Sustainable Development for Digital Transformation Through Identity Governance and Administration, Part 2

Creating Complex Adaptive Systems for Identity Governance and Digital Transformation Using COBIT 2019

Increasingly, organizations connect their on-premises infrastructures to cloud-based technologies, both from a Software-as-a-Service (SaaS) and an overarching infrastructure perspective. While organizations have developed strategies for securing data privacy and security for their on-premise environments, their adoption of cloud-based technologies to streamline business operations changes their ability to control user access to resources. Cybersecurity professionals refer to the cloud as ephemeral when, in some ways, it is more organic. With constantly growing and changing cloud-based initiatives, organizations need to move beyond static role-based access controls that limit their agility. As organizations move toward adopting digital transformation initiatives (e.g., migrating their business-critical operations to the cloud), the new risk associated with, for example, cloud security, also grows and changes. Integrations between applications streamline business operations and create an interconnected digital ecosystem. The digital ecosystem, much like the physical one, requires a delicate balance. Just as a single chemical spill creates environmental pollution, data leakage pollutes the digital ecosystem. Moving away from on-premises, tightly controlled IT infrastructures pushes the security perimeter away from systems and networks, moving it to identity and access. The *2019 Verizon Data Breach Investigations Report* supports identity as the new perimeter as well, noting that system administrators accounted for an

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, JD
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®.

increased number of threat actors, and that privilege abuse was the primary internal actor cause of data breaches.[1] With identity as the new data privacy and security perimeter within cloud ecosystems, COBIT® 2019[2] can act as a framework for establishing a complex adaptive identity and access program that supports cybersustainability.

> "PREDICTIVE ACCESS PROTECTS DATA PRIVACY AND SECURITY IN REAL TIME, REGARDLESS OF LOCATION."

The Need for Predictive Access

Complex, interconnected cloud architectures mimic environmental ecosystems. In the physical world, each organism depends on the others to maintain the habitat. The coral reef, for example, provides a home for algae, while the algae provide nourishment to the coral. In the same way, organizations adopting digital transformation provide revenue for their technology partners, while those partners streamline business operations. These symbiotic relationships not only provide a parallel between the environmental movement and digital transformation, but they highlight the importance of incorporating sustainable strategies for technology adoption. Cybersustainability can be defined as:[3]

- 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

With identity as the new perimeter, digital transformation strategies need to treat identity governance and administration (IGA) as the foundation for their data privacy and security programs rather than as a value add supplementing their external vulnerability pursuits. In a 2018 paper on access policy control, researchers explained,

> *[the] access control (AC) system will therefore need to adapt dynamically to incorporate risk assessment into the access control process…a main result of these trends is a move away from the traditional perimeter based security model.*[4]

Whether realizing it or not, the researchers embraced cybersustainability when focusing on the shift from external security to access enforcement. By discussing the importance of a dynamic, adaptive access system, they acknowledge the organic nature of the new perimeter—identity.

Problematically for cybersustainability purposes, the adaptive access model only partially responds to the key components of both cybersustainability and the complex adaptive systems model applied to digital transformation. **Figure 1** aligns the primary components of cybersustainability to adaptive access control and predictive access as tools for incorporating CAS theory to digital transformation.

While adaptive access control applies to complex adaptive systems theory in name, it focuses only on decisions related to real-time authorization to a system. Organizations looking to create digital transformation strategies aligned with cybersustainability should seek to incorporate predictive access to mitigate risk arising from excess access within their infrastructures.

Figure 1—Aligning Cybersustainability, CAS, Adaptive Access Control, and Predictive Access

Key Components of Cybersustainability	Complex Adaptive Systems (CAS) Applied to Digital Transformation	Adaptive Access Control	Predictive Access
Adopting/maturing digital transformation strategies	Big data, interconnected applications, robotic process automation within cloud infrastructures	• Controls access to a system or network	• Controls access within a system or network
Establishing access and governance policies that promote cyberhealth	High-level access entitlements within cloud infrastructures lacking detailed privileges	• Incorporates user identity, mission need, security risk assigned to system accessed	• Incorporates user identity, mission need, security risk assigned to system and security risk assigned to data types within the system
Continuous monitoring to maintain data privacy/security	Continuous monitoring, documenting and assurance processes	• Requires association with sources that provide real-time information • Requires assessment of each authentication request	• Natively incorporates analytics for continuous monitoring • Suggests access based on similarly situated users • Prevents excess access and enables appropriate additional access when necessary
Communicating across stakeholders	Collaboration tools and integrated applications within the ecosystem assurance processes	• Integrates natively with applications and infrastructures	• Integrates natively with applications and infrastructures • Single source of information for auditability

