1 - Netflix & The Case for Cloud

Youtube. (n.d.). *How Netflix migrated to the cloud* [Video]. Youtube. https://youtube.com/watch? v=pR2j;ScmrYw

Netflix turned to Amazon Web Services (AWS) with the hopes of achieving their goals. AWS provided global infrastructure availability, high performance and reliability, elastic scalability, and infrastructure support which enabled Netflix to serve the demands of its customer base (Amazon Web Services, 2016). The migration was planned

as a gradual multi-year process involving a full re-architecture of the Netflix platform into a micro-services architecture to improve fault tolerance and scalability.

The migration was initiated in 2010 and was completed by early 2016, following a phased, service-by service approach (Netflix, 2016). Netflix's transition also included the adoption of a DevOps culture, site reliability engineering (SRE) and the extensive use of automation and observability tools (Netflix, 2016).

The migration was not without its own challenges and hurdles. Re-architecting legacy systems prove to be complex, time-intensive process. Cloud cost management, vendor lock-in, and ensuring data privacy in a multi-tenant environment were also ongoing concerns. (Tech Republic, 2018) The culture shift to a DevOps and cloud-first mindset demanded significant training, buy-in from leadership which enabled true organizational change and enterprise transformation.

Figure 2 - Netflix Usage Profile: Key Facts

86 Million Members	**190** Countries	**150** Million Hours of Streaming / Day	**10,000+** streams start every second at peak times
3 AWS Regions	**12 Availability Zones**	**100,000+** AWS instances	

Source: Amazon Web Services, Inc. (2016). Netflix case study. https://aws.amazon.com/solutions/case- studies/netflix-case-study

Table 2 - Netflix's Use of IaaS, PaasS, and SaaS During AWS Cloud Migration

Cloud Model	Did Netflix Use it	Description
IaaS (Primary)	Yes	Core Infrastructure from AWS (EC2, S3, VPC, etc)
PaaS	Yes	Built internal platforms on top of AWS infrastructure
SaaS	No	Netflix built its own software stacks preferring full control over user experience. (Did not rely on SaaS Products like Amazon WorkSpaces, Chime, or QuickSight)

Source: (AWS, 2016)

Table 3 - Netflix's Cloud Deployment Model

Cloud Type	Used by Netflix	Explanation
Public Cloud	Yes	All infrastructure runs on AWS which is shared with other organizations but isolated
Private Cloud	No	Netflix does not maintain its own data centres for video delivery or computer
Hybrid Cloud	No	Netflix completed its full migration to AWS in 2016 and does not rely on on-premises systems.

Source: (AWS, 2015)

Success Factors

Several factors contributed to Netflix's successful cloud migration.

Full Commitment to Cloud Migration: As an enterprise, a decision was made to abandon on-premises data centers allowing the adaptation into a public cloud, avoiding the complexities of a hybrid cloud model. (Amazon Web Services, 2016).

Microservices Architecture: Netflix decomposed its monolithic application into hundreds of microservices. Each microservice handled a specific business capability (e.g., recommendations, billing, playback) The use of microservice architecture allowed fault-isolated and scalable delivery of services, enabling Netflix to deploy updates frequently without systemic disruptions. (Netflix, 2016).

Cloud Efficiency: In addition to architectural changes, network continuously invested in optimizing cloud efficiency to reduce costs and improve performance. Dynamic workload scheduling, and intelligent autoscaling policies have allowed Netflix to optimize computing resources in real-time without compromising service quality. (Han and Phadnis, 2024).

DevOps Culture and Automation: Netflix embraced continuous integration and deployment, coupled with automated testing which minimized error and accelerated feature releases. (Netflix, 2016; TechRepublic 2018).

Resilience Engineering with Chaos testing: Development of tools like Chaos Monkey and later the Simian

army, which intentionally inject faults to test the robustness of the system ensures high latency and fast recovery from failures. This forced services to be resilient to instance failures, latency spikes, and regional outages.

Leadership and Innovation Culture: Strong executive backing created an environment encouraging experimentation, innovation, and team ownership of services which acted as a driver towards continuous improvement. (Bacancy Technology, n.d.).

Global Scalable Infrastructure: Netflix implemented Open Connect, its own custom Content Delivery Network (CDN) (Manikin et al., 2018; Bacancy Technology, n.d.) While the control plan ran in AWS, larger video assets were delivered from edge locations improving latency and reducing AWS egress costs. Utilizing AWS's global data centres, Netflix was able to deliver low-latency streaming across the globe dynamically scaled to meet the demand spikes during new content launches. Netflix also adopted Apache Cassandra for high availability across regions and utilized Apache Kafka and Amazon Kinesis for real-time data streaming. Big data analytics were processed using Amazon S3, Presto, Apache Spark, and Hive on EMR (Netflix, 2016).

Multi-Region Active-Active Deployments: Critical services were deployed across multiple AWS regions in active-active mode. This enabled seamless failover and geographic redundancy (Bacancy Technology, n.d.).

