

Sustainable Development for Digital Transformation, Part 1

Applying Environmental Theory to the Digital Ecosystem

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website (www.isaca.org/journal), find the article and click on the Comments link to share your thoughts.

<https://bit.ly/2ynbGoi>

Digital business models expand the types and numbers of an organization's identities. Using new technologies to increase enterprise revenue and streamline business operations creates an interconnected digital ecosystem that increasingly leads to data leakage and digital pollution. For example, as organizations transition to the cloud, their digital ecosystems become polluted with excess access that leads to privilege misuse and data breaches. Cybersecurity professionals refer to the cloud as an ecosystem that can suffer from data leakage, evoking a parallel to the physical environment and contaminant leakages. As organizations increasingly migrate their business-critical operations to the cloud, incorporating environmental sustainability principles may be a way to establish policies and programs that protect data within the constantly evolving cloud infrastructure. To create a sustainable digital ecosystem, organizations should align their identity governance and administration (IGA) programs with tenets of the physical environmental sustainability movement such as sustainability theory and sustainability governance.

An increase in system administrators has been noted as a cause of data breaches, and that privilege abuse is the leading cause of data breaches from internal actors.¹ Cybersecurity sustainability requires strong IGA as organizations migrate to the cloud, yet many business models fail to recognize the risk inherent in their legacy solutions. Thus, to maintain data privacy and security, enterprises need to focus their digital transformation business strategies on identity access and use risk because new technologies that incorporate cloud-based and on-premises architectures fundamentally rely on governing access, not just to the cloud but within it. The World Economic Forum (WEF) highlights the need to create sustainable digital transformation strategies and incorporates sustainable development as a necessary step to becoming an economic leader as part of Industrial Revolution 4.0.² Under the umbrella of Sustainable Digital Transformation, the WEF incorporates innovation, entrepreneurship, and artificial intelligence (AI) and robotics. Meanwhile, it focuses on technological sustainable development as responsible innovation that incorporates AI,

Joe Raschke, CRISC, CIPP, CISSP

Is a field chief technology officer with Saviynt and has spent the majority of his career across many vertical markets including manufacturing, financial, legal and healthcare. Raschke has managed teams of people at organizations ranging from regional to global enterprises to develop infrastructure, security and compliance programs. Bringing insight into the mind of a chief information security officer, Raschke, a long-time ISACA® member, has implemented regulatory programs to address today's complex compliance requirements, such as the US Health Insurance Portability and Accountability Act (HIPAA)/the Health Information Technology for Economic and Clinical Health Act (HITECH), the US Sarbanes-Oxley Act (SOX), and the EU General Data Protection Regulation (GDPR).

Karen Walsh, J.D.

Is a product marketing manager at Saviynt who spent 12 years working in internal audit. Focused on risk management and compliance, Walsh uses her law background to align products and tools with information security requirements including the International Organization for Standardization (ISO) ISO 27000 series, US National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53, the Payment Card Industry Data Security Standard (PCI DSS), GDPR, New York State Department of Financial Services Cybersecurity Regulation, Saudi Arabian Monetary Authority Cybersecurity Framework (SAMA), Banking Supervisory Requirements for IT (BAIT), Minimum Requirements for Risk Management (MaRISK), the revised Payment Services Directive (PSD2), Basel III/IV, Society for Worldwide Interbank Financial Telecommunication (SWIFT), Committee of Sponsoring Organizations of the Treadway Commission (COSO), HIPAA (also, specifically, the Health Information Trust Alliance Common Security Framework [HITRUST]), US Federal Risk and Authorization Management Program (FedRAMP), and COBIT®.

mobility and agile governance.³ To achieve sustainable digital transformation using a sustainable development model, organizations need to align their on-premises technologies with new cloud-based technologies, including Software-as-a-Service (SaaS) applications and cloud-based infrastructures. Problematically, many organizations find themselves struggling to meet data privacy requirements as they begin their digital transformation strategies because they focus on technology first and leave data privacy and security for later. To protect data privacy while modernizing business operations, digital transformation strategies must incorporate policies and processes that create dynamic user access while providing visibility into the ecosystem.