Predictive access controls focus on risk-based policies and entitlements that enable organizations to prove governance of the data privacy and security postures. Predictive access protects data privacy and security in real time, regardless of location. As users request access to the new resources necessary to fulfill their job functions, predictive access uses peer-based and usage-based analytics that align with policies. These predictive access controls go beyond authenticating the identity to ensuring that the authenticated identity should be accessing the resource. While adaptive access streamlines authentication as users access IT ecosystems from different locations, predictive access controls act as a proactive strategy that supports cybersustainability as a complex adaptive system by protecting access to resources within the cloud ecosystem to ensure that users have the right access to the right resources at the right time.

Working within the cloud, predictive access analytics uses big data to incorporate more context for these identities providing detailed, fine-grained entitlements across all collaborative and cloud-native applications to ensure continuous monitoring of continuous assurance.

Complex Adaptive Systems and Risk-Based Compliance

In the physical environment, complex adaptive systems respond to new patterns arising from new ideas, interactions and interrelationships. Similarly, cybersustainability requires organizations to adapt to new threats and new risk factors. Continuous monitoring over the organization's ecosystem, as viewed traditionally, focuses on external threats. However, as privilege misuse and system administrator risk increasingly impact data privacy and security, organizations need to begin focusing on creating adaptive identity and governance programs grounded in continuous monitoring and new risk.

Risk-based industry standards and regulatory compliance requirements align with this need to embrace complex adaptive system theory. The

> THE PRINCIPLES OF EMERGENCE, CO-EVOLUTION AND PATH DEPENDENCE ALL INHERENTLY INTEGRATE RISK.

principles of emergence, co-evolution and path dependence all inherently integrate risk. For example, in the physical environment, an animal's adaptation to the ecosystem often arises out of a new risk, such as London's moths changing color after the Industrial Revolution to remain hidden from predators.[5] In the same way, risk-based compliance requirements that incorporate continuous risk monitoring seek to respond to new data threats and promote adaptation through an iterative risk-response-mitigation process.

COBIT 2019 addresses variation from one organization to the next. Specifically, the *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*[6] notes that management objectives set the design, but that the various factors then feed back to the capability levels. Using COBIT 2019's iterative risk-respond-mitigate-monitor cycle as a framework for IGA in on-premises, hybrid and cloud ecosystems, organizations can focus on the new perimeter with an adaptive compliance standard that enables stronger cybersustainability.

COBIT 2019: A Compliance Framework for Cybersustainability

COBIT 2019 provides a way for organizations to incorporate cybersustainability while ensuring that they appropriately secure access, monitor effectiveness and prove the benefits of their program to management. As described in the *COBIT® 2019 Framework: Governance and Management Objectives*,[7] its core objectives and Evaluate, Direct and Monitor (EDM) EDM02 *Ensure Benefits Delivery*, establish the framework as a model that can be used to promote cybersustainability. **Figure 2** aligns COBIT 2019's EDM02 with environmental sustainable development theory and cybersustainability.

COBIT 2019 is a framework rooted in providing economic value while promoting communication across stakeholders regarding policies that enable cyberhealth, continuous monitoring and operational

Figure 2—Applying Sustainable Development and Cybersustainability Principles to EDM02

Sustainable Development	Cybersustainability	COBIT 2019
Economic value	Adopting/maturing digital transformation strategies	***EDM02 Ensure benefits delivery*** Purpose: Secure optimal value from information and technology (I&T)-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.
Healthy ecosystems	Establishing access and governance policies that promote cyberhealth Continuously monitoring to maintain data privacy/security Promoting operational resiliency	1.3.1: Governance objectives are grouped in the EDM domain. In this domain, the governing body evaluates strategic options, directs senior management on the chosen strategic options and monitors the achievement of the strategy. Management objectives are grouped in four domains: • Align, Plan and Organize (APO) addresses the overall organization, strategy and supporting activities for I&T. • Build, Acquire and Implement (BAI) treats the definition, acquisition and implementation of I&T solutions and their integration in business processes. • Deliver, Service and Support (DSS) addresses the operational delivery and support of I&T services, including security. • Monitor, Evaluate and Assess (MEA) addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements.
Building community	Communicating across stakeholders	1.1.1: Governance ensures that: • Stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives. • Direction is set through prioritization and decision-making. • Performance and compliance are monitored against agreed-on direction and objectives.

resiliency. Organizations using it can create policies, processes and procedures today that can later adapt to new risk factors, thus advancing cybersustainability.