Table 4 - AWS Services Used by Netflix

Amazon Elastic Compute Cloud (EC2)	*X*	Achieves desired scalability ensuring smooth screaming experience. Custom created EC2 instances power computational engines behind content delivery, and other compute-intensive tasks.
Amazon Kinesis Data Streams (Amazon KDS)	*X*	Accumulates terrabytes of data from many sources. Data is instantly made available for real-time analytics and stored in Amazon S3 buckets for additional use. Assists Netflix in adapting content recommendations, improving streaming quality and enhancing user satisfaction
AWS Lambda	*X*	Streamlined processes (ie - data manipulation, backup decisions and security checks). Automates security measures, enforces compliance during instance setup and response to unauthorized access

Amazon Machine Learning (AML)	*X*	Helps to personalize viewer experience with recommendation engine. Analysis of user behaviour, patterns, and context preferences to customize library to suit individual tastes
Amazon Redshift	*X*	Aids in rapid analysis of vast amounts of data, content refinement and recommendation, as well as streaming optimization. Can perform complex queries and get insights.
Amazon Route 53	*X*	Offers seamless viewing experience to worldwide customers by efficiently routing traffic to alternative regions in case of server failure, region overloads, or other disruptions.

Source: (AWS, 2016), Bacancy (n.d.), and Netflix (2016)

Conclusion

Netflix's cloud migration is a classic example of a well-planned and executed digital transformation. Netflix built a platform that is not only highly scalable and reliable, but also nimble enough to support innovation (Amazon Web Services, 2016). The success of this enterprise transformation emphasizes the importance of architectural alignment with cloud paradigms and a strong organizational culture which is cemented in the value of continuous improvement.

Target Canada: A Missed Opportunity

Founded in 1902, Target Corporation is a major American retail chain that is known for offering a variety of home goods through its physical stores and online platform. In 2013, Target expanded into Canada by acquiring leases from Zellers (also a retail company now out of business), opening over 130 stores. To support its operations, they adopted a hybrid cloud approach integrating on-premises SAP retail ERP system with various cloud-based inventory and supply chin tools with the goal to modernize operations and emblem real-time inventory tracking across its network. Target Canada struggled with operational and supply chain issues, resulting in the company shutting down in 2015, only 3 years after its entrance to the Canadian marketplace. (Wikipedia contributors, 2025; Dahlhoff, 2015)

The project failed for a multitude of reasons, but primarily as a result of being rushed and poorly managed. Whereas the average ERP deployment takes several years in the retail sector, SAP was rolled out in less than two years. Target Canada also elected to go live with a full-scale implementation, as opposed to a more pragmatic pilot or phased approach (Blue Link ERP, 2022). Third party cloud based supply chain and inventory tools were used for demand forecasting and vendor coordination, coupled with middleware that was used to connect SAP with cloud applications.

Unlike companies that leveraged cloud platforms to enable real-time data analytics and system integration, Target Canada operated on centralized, on-premises infrastructure. The ability to make dynamic updates, synchronize, or scale its systems made it nearly impossible to correct course quickly.

A Case for Cloud Strategy

A hybrid cloud strategy, which blended the flexibility of public cloud services that also allowed control of private infrastructure could have helped Target Canada in managing their inventory systems in real time. There were several cloud based data management tools that could have helped Target Canada cleanse and validate data before it entered the ERP system thereby reducing cascading errors. Scaling systems gradually and the ability to roll out features as well as patch problems without full system shutdowns would also have been performed with more ease had Target Canada adapted a hybrid cloud as part of their digital transformation prior to entering the Canadian market. Cloud platforms allow for localized services and rapid deployment of features that are tailored to regional markets - which may have been very helpful in a new market like Canada.

Whereas companies like Netflix adapted cloud computing early on to improve a service delivery and scalability, Target Canada had a relatively rigid infrastructure that led it to be unable to adapt to real-world business conditions a contrast that underscores the strategic value of cloud computing in modern enterprise transformation. Target Canada's failure highlights various errors in not only project management but a missed opportunity to leverage cloud computing as a strategic enabler. Rather than being a case of failed cloud adoption, it represents a failure due to the absence of cloud adoption. In doing this, the critical role hybrid cloud solutions can play in supporting dynamic, data-driven and scalable enterprise operations comes to the forefront.

Table 5 - Analysis of Target Canada's IT Failures & Potential Cloud Based Solutions

Business Outcome	Billions of dollars in loss, 133 stores closed in 2 years	Risk reduction, improved agility, and supported gradual market entry
Data Accuracy & Integration	Manual data entry, poor quality vendor and inventory data	Cloud-based data validation, cleansing, and integration using real-time API
Deployment Speed & Flexibility	Rushed rollout, proper testing not performed	Agile development with CI/CD pipelines in hybrid cloud environments
Disaster Recovery & Resilience	Limited recovery capabilities, no cloud redundancy	Cloud backup and failover systems ensuring continuity and faster issue resolution

ERP Implementation	On-premises SAP system	Cloud-hosted ERP (SAP/4HANA) with modular deployment
Inventory Management	No real-time tracking, highly prevalent stock issues	Real time inventory monitoring via cloud analytics tools
System Scalability	Rigid infrastructure, hard to scale or patch quickly	Scalable cloud infrastructure enabling fast expansion and updates

It is of interest to note that prior to the Target's departure from Canada, the company initiated a large-scale digital transformation effort which was focused on migrating its complex legacy IT systems which included inventory management, e-commerce, and customer databases to a cloud infrastructure. Motivated by the desire to enhance scalability, agility, and customer experience, Target hoped to gain a stronger market share in the digital marketplace by integrating their ERP system into a cloud based infrastructure. (IERP, 2023).