The Unique Challenges of Governing Identity in the Cloud

Security challenges arising from cloud migration mimic the challenges in sustainable environmentalism. Digital transformation creates a complex, interconnected ecosystem that often requires legacy on-premise applications to connect with cloud-based software and infrastructures. Industry analysts note that the average organization spent US\$343,000 on SaaS deployments in 2018, an increase of 78 percent compared to 2017.⁴ Whether connecting their current on-premises operations to cloud-based applications or trying to create a cloud-only IT infrastructure, organizations need to shift their thinking. Traditional on-premises IT infrastructures created isolated environments, but modernized architectures incorporate on-premises, hybrid and cloud-based ecosystems. Digital transformation creates complex, interconnected architectures that continuously evolve, similar to physical ecosystems.

Although digital transformation and its associated ecosystems exist as software rather than plants, the different digital ecosystem constructions and the need to create total digital ecosystem protection programs parallel the struggles facing the physical world:

- **Different assets and cloud providers**—No two cloud providers are the same. Moreover, no two enterprise architectures are the same. Some enterprises may adopt mature Infrastructure-as-a-Service (IaaS) cloud service providers, such as Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP), that incorporate



application programming interfaces (APIs) with robust auditing controls. However, other organizations may incorporate less mature SaaS providers in conjunction with their on-premises architecture, leading to a loss of visibility. These different views of identity and access information obfuscate what people are doing with their access. Additionally, some SaaS providers do not provide the same level of open APIs and role-based security models.

- **Risk-based approach to security**—Security lacks a one-size-fits-all strategy, which means as the enterprise migrates some or all of its business operations to the cloud, it should focus on critical assets first. Meanwhile, the interconnectedness inherent within these new IT infrastructures creates a lack of visibility over access and resource use, making it difficult to apply user access controls as required by the Shared Responsibility Model. As users request more access to resources and the organization increases the number of technologies used, organizations find themselves facing compliance gaps or struggling with cumbersome ways of mitigating risk.
- **Compliance across ecosystem**—Without appropriately setting controls that align with established risk tolerances and continuously monitoring for exceptions, organizations lack

“SECURITY CHALLENGES ARISING FROM CLOUD MIGRATION MIMIC THE CHALLENGES IN SUSTAINABLE ENVIRONMENTALISM.”

consistent control over data access and use, which leads to noncompliance.

Business-critical needs drive enterprise ecosystem decisions, which further complicates the ability to set data privacy and security controls. Just as the coral reef's ecosystem differs from the tundra, so does each enterprise's ecosystem, requiring organizations to create their own unique set of requirements. For example, consider three scenarios for creating an IGA program for the cloud (**figure 1**).

Each enterprise needs to start with a risk-based IGA process grounded in business-critical requirements to create a flexible, resilient access process that scales across the complex ecosystem rather than treating it as an afterthought. Moreover, each enterprise needs a way to empower users to obtain access to information necessary to perform their job functions. However, current legacy models fail to meet these ecosystem needs while also providing the documentation necessary for proving governance during an audit.

Defining Identity Across On-Premises, Hybrid and Cloud Ecosystems

The cloud establishes new identities and new technological business enablements. For example, as remote work and employee mobility become the norm, enterprises need to find ways to create identity and access management programs that incorporate the different definitions for roles and groups across the ecosystem. These hybrid identities use and access data across collaboration sites and infrastructure components to create a seamless set of business processes. Identities—

both human and application—need access to cloud and on-premises IT infrastructures. Hybrid identities encompass access to servers, application and resources that often set different policies and requirements. Moreover, hybrid identities can include people, application accounts, system accounts or robotic process automation (RPA) that access resources. Defining identity in the cloud creates a challenge when trying to create a sustainable cloud ecosystem.

Hybrid identities can occur not only within hybrid IT environments, but within geographical locations as well. Strategic business units within global enterprises often benefit from using their own local IT resources, adding an additional dimension to infrastructure access and data-use security.⁵ Strategic business units enable large organizations to address market uncertainty. Thus, digital business models governing identity need to address the need for localized IT infrastructures and organizational platform use.

Organizational platforms such as cloud-based ERP systems enable standardization of access and use across the organization. However, strategic business units often need to create or process data about their localized market. Many choose to create their own IT applications as a way to manage their data needs outside of the organization's platform.⁶ Meanwhile, this leads to significant risk arising from coarse-grained entitlements that, ultimately, cause unauthorized access and use. Defining identity in the cloud requires detailed, fine-grained entitlements for user access to resources, such as read/write access as opposed to view-only access in collaborative tools, to ensure that organizations appropriately limit access.