COBIT 2019: Creating Complex Adaptive Systems for Identity Governance and Digital Transformation

Establishing COBIT 2019 as a framework that aligns with cybersustainability principles requires bringing together the key tenets of the environmental principles and aligning them with specific COBIT 2019 guidelines.

Applying complex adaptive systems theory to the workflow, COBIT 2019 engages the key principles of CAS as applied to digital transformation as seen in **figure 3**.

Finally, applying complex adaptive governance to the workflow, **figure 4** shows what COBIT 2019 can enable.

COBIT 2019: Creating Cybersustainable Identity and Access Processes

Delving deeper into COBIT 2019, the framework supplies a workflow that supports cybersustainability for managing access and identity across on-premises, hybrid and cloud ecosystems. With identity as the new perimeter, organizations using the COBIT 2019 framework can establish flexible IGA programs that help secure identity and access.

Figure 5 highlights the iterative and adaptive nature of identity governance within COBIT 2019.

The continuous monitoring over access controls in conjunction with the requirement to continually improve processes establishes a risk-based approach to IGA. This risk-based approach, when applied to CAS theory, further reinforces the COBIT 2019 framework as one that enables cybersustainability as outlined in **figure 6**.

> “INTERCONNECTED CLOUD INFRASTRUCTURES CREATE COMPLEX DEFINITIONS OF IDENTITY THAT REQUIRE PREDICTIVE ACCESS.”

Figure 3—Applying Complex Adaptive Systems Theory to COBIT 2019 for Cybersustainable Digital Transformation

Key Components of CAS	Traditional Definition	Application to Digital Transformation	COBIT 2019
Self-organization	Interactions and interrelationships not imposed by hierarchical structures	Collaboration tools and integrated applications within the ecosystem	Internal stakeholder communications are necessary to design the program.
Emergence	New patterns and ideas arising from interactions, interconnection, independencies	Big data, interconnected applications, robotic process automation within cloud infrastructures	Organizations embracing cutting-edge automation can be disruptors.
Co-evolution	Dynamic and continuously changing adaptation	Dynamic identities, flexibility, scalability	Iterative process enables organizations and identity governance to evolve together.
Path dependence	Changes tied to systems and history lacking universal causes and truths	High-level access entitlements within cloud infrastructures lacking detailed privileges	Choices made at the APO level impact decisions and activities at the DSS level.
Feedback loops	Changes from individual behaviors create critical formal or informal communication networks	Continuous monitoring, documenting and assurance processes	Monitoring over identity and access create a continuously evolving feedback loop.

Figure 4—Applying Adaptive Governance Theory to COBIT 2019 for Cybersustainable Digital Transformation			
Key Tenet of Adaptive Governance	**Traditional Definition**	**Application to Digital Transformation**	**COBIT 2019**
Complexity and scale	Interactions within and across locations and time zones	Large organizations incorporate customers, remote workers and vendors in different geographic locations and time zones.	Flexibility and feedback enable complexity and scale.
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.	Continuous iteration enables focusing on 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.	Continuous monitoring enables trust management and information sharing through the review process.
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.	Apply emerging standards allows for access policies to incorporate new 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.	Security professionals and senior management provide feedback and review to manage cloud identities to prevent SoD conflicts, secure joiner/mover/leaver provisioning, and adapt to new access needs rapidly.
Outcomes	Evaluation of whether desired outcomes occur	Audits provide assurance on whether security controls meet desired levels.	Audits provide assurance on whether security controls meet desired levels.