Nanaimo Regional General Hospital

Background

Nanaimo Regional Hospital (NRGH)is part of Island Health in British Columbia, was among one of the first Canadian hospitals to implement a fully digital cloud-based health information system called iHealth. The iHealth project was launched by Island Health with the goal of creating an integrated electronic health record system that would centralize patient information and enable clinicians to access real-time data from any location. It was built on Cerner's Millennium platform and was hosted via private cloud infrastructure and aligned with the Canadian Health Infoway's national eHealth strategy. (Canada Health Infoway, 2014).

Despite very ambitious goals, the deployment at NRGH encountered major challenges. Clinicians reported that the system was counterintuitive, slow, and often prone to errors affecting patient safety and disrupting clinical workflow.

According to a report written by the BC Auditor General in 2017, the iHealth project lacked adequate stakeholder consultation and failed to involve frontline clinicians in early-stage design and testing. Both nurses and physicians often found themselves learning the new system on the job with minimal training leading to a great deal of frustration and resistance to embrace the new system. The frustration grew so much that physicians circulated petitions demanding the redaction of the system altogether. Failure can be attributed to several factors.

Poor Change Management: Transitioning to cloud based Electronic Health Records requires careful change

management. NRGH rushed its deployment without a thorough preparation for end-users. End users were also not involved in piloting the technology in phases.

Insufficient Training: Clinicians received inadequate training on how to use the new system. Many users reported having to figure out essential functions under pressure, resulting in errors made.

User Interface and Usability Problems: The system's interface was not intuitive. Tasks that clinicians described as once being simple now became time consuming and error prone.

Lack of Clinical Buy-In: Many front line workers felt excluded from the planning process. This lack of early engagement fostered skepticism and resistance.

Over Reliance on Technology: The system was expected to replace manual process without enough validation of its reliability in high stakes clinical settings.

The Nanaimo iHealth case underscores several critical lessons which can apply towards other enterprises endeavouring to undergo digital transformation. Perhaps one of the most critical is to engage end-users early. In this case, clinician involvement from the planning stages can increase adoption and bring to surface any usability issues while they are smaller and more manageable Testing systems in smaller and controlled environments allows for iterative improvements. It is also important to understand that there has to be continuous education and support available to ensure end users can adapt to the new workflows. Ensuring that rollouts are phased also minimizes disruption and allows for feedback loops. Finally, once implementation is completed, it is essential that regular audits are done in order to have a true reflection of progress and what corrective steps need to be taken to correct course.

Conclusion

NGRH's iHealth implementation highlights the complexities of cloud based digital transformation in healthcare. Though their goals were progressive, the project failed to align technology with clinical realities emphasizing that culture, inclusion, and sensitivity to everyday practice circumstances have to be weighed in very carefully when undergoing a large-scale transformation in a healthcare setting.

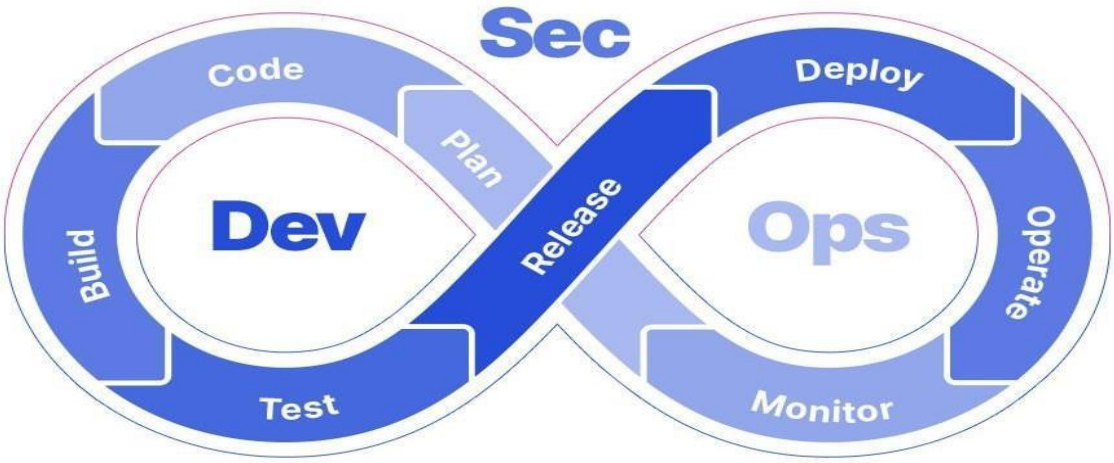
Challenges s Risks

Transitioning to the cloud is more than just a shift in infrastructure; it's about reimagining how technology, people, and processes work together in a shared environment. Our analysis reveals three interconnected challenge areas: technical vulnerabilities, organizational transformation, and regulatory compliance. Effectively addressing these challenges is crucial for maintaining security, ensuring smooth operations, and meeting legal requirements

The world of cloud computing is constantly evolving, bringing with it a mix of exciting opportunities and potential pitfalls. For example, the power to spin up hundreds of virtual machines, containers, and storage volumes with just one command. While this speeds up development processes, it also raises the risk of misconfigurations slipping through the cracks. Imagine a storage container that's set up incorrectly, leaving sensitive customer data exposed on the public internet for days. Or consider outdated virtual machine images that could harbor vulnerabilities just waiting for an attacker to exploit. To stay ahead of these risks, many organizations are embracing infrastructure-as-code frameworks such as Terraform and AWS CloudFormation. This method automates the creation, modification, and monitoring of cloud resources, treating security settings, network configurations, and policy rules like code that can be version-controlled and tested automatically. Plus, cloud providers offer encryption services to safeguard data both at rest and in transit. Continuous security monitoring tools are also in play, scanning for unusual activities—like strange login attempts or unexpected data transfers—to send out alerts before any issues escalate.