Figure 1—Scenarios for Creating an IGA Program for the Cloud			
	Enterprise 1	Enterprise 2	Enterprise 3
Phase 1	Use human resource connections as authoritative source of identity to understand people and their roles.	Start with enterprise resource planning (ERP) to protect data to understand how to manage business operations.	Establish a governance structure for risk-based provisioning/deprovisioning and enroll business-critical applications in parallel.
Phase 2	Connect applications to the IGA solution.	Onboard users already stored in an on-premises identity warehouse.	Retire and replace legacy tools.
Phase 3	Connect partners to the IGA solution to promote vendor-risk management strategies.	Ensure that attestations meet compliance requirements.	Enroll all applications to build brand.

Defining Cybersustainability

Inherently, cybersecurity professionals recognize the parallel struggles facing the physical and digital environments as they increasingly adopt terminology such as digital ecosystem, data leakage and cyberpollution. These terminologies, rooted in the physical environmental movement, indicate that digital transformation may require applying sustainability theory to data privacy and security.

Two simple definitions of sustainability exist. The first definition focuses on the ability to maintain a rate or level. The second definition, focused on the environmental movement, categorizes sustainability as a way to avoid resource depletion in a way that maintains ecosystem balance.⁷ Both definitions apply to the cybersecurity problems facing organizations migrating their business-critical operations to the cloud. Cloud migration strategies require organizations to maintain data privacy and security at a consistent level based on their risk tolerance. Second, they need to engage in security and privacy activities without depleting their financial resources.

To create economically sustainable digital transformation strategies, organizations need to find ways to secure their digital ecosystems. Lacking the appropriate privacy and security protections, the data-breach-risk costs associated with digital transformation and cloud migration strategies will outweigh the operational benefits. On-premises, hybrid and cloud IT infrastructures create complex digital ecosystems consisting of users and integrated applications across multiple cloud environments. In the digital ecosystem, a user with excess access creates a data leakage risk that can ripple through the cloud infrastructure. For example, an organization that accepts payments may create a multi-cloud ecosystem to meet Payment Card Industry Data Security Standard (PCI DSS) compliance requirements with one cloud for cardholder data and another for business operations. Single sign-on solutions provide access and authentication to these cloud environments, but they lack the ability to limit access within the ecosystem. Lacking the ability to limit access to least privilege necessary, a single user may lead to a digital ecosystem imbalance arising from excess access and cause a data leakage. If organizations

“FOR ORGANIZATIONS TO INCREASE REVENUE BY USING NEW TECHNOLOGIES, THEY NEED TO KEEP THE FUTURE AT THE FOREFRONT AND PLAN ACCORDINGLY TO PROTECT DATA PRIVACY.”

cannot appropriately protect digital asset privacy and security, digital transformation will become untenable.

For organizations to increase revenue by using new technologies, they need to keep the future at the forefront and plan accordingly to protect data privacy. Digital transformation strategies require cybersustainability. In this context, cybersustainability means:

- Adopting/maturing digital transformation strategies
- Establishing access and governance policies that promote cyberhealth
- Continuous monitoring to maintain data privacy/security
- Communicating across stakeholders
- Promoting operational resiliency

At its core, digital transformation exists to enable an organization's users—internal and external. Beyond enabling users, organizations need to promote healthy cybersecurity to protect people's data privacy and security. Migration plans, in conjunction with data privacy and security risk, highlight the importance of creating a sustainable cyberecosystem rooted in people. Thus, as organizations move forward with their digital transformation strategies, they should establish a program founded on governing access and identity that reinforces cybersustainability within their cloud ecosystems.

Applying Sustainable Development Theory to Cybersecurity

The comparison between physical and digital ecosystems opens the door to applying environmental sustainability to cybersecurity.

Bringing together key sustainability theories can provide a road map for creating stronger access controls and strengthening data privacy and security. Sustainable development can be defined as “development that meets the needs of the present without compromising the ability of future generations to meet their own needs.”⁸ Business operations normalize digital ecosystems, meaning that organizations embracing digital transformation need to address current data privacy and security concerns in addition to future concerns.

Cybersecurity professionals recognize the importance of adapting IT strategies to meet current and future needs. Eighty-seven percent of business and IT leaders recognize the need to rethink their approach to cybersecurity by focusing holistically on their ecosystems.⁹ Although not speaking to the environmental movement’s definition of sustainable development, Accenture echoes similar sentiments noting, “Security in an ecosystem-driven world is no longer about protecting the organization—it’s about protecting everyone.”¹⁰ Today’s digital transformation strategies need to be forward-thinking to ensure continued data privacy and security.