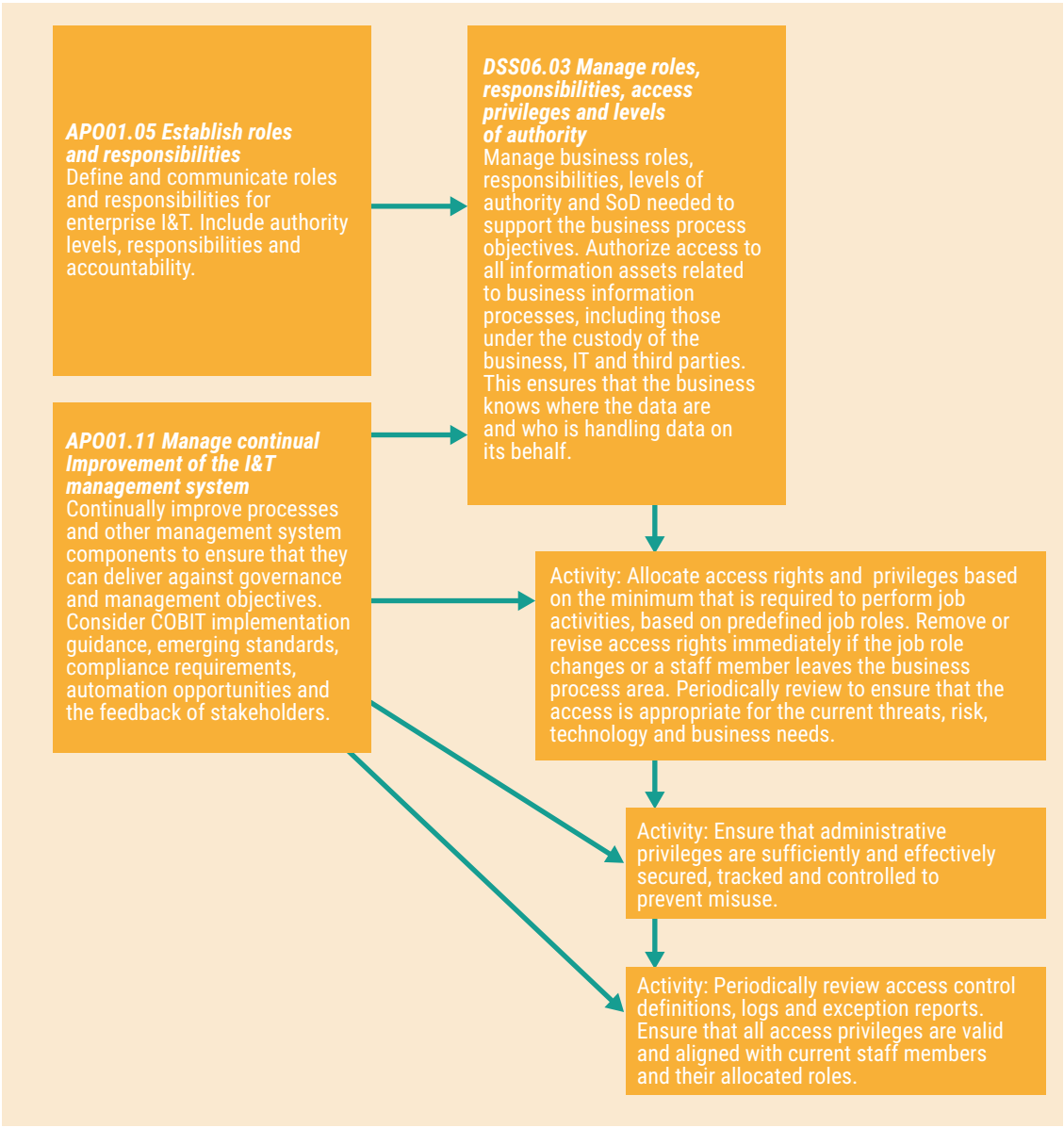
Aligning with complex adaptive theory as redefined for cybersustainability, COBT 2019's access workflow acknowledges and responds to identity's shifting, dynamic nature across on-premises, hybrid and cloud ecosystems. Interconnected cloud infrastructures create complex definitions of identity that require predictive access. COBIT 2019 addresses the need to continuously monitor access controls and continually improve processes. Using predictive access controls, organizations can close the feedback loops to meet COBIT's requirements.