When it comes to moving to the cloud, it’s not just about the technical side of things; it really requires a big change in how an organization thinks and operates. Traditional IT teams, who are used to handling physical servers and storage systems, need to embrace new concepts like container orchestration, serverless functions, and microservices. The speed of change is remarkable: small updates can be rolled out several times a day, and systems are expected to automatically fix themselves and scale as needed. This new landscape demands that development, security, and operations teams work closely together—a practice known as DevSecOps—to weave risk management into the fabric of continuous integration and delivery (Skyhigh Security, 2023).

Organizations that have a hard time defining clear roles, responsibilities, and communication paths often end up with disjointed tools and isolated workflows, which can lead to more mistakes and slower deployments. On the flip side, companies that focus on building cross-functional governance teams, offering thorough training, and establishing a solid cloud operating model tend to see quicker adoption and fewer issues after migration.



Source: (Comtrade, 2024)

The third big challenge we face is navigating the maze of regulatory compliance and data privacy. Just because you're using cloud environments doesn't mean you're off the hook when it comes to laws like the General Data Protection Regulation in Europe, the Health Insurance Portability and Accountability Act in the U.S., or specific industry standards like PCI DSS for payment data (PCI Security Standards Council, 2025). In fact, these regulations can get even trickier in the cloud, since data can zip across different geographic and administrative lines in no time. There are data residency rules that might require certain records to stay put in a specific country, and audit standards often demand meticulous logging of every access, configuration change, and administrative action. To tackle these requirements, companies are embedding compliance checks right into their deployment processes, making sure that policy controls like encryption, log collection, and access reviews kick in automatically whenever new resources are set up. Plus, with provider-native compliance dashboards and automated evidence-gathering tools, preparing for audits becomes a lot smoother, cutting down on manual work and minimizing the chances of human error.

To tackle the wide range of potential risks, our team suggests using a structured risk prioritization framework. In this approach, we evaluate each identified risk along two key dimensions: how likely it is to happen and the potential impact it could have on our business operations. Risks that are both high in likelihood and high in impact—like misconfigured identity and access management policies— require immediate attention. We recommend using automation to enforce secure defaults and quickly spot any deviations. For risks that are either less likely or have a lower impact, we can manage

them through regular policy reviews, oversight from governance committees, and focused process improvements. This heatmap-driven strategy allows us to direct our limited security and compliance resources to the areas that need them most, striking a balance between the speed of innovation and careful risk management (HIPAA Journal, n.d.).

Tackling the challenges of cloud migration successfully calls for a well-thought-out, layered approach. By embedding policies into the infrastructure definitions, we can ensure that security and compliance standards are met before any workloads are launched. With continuous monitoring and automated reporting, we gain real-time insights into the health and configuration of our cloud environments, allowing us to quickly address any issues that arise. Cross-functional governance teams play a crucial role in overseeing the overall strategy and policies, while ongoing training and knowledge sharing help development and operations teams embrace best practices. When combined, these strategies foster a resilient and adaptable cloud environment where innovation and security can thrive together.

Ethical Concern and Mitigation Strategies

Ethical responsibilities are talked about in our Cloud Computing textbook (Bhowmik, 2017, p 48). Cloud computing brings a number of ethical responsibilities to the table, mainly because it shifts control of data and systems from internal company networks to third-party providers. When an organization moves its operations into the cloud, it gives up direct oversight, which can create uncertainty about who is truly accountable when issues occur.

Because cloud systems often involve multiple parties and complex structures, it's not always obvious who is responsible if something goes wrong. That's why both cloud providers and their clients need a clear understanding of their roles. Often, resolving ethical or technical problems requires both sides to cooperate and communicate effectively.

There's always a bigger ethical burden on cloud providers themselves. Since users are trusting these companies with valuable information, including sensitive data and intellectual property, providers have a moral responsibility to protect that data. While cloud services make it easier to share and access digital content, they also open the door to misuse. It's important that reliable cloud providers have strong security measures to protect information.

According to an article written on *Medium,* cloud computing has completely transformed how individuals and companies store, manage, and access data (Popat, 2025). It provides affordable access to resources, the ability to scale operations quickly, and new opportunities for innovation. However, it still comes with ethical concerns that need attention to make sure it's used in a way that is fair, transparents, and socially responsible. Some of the most pressing issues include data privacy, security, environmental sustainability, and legal complications.

Storing data in the cloud often means handing it over to third-party providers. While this makes things more convenient, it also creates confusion around who actually owns the data and what

happens to it. Unclear ownership is when users rely on cloud services, they may unintentionally give up some control. In some cases, providers may claim rights over the data, which can blur legal and ethical lines. Along with that, there is the risk of surveillance. Government agencies or corporations may access stored data without user consent, raising major privacy concerns.
Lastly, there is the need for transparency. Ethical cloud practices require clear policies that explain how data is collected, stored, and shared. Users should always know what is being done with their information.