The primary tenets of sustainable cybersecurity align with the environmental sustainability model.¹¹ Sustainable development within the environmental movement focuses on:

- Economic value
- Healthy ecosystems
- Building community

Comparing the tenets of sustainable development with the concept of cybersustainability further explicates how the two are interrelated (**figure 2**).

In the case of the cloud, organizations adopt cloud migration to achieve economic savings and

increase revenue. Unfortunately, with privilege misuse and system administrator risk increasing, cloud ecosystems require additional controls to remain healthy. Moreover, complex cloud architectures lack visibility, leaving stakeholders siloed from one another, undermining the community-building necessary to maintain a healthy, secure, compliant cloud ecosystem.

As organizations move business-critical operations to the cloud, they need to establish access management programs that prevent the ecosystem pollution arising from the proliferation of cloud access points and identities. To meet increasingly stringent compliance standards, they also need to address communication silos to prevent fines and data breaches that diminish the cloud’s economic value.

Applying Complex Adaptive Systems Theory to Digital Transformation

Businesses and ecosystems are not static; they are dynamic and constantly evolving. Thus, environmentalists incorporated complex adaptive systems (CAS) as a model for creating sustainable development. CAS recognizes the complex behaviors within systems and the way that systems learn from and adapt to changes. Some of the key components relevant to cybersecurity are shown in **figure 3**.¹²

Cybersecurity professionals often address sustainable digital transformation and CAS from the external perspective, choosing to focus on vulnerability monitoring and supply chain data breach from control ineffectiveness. However, transformation such as cloud migration shifts the perimeter. To embrace cybersecurity sustainability, organizations need to look to identity as the new perimeter and treat it as the cornerstone to long-term sustainability within the new digital ecosystem that creates threats for their on-premises, hybrid and cloud IT strategies.

Figure 2—Mapping Sustainable Development Practices to Cybersustainability Practices

Sustainable Development	Cybersustainability
Economic value	Adopting/maturing digital transformation strategies
Healthy ecosystems	<ul style="list-style-type: none"> • Establishing access and governance policies that promote cyberhealth • Continuous monitoring to maintain data privacy/security • Promoting operational resilience
Building community	Communicating across stakeholders

Figure 3—CAS Applied to Digital Transformation

Key Components of CAS	Traditional Definition	Application to Digital Transformation
Self-organization	Interactions and interrelationships not imposed by hierarchical structures	Collaboration tools and integrated applications within the ecosystem
Emergence	New patterns and ideas arising from interactions, interconnection, independencies	Big data, interconnected applications, robotic process automation within cloud infrastructures
Co-evolution	Dynamic and continuously changing adaptation	Dynamic identities, flexibility, scalability
Path dependence	Changes tied to systems and history lacking universal causes and truths	High-level access entitlements within cloud infrastructures lacking detailed privileges
Feedback loops	Changes from individual behaviors create critical formal or informal communication networks	Continuous monitoring, documenting and assurance processes

Applying Environmental Sustainability Governance to Digital Identity

Policy and governance often act as barriers to traditional environmental sustainability efforts. Adaptive governance provides insight for cybersecurity professionals on how to manage the shifting perimeter as business priorities adjust to embrace new technologies. Cybersecurity compliance, particularly when governing identity and access, aligns with the adaptive governance model used by environmental policy researchers. The key tenets of adaptive governance that apply to cybersecurity compliance are shown in **figure 4**.¹³

Cybersustainability: Creating Today's Digital Transformation Strategies for Tomorrow's Needs

IT modernization is no longer a growing trend but a business imperative. Many digital transformation efforts shift the perimeter, changing the face of security. Today, enterprise operations rarely remain fully contained within an organization's physical location, and, for example, as on-premises, hybrid and cloud architectures evolve, organizations must create sustainable cyberstrategies that address the new perimeter—identity and access.