COBIT 2019: Adaptive Governance for Cybersustainable Identity and Access Policies

Having situated COBIT as a framework that enables cybersustainability, organizations using it need to establish programs and processes. Traditional approaches to identity governance lack the flexibility to meet evolving identity governance needs as organizations incorporate new technologies. COBIT 2019's introduction outlines four principles underlying its methodology:

1. Flexibility and openness

Figure 5—The Iterative and Adaptive Nature of Identity Governance in COBIT 2019



2. Currency and relevance
3. Prescriptive application
4. Performance management of IT

These four underlying principles, when combined with IGA, reinforce the way in which COBIT enables organizations to create cybersustainable identity and access programs that incorporate governance and auditability.

Of note, when reviewing COBIT 2019 as a complex adaptive system, the framework's requirements for IGA easily fit into a single key theory component. However, when viewing COBIT 2019 through the lens of adaptive governance, the individual requirements align in a more fluid manner. For example, viewed as a complex adaptive system, COBIT's requirement for authorizing access is a function of emergence—the interconnected nature of a complex adaptive system. However, viewed

Figure 6—Applying CAS Theory to the COBIT 2019 Model of Identity Governance			
Key Components of CAS	**Traditional Definition**	**Application to Digital Transformation**	**COBIT 2019**
Self-organization	Interactions and interrelationships not imposed by hierarchical structures	Collaboration tools and integrated applications within the ecosystem	• Define and communicate roles and responsibilities for enterprise I&T including authority levels, responsibilities and accountability.
Emergence	New patterns and ideas arising from interactions, interconnection, interdependencies	Big data, interconnected applications, robotic process automation within cloud infrastructures	• Manage business roles, responsibilities, levels of authority and SoD needed to support the business process objectives. • Authorize access to all information assets related to business information including those under the custody of the business, IT and third parties.
Co-evolution	Dynamic and continuously changing adaptation	Dynamic identities, flexibility, scalability	• Allocate access rights and privileges based on the minimum required to perform job activities, based on predefined job roles. • Remove or revise access rights immediately if the job role changes or a staff member leaves the business process area.
Path dependence	Changes tied to systems and history lacking universal causes and truths	High-level access entitlements within cloud infrastructures lacking detailed privileges	• Ensure that administrative privileges are sufficiently and effectively secured, tracked and controlled to prevent misuse.
Feedback loops	Changes from individual behaviors create critical formal or informal communication networks	Continuous monitoring, documenting and assurance processes	• Periodically review access control definitions, logs and exception reports. • Continually improve processes and other management system components to ensure that they can deliver against governance and management objectives. • Consider COBIT implementation guidance, emerging standards, compliance requirements, automation opportunities and the feedback

through the lens of adaptive governance, the requirement for authorizing access aligns with two principles from **figure 6**: "networks" and "institutions, adaptation and social learning." This fluidity highlights the difference between the system itself and creating policies that govern the system. As complex adaptive systems, in this case IT infrastructures, evolve along a path dependency, policies and governance need to be dynamic rather than static.

Creating Sustainable Privacy and Security With COBIT 2019

Complex adaptive systems for IGA need to incorporate a variety of new technologies that provide greater insight into how users access data, where they access data, and the risk factors that arise from embracing these new technologies and capabilities. Legacy solutions limit sustainable cybersecurity practices as they often lack the ability

Figure 7—Applying Adaptive Governance Theory to the COBIT 2019 Model of Identity Governance

Key Tenet of Adaptive Governance	Traditional Definition	Application to Digital Transformation	COBIT 2019
Complexity and scale	Interactions within and across locations and time zones	Large organizations incorporate remote workers and vendors in different geographic locations and time zones.	• Define and communicate roles and responsibilities for enterprise I&T, including authority levels, responsibilities and accountability.
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.	• Remove or revise access rights immediately if the job role changes or a staff member leaves the business process area.
Networks	Self-organizing multilevel networks to enabling learning, trust and information sharing	Access to digital networks needs to enable self-servicing based on trust management and information sharing.	• Manage business roles, responsibilities, levels of authority and SoD needed to support the business process objectives. • Authorize access to all information assets related to business information, including those under the custody of the business, IT and third parties.
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.	• Allocate access rights and privileges based on the minimum that is required to perform job activities, based on predefined job roles. • Authorize access to all information assets related to business information including those under the custody of the business, IT, and third parties.
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 SoD conflicts; secure joiner/mover/leaver provisioning; and continuously, rapidly adapt to new access needs.	• Define and communicate roles and responsibilities for enterprise I&T, including authority levels, responsibilities and accountability. • Ensure that administrative privileges are sufficiently and effectively secured, tracked and controlled to prevent misuse
Outcomes	Evaluation of whether desired outcomes occur	Audits provide assurance over whether security controls meet desired levels.	• Periodically review access control definitions, logs and exception reports. • Continually improve processes and other management system components to ensure that they can deliver against governance and management objectives. • Consider COBIT implementation guidance, emerging standards, compliance requirements, automation opportunities and the feedback of stakeholders.