Even though cloud platforms use strong security measures, they're not immune to cyber attacks. In the article by Popat (2025), high-profile breaches have shown how important it is for providers to take responsibility for keeping user data safe. There can be accountability issues when a breach happens. It's often unclear who is at fault, the provider or the customer, which can leave users vulnerable and without support. There needs to be standardized protections in place where providers should use the latest security tools, like encryption, to protect data regardless of the financial cost. A lot of breaches happen because of user mistakes, like weak passwords. Providers should educate users on safe practices to minimize these risks.

An article from *Holistic AI* talks about the bias and discrimination in AI services which is a big ethical concern (Holistic AI Team, 2024). As AI becomes more integrated into critical areas like hiring, healthcare, finance, and law enforcement, concerns about bias in AI systems are growing rapidly. While AI can improve decision-making speed and efficiency, it can also produce unfair outcomes, especially when trained on biased or incomplete data. These outcomes are often harder to detect than human bias but can affect large numbers of people very quickly.

According to Holistic AI Team (2024), AI bias happens when algorithms make decisions that favor or disadvantage certain groups due to flawed training data, unfair objectives, or unbalanced algorithms. For Example, a hiring algorithm trained on male-domincated data might unintentionally screen out female candidates. Similarly, biased crime statistics used in law enforcement AI tools could lead to discriminatory profiling of certain communities.

The impact of AI bias isn't just ethical, it's a business risk. According to Holistic AI Team (2024), companies using biased AI systems may face legal challenges, damage to their reputations, and the loss of public trust. In healthcare, this could mean unequal access to treatment. In finance, it might lead to unfair credit scoring or loan denials. In human resources, it can result in a lack of diversity and missed talen opportunities.

Addressing AI bias requires both awareness and action. Organizations should ensure their AI systems are trained on diverse, representative data and regularly audited for fairness.
Establishing AI frameworks that promote transparency, human oversight, and ethical accountability is key. When businesses take these steps, they reduce risk, improve performance, and show a commitment to fairness.

As artificial intelligence becomes more deeply integrated into cloud-based platforms, new security and ethical challenges are emerging. According to an article from *Cloud Security Alliance*, while the combination of AI and cloud computing opens doors to innovation and efficiency, it also introduces risks that must be managed carefully (Thales, 2024). To address these concerns, organizations need to have strategies that focus on transparency, data protection, and ethical AI practices.

One of the first steps of ethical cloud computing is clear communication. Companies must ensure that their privacy policies in terms of service are easy and accessible. These documents should outline how your data is collected, used, and stored, helping users make informed decisions about whether and how to engage with the service.Transparency is not only an ethical responsibility, but also a key factor in building a long-term trust with customers and meeting legal expectations.

According to Thales (2024), cloud-based AI systems are increasingly targeted by attacks like model theft and data poisoning. To defend against model theft, organizations should encrypt

their models and enforce strict access controls. This includes setting clear user rules and applying multi-factor authentication.

Legal compliance is a critical part of responsible cloud computing. As governments create new AI and data protection laws, businesses must ensure they meet regulatory requirements. This includes following privacy laws, implementing fair data practices, and ensuring that AI systems align with legal definition of accountability, transparency, and non-discrimination.By designing systems that meet the standard business is not only reduce legal risk, but also build a stronger, more ethical platform.

As cloud computing continues to shape the way we live and work, ethical accountability must be part of its foundation. From data privacy in AI, fairness to transparency and regulatory compliance, the ethical concerns surrounding cloud technologies are too important to ignore.

Addressing these challenges isn't the responsibility of anyone group, it requires collaboration. Cloud service providers, users, policy makers, and regulatory all play a role in building a responsible digital future. By working together to implement clear guidelines, secure measures, and ongoing oversight, we can ensure that cloud computing remains a tool for progress, not harm.

Future Trends and Recommendations

Future Trends

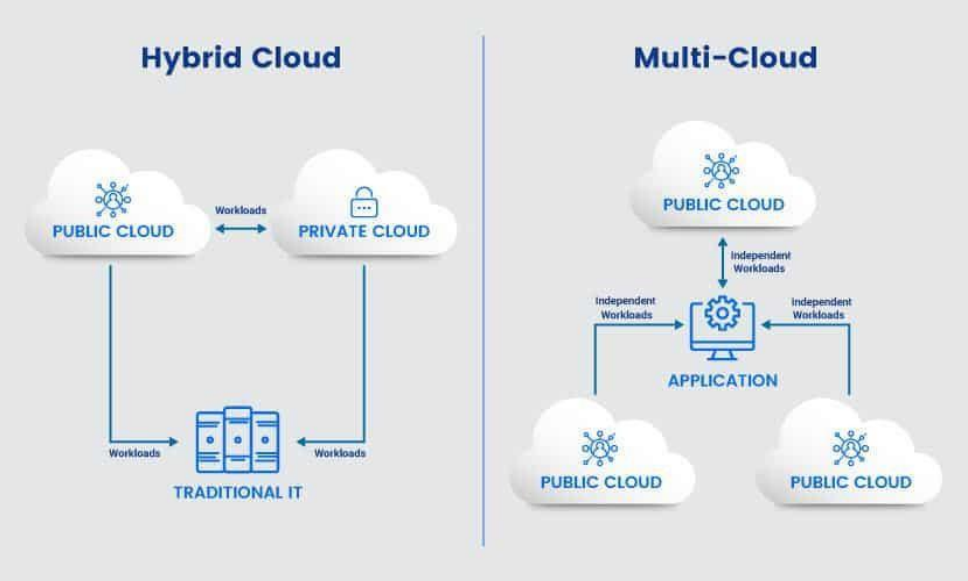
When looking at the future trends in cloud computing the automation of cloud operation is one of the most intriguing features and use of Artificial Intelligence. When thinking about operations Artificial Intelligence can allow these enterprises to automate tasks which will lead to a reduced burden of enterprises to manually handle these tasks and can help them operate more efficiently. When looking at some of the tasks that can be automated include resource allocation, security, and monitoring the performance of the system. Although