Figure 4—How Adaptive Governance Applies to Cybersecurity Compliance

Key Tenet of Adaptive Governance	Traditional Definition	Application to Digital Transformation
Complexity and scale	Interactions within and across location and time	Large organizations incorporate remote workers and vendors in different geographic locations and time zones
Resilience	Reorganizing or adapting while retaining foundational functions and characteristics	Identity and access need to retain their purpose while reorganizing or adapting to the new digital landscape
Networks	Self-organizing multilevel networks to enable learning, trust and information sharing	Access to digital networks needs to enable self-servicing based on trust management and information sharing
Institutions, adaptation and social learning	Structures of rules, laws, policies and norms that incentivize people's actions	Access policies need to create rules and norms that incentivize collaboration while maintaining privacy and security
Power and agency	Transformation through powerful actors championing transformation, providing leadership, generating trust, managing conflicts, preparing for change and establishing educational opportunities	Security professionals and senior management need to work together to promote digital transformation by managing cloud identities to prevent segregation of duties (SoD) conflicts; secure joiner/mover/leaver provisioning; and continuously, rapidly adapt to new access needs
Outcomes	Evaluation of whether desired outcomes occur	Audits provide assurance over whether security controls meet desired levels

Enjoying this article?

- Read *Continuous Oversight in the Cloud*. www.isaca.org/continuous-oversight
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. <https://engage.isaca.org/onlineforums>



Cybersustainability, like environmental sustainability, means establishing new processes and procedures for managing resources. Fundamentally, digital transformation exists to enable people, who, ultimately, streamline business operations. Employees need access to resources related to their job functions. Contractors need access to resources to meet contractual obligations. Customers need access to retail accounts. Patients need access to health records. People lie at the heart of digital transformation strategies. Managing user access to resources needs to focus on ensuring that the right people maintain least privileged access to the right resources for the right amount of time.

Changes such as the use of hybrid and cloud infrastructures enable organizations to meet future digital needs. Unfortunately, meeting those needs requires organizations to change the way they engage in identity and access management. Controlling on-premises devices and applications using traditional solutions such as login and password no longer provide a secure approach to data privacy, as many remain rooted in legacy role-based access policies.

Applying environmentalism's sustainable development to achieve sustainable digital transformation requires reassessing IGA and focusing on hybrid, dynamic identities rather than legacy solutions. Since both people and digital transformation technologies such as the cloud are dynamic in nature, organizations should begin focusing on dynamic identities that incorporate context to ensure compliance with least-privilege-necessary mandates and to prevent SoD violations. Maintaining an unpolluted cloud ecosystem—that is, one lacking data leakage—requires organizations to refocus their strategies and embrace cybersustainability.

Endnotes

- 1 Verizon, *2019 Data Breach Investigations Report*, USA, 2019, <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>

- 2 World Economic Forum, "Digital Economy and Society," <https://intelligence.weforum.org/topics/a1Gb0000001SH21EAG?tab=publications>
- 3 World Economic Forum, "Sustainable Development," <https://intelligence.weforum.org/topics/a1Gb0000000LHN7EAO?tab=publications>
- 4 Blissfully, *2019 Annual SaaS Trends Report*, <https://www.blissfully.com/saas-trends/2019-annual/>
- 5 Queiroz, M.; P. Tallon; T. Coltman; R. Sharma; "Corporate Knows Best (Maybe): The Impact of Global Versus Local IT Capabilities on Business Unit Agility," Proceedings of the 51st Hawaii International Conference on System Sciences, 2018, <https://scholarspace.manoa.hawaii.edu/bitstream/10125/50539/paper0652.pdf>
- 6 *Ibid.*
- 7 Dictionary.com, "sustainability," <https://www.dictionary.com/browse/sustainability>
- 8 International Institute for Sustainable Development, "Sustainable Development," <https://www.iisd.org/topic/sustainable-development>
- 9 Daugherty, P.; M. Carrel-Billard; M. Biltz; *Secure Us to Secure Me*, Accenture, 7 February 2019, <https://www.accenture.com/us-en/insights/technology/cybersecurity-digital-ecosystem>
- 10 Accenture, "Secure Us to Secure Me Video," https://www.accenture.com/_acnmedia/PDF-94/Accenture-TechVision-Secure-US-Video-Transcript.pdf#zoom=50
- 11 Naudé, M.; "Sustainable Development and Complex Adaptive Systems," *Corporate Ownership & Control*, vol. 10, iss. 1, 2012, <https://pdfs.semanticscholar.org/6c65/79fdb8dd7be13deef3ce766d6b9569906c99.pdf>
- 12 *Ibid.*
- 13 Preiser, R.; R. Biggs; A. De Vos; C. Folke; "Social-Ecological Systems as Complex Adaptive Systems: Organizing Principles for Advancing Research Methods and Approaches," *Ecology and Society*, vol. 23, iss. 4, 2018, <http://eprints.whiterose.ac.uk/133648/1/ES-2018-10212%20%282%29.pdf>