to manage dynamic, evolving identity and access needs. To meet the organic demands of the cloud, organizations need predictive technologies that provide insight into their access and use as they shift their threat detection mentalities to make their core focus people—the new perimeter.

> “LEGACY SOLUTIONS LIMIT SUSTAINABLE CYBERSECURITY PRACTICES AS THEY OFTEN LACK THE ABILITY TO MANAGE DYNAMIC, EVOLVING IDENTITY AND ACCESS NEEDS.”

Dynamic Transformation, Dynamic Identity, Dynamic Risk

People and the cloud share a dynamic nature, both of which come with inherent risk. Legacy solutions can provide rules and monitor point-in-time compliance, but the cloud’s organic nature is only managed through dynamic intelligent analytics and context for those rules. Even with these inherent and dynamic angles, static factors cannot be ignored when calculating risk.

For example, granting a user application access can lead to data integrity issues associated with the “everyone with a link” sharing risk. Fine-grained, or detailed, access permissions that limit access to read or write access mitigate these excess access risk factors.

Thus, organizations need to incorporate modernized analytics that provide predictive access to address true organizational risk as shown in **figure 8**.

Continuous Monitoring, Continuous Visibility, Continuous Sustainability

Increasing technology to enable compliance obfuscates the overarching view of access and identity, ultimately leading to noncompliance arising from human error across platforms and services. Organizations also need automation to streamline continuous monitoring and documentation processes to create a more robust IGA compliance program and meet the iterative nature of COBIT 2019 compliance. Traditional reports and application-level coarse-grained controls provide little insight, which leaves organizations at risk. For example, role-based access to an application provides access for all users with a similar job function. Organizations need detailed, context-driven entitlements to limit access within the application. The additional context creates a frictionless user experience, while predictive access analytics can prevent SoD violations.

Digital transformation sustainability relies on continuous visibility and monitoring. Organizations need architectures and tools that allow them to control access and streamline operational