automation is good for the enterprise it can have negative effects if relied on too heavily like Skill degradation, lack of contextual understanding, overdependence, and automation bias and complacency. These are all things that could negatively affect the enterprise if they choose to solely focus on automation. Artificial Intelligence can also be used to do predictive analysis which is where the enterprise can collect data and analyze it to predict the future. Predictive analytics can predict things such as system failures, faulty security , or even capacity issues which are all things that can be caught by the system before it happens.

One of the developments that is looking to be the future of cloud is the rise of self- healing cloud systems. These types of cloud systems can use Artificial Intelligence to detect anomalies, monitor infrastructure, and also trigger corrective actions all without having a human intervene in the process. An example of this in action would be an application experiencing node failures. The self healing cloud would then respond by rerouting traffic or using other resources to keep the server running smoothly. If implemented in the future it would allow enterprises to not only enhance the reliability of their systems but it would also allow the enterprise to reduce operational costs as the AI has the capability to deliver the work on its own. When looking into the use of AI-enhanced cloud infrastructure it is something enterprises will look into to create an efficient environment and a cost-effective one as well.

Another future trend in the cloud computing world is that of edge computing as it is part of the centralized cloud models. Looking into what edge computing is, it is the processing of data closer to where it was generated which would then reduce the latency and enable the real time decision making of the cloud. Edge computing is mainly found in areas that would need to process data quickly which can include industries like healthcare. Looking specifically into the use of edge computing in the health care industry, these edge computing technology can help analyze patient data and try to detect health risks in the patients which can be done locally instead of having to go through the process of sending data to a data center then getting a response later than a local edge computing device would give the hospital or clinic.

Recommendations



Another leading trend that is recommended in the cloud computing space is the adoption of multi-cloud and hybrid-cloud strategies within the enterprises. When looking at the figure above the hybrid cloud is a combination of public and private clouds and gets the best features of both clouds. These features include being able to scale with ease, have control over private and sensitive data, and even have the cost efficiency of normal cloud. Now the other figure on the right side of the graphic is what we call Multi cloud platform. This service uses multiple clouds providers like AWS, Google Cloud Platform, and Microsoft Azure. These are used because the enterprise can avoid situations like vendor lock-in where they are stuck to one vendor, and it also optimizes the performance of the enterprise. Another advantage to using multi-cloud is that it enables workload portability, which allows the enterprise to replicate applications and move easily as needed by the enterprise. “a multi-cloud system helps organizations choose what tools will be the most useful to them and not have to be tied to one provider and instead get the best tools possible making for a strong cloud system” (Google Cloud). This makes it one of the best possible routes an enterprise can go through to improve the

When looking forward in the cloud computing space it is important that enterprises implement the newest strategies to stay ahead of evolving technology. One of the recommendations that should be made to these enterprises would be to make a well-defined cloud strategy. This would help the enterprise align their business objectives with their cloud adoption initiatives. The enterprises would need this as they would be able to deal with the application workloads best suited for transformation, maintaining budgets. And ensuring that the enterprise is complying with governance frameworks. By addressing these frameworks, it would help ensure that the enterprise is successful.

Future Research

Quantum computing is a new form of technology that is still in its early stages of development, but it has the potential to completely change the cloud computing world. Unlike traditional computers, quantum machines can handle very large amounts of data all at once, this makes it very effective in improving areas like optimization and machine learning. As this new form of technology is developing and the algorithms are advancing the researchers are trying to find a way to incorporate and change the landscape of cloud computing. There are companies that are already experimenting with quantum computing and these companies include Google and IBM. Future research will be needed to really gauge how quantum computing will affect performance, data security, and software development.

Conclusion

The goal from this paper has been to examine different aspects of cloud computing by way of industry analysis, case study, and literature review in order to better understand key considerations and drivers, benefits, as well as challenges and risks that are often associated with cloud adoption.

Cloud computing is integral with today's digital transformation. It allows businesses to scale and grow their operations by becoming adaptive to the market. Service models like IaaS, PaaS, and SaaS, provide companies to choose what works for them. As businesses transition to cloud

computing, it's clear that there are drivers influencing this transformation. This digital transformation is about more than technology, it's about an organization's leaders, culture, people, and processes.

The challenges companies face to adopt cloud computing can come from undefined roles, lack of communication, and un-adaptive processes. Successful transformation to the cloud can come from businesses who foster a culture of collaboration, are capable of data-driven decisions, and have a digital strategy that is aligned to business objectives. Cloud computing is exciting, however it is not the only digital transformation taking place.

Emerging technologies such as AI are rapidly enhancing cloud computing. Some ways AI is being used in cloud computing is automating mundane cloud operations, self-healing systems, and detecting components that need to be fixed. Some other technological trends during this digital age are multi-cloud strategies, edge computing, and quantum computing.

The implications for businesses who fail to adapt to the current digital transformation is a missed opportunity of growth and financial success. As such, digital maturity models are a framework that can help companies highlight gaps in their technology, operationally, strategically, and in their internal culture. These frameworks can effectively guide a business to digitally adapt and be ready for long-term growth. As the digital environment continues to evolve, businesses who are intentional and agile will be better positioned to thrive in this digital transformation era.

References

A Complete Guide to Digital Maturity Models: Assess and Elevate Your Transformation. (2024, September). *Upcore*. May 2025, https://www.upcoretech.com/insights/digital-maturity-models/#:~:text=1,It%20provides%20a%20comprehensive%20assessment

Amazon Web Services. (2016). *Netflix case study*. https://aws.amazon.com/solutions/casestudies/innovators/netflix/

Auditor General of British Columbia. (2017). *An independent review of the Island Health iHealth project.* https://ihealth.islandhealth.ca/wp-content/uploads/2022/02/ihealth-review-2017-Cochrane-Report.pdf

Aztech IT Solutions. (2023, September 27). *Public, Private or Hybrid Cloud: Exploring the Major Differences*. https://www.aztechit.co.uk/blog/private-public-hybrid-cloud-difference

Bacancy Technology. (n.d.). *Netflix AWS migration*. https://www.bacancytechnology.com/blog/netflix-aws-migration

BasuMallick, Chiradeep. 2022. "What Is Cloud Computing? Definition, Benefits, Types, and Trends." Spiceworks. February 9, 2022. https://www.spiceworks.com/tech/cloud/articles/what-is-cloud- computing/.

Bhowmik, S. (2017). *Cloud Computing*. Cambridge University Press.

Blue Link ERP. (2022, March 10). *Target Canada: Mistakes made from a software perspective. https://www.bluelinkerp.com/blog/target-canada-mistakes-made-from-a-software- perspective/*

Canada Health Infoway. (2014) Better health together: A digital health plan for Canada. https://www.infoway-inforoute.ca/en/component/edocman/2771-*annual-report-2014-2015/view-document?Itemid=103*

Catlin, T., Segev, I., & Singer, M. (2015, January). McKinsey Digital Building up your digital quotient.https://www.mckinsey.com/ch/~/media/ClientLink/Building%20up%20your%20digital%20quotient%20How%20to%20harness%20digital%20to%20accelerate%20business%20performance/McKinsey%20-%20Digital%20Quotient%20final.ashx

Chui, M., Issler, M., Roberts, R., & Yee, L. (2023, July 20). *McKinsey Technology Trends Outlook 2023 | McKinsey*. Www.mckinsey.com. https://www.mckinsey.com/capabilities/mckinsey-digital/our- insights/the-top-trends-in-tech#new-and-notable

Cloudflare. (n.d.). *Why use serverless computing? Pros and cons of serverless* https://www.cloudflare.com/learning/serverless/why-use-serverless/

Cloudflare. (n.d.). *What is edge computing?* https://www.cloudflare.com/learning/serverless/glossary/what-is-edge-computing/

Dahlhoff, D. (2015). *Why Target's Canadian expansion failed.* Harvard Business Review. https://hbr.org/2015/01/why-targets-canadian-expansion-failed

Digital Maturity Model. Achieving digital maturity to drive growth. (2018, February).

https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/deloitte-digital-maturity-model.pdf

Digital Transformation Model in Collaboration With TM Forum. (2017, May). May 2025, https://www.prnewswire.com/news-releases/deloitte-leads-development-of-new-digital-transformation-model-in-collaboration-with-tm-forum-300457674.html

Erickson, J. (2024, June 21). *The Role and Benefits of AI in Cloud Computing*. Oracle. https://www.oracle.com/artificial-intelligence/ai-cloud-computing/

Google. (n.d.). *Advantages Of Cloud Computing*. Google Cloud. https://cloud.google.com/learn/advantages-of-cloud-computing

Han, J., & Phadnis, P. (2024, December 17). Cloud Efficiency at Netflix. Netflix Technology Blog. https://netflixtechblog.com/cloud-efficiency-at-netflix-f2a142955f83

HIPAA Journal. (n.d.). *HIPAA compliance in the cloud.* https://www.hipaajournal.com/

Holistic AI Team. (2024). *What is AI Bias? - Understanding Its Impact, Risks, and Mitigation Strategies*. Holistic AI. https://www.holisticai.com/blog/what-is-ai-bias-risks-mitigation-strategies

IERP. (2023, January 15). *Target in Canada: An example of an ERP failure.* Medium. https:// medium.com/1erp

Island Health. (2024). About us. https://www.islandhealth.ca/about-us

Khurana, D. (2024). *Optimizing artificial intelligence and machine learning with cloud computing*. Orange Business; Orange Business Services. https://www.orange-business.com/en/blogs/optimizing-artificial-intelligence-machine-learning-cloud-computing

Limited, I. (n.d.). The Necessity for Agile Framework for your Digital Transformation | Infosys BPM.https://www.infosysbpm.com/blogs/business-transformation/the-necessity-for-agile-framework- for-your-digital-transformation.html