Figure 8—Moving From Static to Dynamic Risk Models

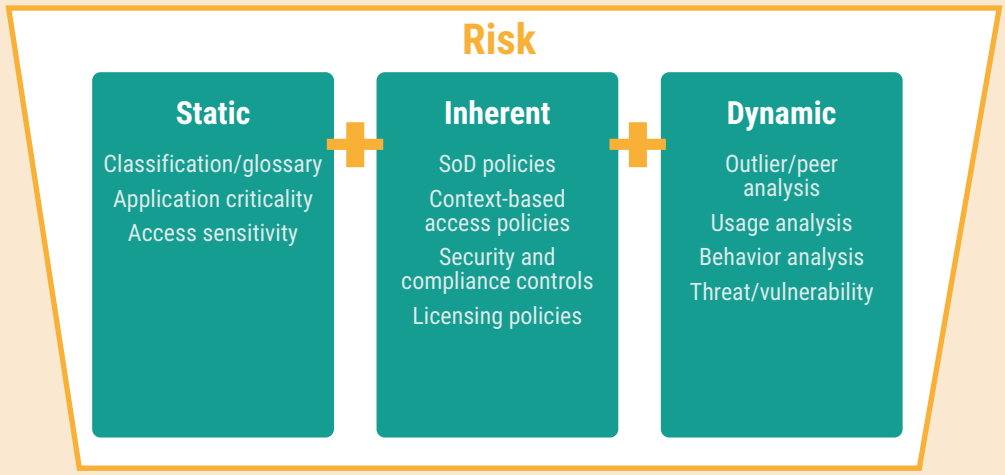
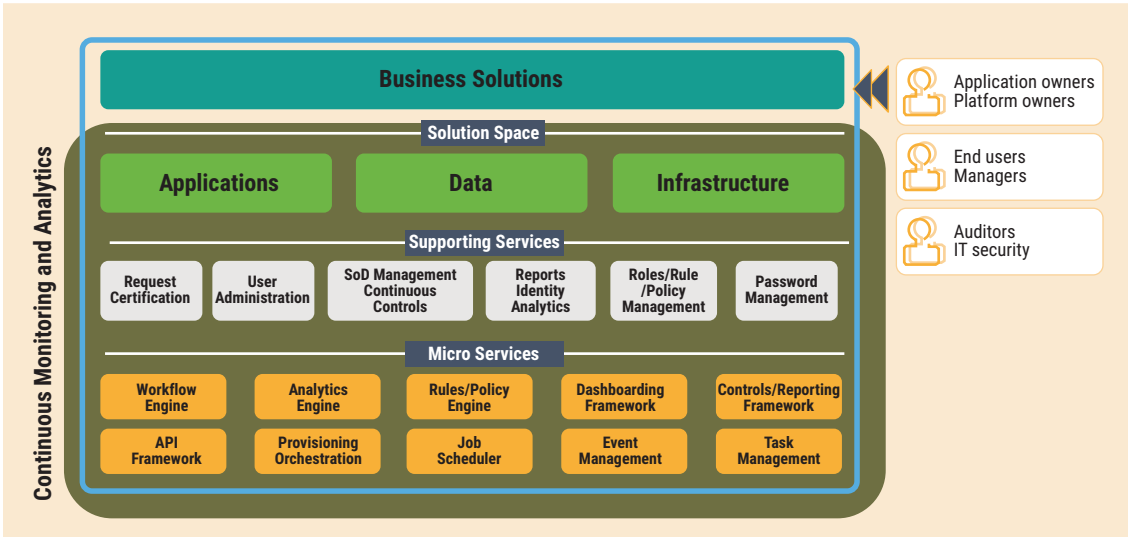


Figure 9—Applying Continuous Monitoring With Predictive Analytics



workflows. Moreover, they need tools that provide auditors with the appropriate documentation. Incorporating intelligent analytics as part of continuous monitoring activities strengthens the organization's cybersecurity posture and, thus, its compliance posture as shown in **figure 9**.

Creating a Fully Sustainable Digital Ecosystem

Although digital transformation enables globalization of business practices, digital transformation security needs to begin at the individual level. Digital transformation strategies increase the number of identities—individuals and applications—that access resources. To create a sustainable digital ecosystem, organizations need digital tools that match the elasticity and velocity of the cloud to promote better organizational hygiene across disparate cloud-based systems and applications. With identity as the new perimeter, cybersustainability needs to include technologies that promote predictive access in ways that can evolve with the new risk arising from digital transformation, such as excess access within a cloud ecosystem. Maintaining data privacy and security as part of a cybersustainable cloud migration strategy, therefore, must start with the principle of least privilege and maintain monitoring to limit privilege misuse.

> "ALTHOUGH DIGITAL TRANSFORMATION ENABLES GLOBALIZATION OF BUSINESS PRACTICES, DIGITAL TRANSFORMATION SECURITY NEEDS TO BEGIN AT THE INDIVIDUAL LEVEL."

Endnotes

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

2 ISACA®, *COBIT® 2019 Framework: Introduction and Methodolgy*, USA, 2018, *www.isaca.org/COBIT*

3 Raschke, J.; K. Walsh; "Sustainable Development for Digital Transformation Through Identity Governance and Administration," *ISACA® Journal*, vol. 5, 2019, *www.isaca.org/archives*

4 Vanickis, R.; P. Jacob; S. Dehghanzadeh; B. Lee; "Access Control Policy Enforcement for Zero-Trust-Networking," 2018 29th Irish Signals and Systems Conference (ISSC), June 2018, p. 1-6

5 Walton, O.; M. Stevens; "Avian Vision Models and Field Experiments Determine the Survival Value of Peppered Moth Camouflage," *Communications Biology*, vol. 1, 2018, *https://www.nature.com/articles/s42003-018-0126-3*

6 ISACA, *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, 2018, USA, *www.isaca.org/COBIT/Pages/COBIT-2019-Design-Guide.aspx*

7 *Op cit* ISACA, *COBIT 2019 Framework*