Lumenova. (2024). *Overreliance on AI: Addressing Automation Bias Today | Lumenova AI*. Lumenova AI; Overreliance on AI: Addressing Automation Bias Today | Lumenova AI. https://www.lumenova.ai/blog/overreliance-on-ai-adressing-automation-bias-today/

Manikin, I, Prabju, A., & Rao, A. (2018). *Scaling Netflix CDN architecture for global streaming.* Netflix Technology Blog. https://netflixtechblog.com/cloud-efficiency-at-netflix-f2a142955f83

Matellio. (2024, August 14). *Cloud Computing and Digital Transformation: Future-Proofing Your Business - Matellio Inc*. Matellio Inc. https://www.matellio.com/blog/cloud-computing-and-digital- transformation/

Multi-cloud vs. hybrid cloud: What's the difference? (2024). Cloudflare.com. https://www.cloudflare.com/learning/cloud/multicloud-vs-hybrid-cloud/

Netflix. (2016, February 11). *Completing the Netflix cloud migration.* Netflix Newsroom. https://about.netflix.com/en/news/completing-the-netflix-cloud-migration

O'Brien, K., Downie, A., & Scapicchio, M. (2025, April 16). Digital transformation. IBM Think. https://www.ibm.com/think/topics/digital-transformation

Online, S. B. U. 2022. "Understanding Cloud Security Benefits and Challenges." Online.sbu.edu. November 28, 2022. https://online.sbu.edu/news/cloud-security-benefits-and-challenges.

PCI Security Standards Council. (2025, May 22). *Protect payment data with industry-driven security standards, training, and programs.* https://www.pcisecuritystandards.org/

Popat, M. (2025). *The Ethical Implications of Cloud Computing.* Medium. https://mihirpopat.medium.com/the-ethical-implications-of-cloud-computing-2ece38591b5d

Quantum Cloud Computing: A Review, Open Problems, and Future Directions. (n.d.). Arxiv.org. https://arxiv.org/html/2404.11420v1

Rosenberg, J. B., & Mateos, A. (2011). *The cloud at your service: The when, how, and why of enterprise cloud computing*. Manning Publications.

Skyhigh Security. (2023, October 16). *Cloud adoption risk report*. https://www.skyhighsecurity.com/lp/the-data-dilemma-cloud-adoption-and-risk-report.html

Sire, Tom. 2024. "Transitioning to the Cloud: Why Are Companies Moving to the Cloud?" Cloud Computing News. September 23, 2024. https://www.cloudcomputing-news.net/news/transitioning-to- the-cloud-why-are-companies-moving-to-the-cloud/.

SuperOffice. (2025, April 30). How Digital Transformation is Driving The Customer Experience.https://www.superoffice.com/blog/digital-transformation/#:~:text=Today%2C%20customers%C2%A0expect%20relevant%20content%20in,their%20journey%20that%20dictates%C2%A0your%20strategy

Tangwaragorn, P., Charoenruk, N., Viriyasitavat, W., Tangmanee, C., Kanawattanachai, P., Hoonsopon, D., Pungpapong, V., Pattanapanyasat, R.-P., Boonpatcharanon, S., & Rhuwadhana, P. (2024). Analyzing key drivers of digital transformation: A review and framework. *Journal of Industrial Information Integration, 42*, 100680. https://doi.org/10.1016/j.jii.2024.100680

Tanner Bill*, Migrating to the cloud: The key to business scalability, flexibility and cost-effectiveness - Intelligent CIO North America*. (2024). Intelligent CIO North America. https://www.intelligentcio.com/north-america/2024/07/22/migrating-to-the-cloud-the-key-to-business- scalability-flexibility-and-cost-effectiveness/

TechRepublic. (2018, January 4). 5 lessons IT learned from the Netflix cloud journey. https:// www.techrepublic.com/article/5-lessons-it-learned-from-the-netflix-cloud-journey/

Thales. (2024, October 2). *How do AI and Cloud Computing Affect Security Risks?* Cloud Security Alliance. https://cloudsecurityalliance.org/blog/2024/10/02/ai-regulations-cloud-security-and-threat-mitigation-navigating-the-future-of-digital-risk

The role of artificial intelligence in digital transformation. (2024, September 25). Business Insights Blog. https://online.hbs.edu/blog/post/ai-digital-transformation

The role of artificial intelligence in digital transformation. (2024b, November 8). PTC. https://www.ptc.com/en/blogs/corporate/artificial-intelligence-digital-transformation

What Is Edge Computing? | Microsoft Azure. (2025). Microsoft.com. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-edge-computing/?msockid=157de31ff9a66c2f3c8ef109f80e6d93

Wikipedia contributors. (n.d.). Netflix. Wikipedia. Wikimedia Foundation. https:// en.wikipedia.org/wiki/Netflix

Wikipedia contributors. (2025, May 15). *Target Canada.* Wikipedia. https://en.wikipedia.org/ wiki/Target_Canada

Youtube. (n.d.). *How Netflix migrated to the cloud [Video].* Youtube. https://youtube.com/ watch?v=pR2jlScmrYw

Zervas, S. (2023, August). *Target's retail failed entry into Canada: Case study.* ResearchGate. https://www.researchgate.net/publication/ 373650015_Target's_Retail_failed_entry_into_Canada_Case_Study