Rethinking the Effectiveness of Controls in the Digital Age

También disponible en español
www.isaca.org/currentissue

In the midst of international geopolitical turbulence, organizations must mobilize to keep their businesses dynamic and establish long-term strategic postures that define ways forward amid instabilities.[1] Control assurance is one of the key elements of maintaining operational and organizational dynamics when faced with known and latent adverse events.

In general, control assurance is effective when the controls are well defined, respond to the risk they are intended to mitigate, and are implemented on time and in proper form as per stated requirements. This traditional effectiveness leads to a level of confidence in closing the risk gaps that have been identified in different areas of the organization, with particular emphasis on operational and transactional issues.[2]

JEIMY J. CANO M. | PH.D., ED.D., CFE, CICA

Has more than 25 years of experience as an executive, academic and professional in information security, cybersecurity, forensic computing, digital crime and IT auditing. In 2016, he was named Cybersecurity Educator of the Year for Latin America, and in 2022, he was named a Resilience Personality for Latin America. He has published more than 200 articles in various journals and presented papers at industry events at the international level.

A change of perspective on security and controls is needed, moving from a static, defined and known vision to a dynamic, changing and often unknown vision.

Because there is higher digital density in today's society (i.e., increased connectivity and flows of information between physical objects), new threats and emerging challenges can lead to unknown IT risk. These types of emerging, systemic and disruptive risk, such as cyberrisk, do not correspond to the traditional practices and controls of IT; therefore, they need complementary and updated approaches and treatments.[3, 4]

Organizations must adjust their traditional approaches based on known security standards and measures within the industry such as reliability, calibration and maintenance, including adapting and periodically updating to account for changes, new trends and the transformation of organizational operations.[5] A change of perspective on security and controls is needed, moving from a static, defined and known vision to a dynamic, changing and often unknown vision.

With this change in perspective, controls transform from having a single definition and periodic monitoring into sensors that, in addition to the basic definitions based on the business environment and relationships, must be validated based on their reliability, calibration and periodic maintenance. In this sense, the controls must adapt to the new conditions of the environment, which may not be equivalent to the time, manner and place in which they were first defined.

It is important to understand the evolution of the notion of control, its conceptual foundations and the transformation that the measurement of its effectiveness has been undergoing due to accelerated digital dynamics, which, although it creates new possibilities and experiences for customers, also causes tension and introduces threats that could compromise the organization's value.

Foundations of Controls

Understanding the concept of control requires acknowledgment that there are different ways to maintain a dynamic equilibrium (i.e., a balance that responds to any instabilities that arise and finds a common place of operation that fits and connects with the other components of the analyzed ecosystem). In this context, there are four elements that are common and fundamental to all control systems:[6]

1. **Measurable and controllable characteristics**—The standards that are known
2. **Sensors**—Enable the measurement of the characteristic
3. **Comparators**—Discriminate between the data delivered by the sensor and the standards known for the established characteristics
4. **Runners**—The means of effecting change in the system to adjust the relevant characteristics

Establishing a distinction between a controlled and an uncontrolled state directly depends on the executor's assessment of the results provided by the sensor. The executor makes decisions, assesses alternative actions based on the deviations delivered by the comparator and appraises the benefits of adjusting the system to a controlled state.

The determination of the final state being controlled or uncontrolled is based on several considerations, including:

- The detail of the characteristics to be assessed and their standards, which should be known and validated beforehand to keep the system as close as possible to these specifications
- The periodic calibration of the sensor that enables the identification of variations of the standard
- The reliability of the comparator in discriminating between the data collected by the sensor and the known standards
- The executor's vision and context for moving forward with the interpretation of the results and making decisions

The controlled distinction is aimed at regulating, lowering and avoiding any adverse conditions that could threaten the system's initial specifications and the standards that govern it. In this regard, the control seeks to decrease any uncertainty in system operations, which includes reporting any condition that is not within the comparator's specifications and, thus, informing the executor so any necessary actions can be taken.[7]

The key to achieving the desired state of control in the system is feedback—taking the result of the execution of the system, assessing it and then incorporating new data to adjust the system's behavior. If the feedback is timely and uses reliable data, the process will be effective and developed within predefined and known standards established by the organization.[8]

Cybernetic Control: Regulations and Adaptation

Cybernetics is the science of communication and control in living and artificial beings.[9] Using the fundamentals of cybernetics and the concepts of required variety helps entities develop organizational cybernetics, which is the science of effective organization.[10]

The viable system model was proposed as the basis for the development of organizational cybernetics, which establishes two fundamental cycles for achieving organizational viability: the regulation cycle and the adaptive cycle. While the regulation cycle is associated with the natural and general dynamics of organizations that seek to ensure that they are functioning based on good practices and coordination of activities, the adaptive cycle seeks

The key to achieving the desired state of control in the system is feedback—taking the result of the execution of the system, assessing it and then incorporating new data to adjust the system's behavior.

The first step to understanding control effectiveness in a dynamic context is to establish the baseline models and the characteristics intended to be compared and measured.

to challenge the existing dynamics by exploring the environment and identifying emerging trends.[11]

Variety in this context is defined as all the identifiable states in which a system can be found in both perspectives. A system that exhibits many interrelations and couplings between its components may not only have multiple identifiable states, but also unidentifiable states that are outside the initially established specifications, which may or may not be in accordance with the expectations, purposes and context of those that were created when the system was designed.[12]

There are at least three ways that a system can meet its needs for variety:

1. It can amplify its own variety.
2. It can maintain a variety equivalent to that of the controlled system.
3. It can reduce the variety of the controlled system rather than reducing its own.[13]

In this regard, the understanding of control goes beyond achieving a standard. Systems are viable (i.e., sustainable for long periods of time) as long as they can exist independently from their environment. In other words, they should not only have the capacity to respond to known instabilities, but also be prepared for and able to adapt to unexpected or unknown situations and changing environments. To achieve this, they must maintain a balance between amplifying and attenuating the variety within the dynamics of the organization and its operating thresholds and the challenges posed by the environment that are relevant to long-term survival.[14]

The distinction of control from the cybernetics perspective not only ensures the operation of the system within the defined standards (regulation cycle), but also establishes mechanisms for amplifying the variety in the system (adaptive cycle), exploring and identifying novel and uncertain conditions in the environment that are relevant for its survival, updating the initial benchmarks, and, consequently, updating the basic characteristics to be controlled. This should lead to the necessary adjustments in the sensor, the comparator and the executor's criteria to realize the final state of the control.[15]

It is important to note that any residual variety that is not assimilated by the environment's responses should be assimilated by the system, otherwise it runs the risk of creating points of instability and compromising the system's medium- and long-term survival.

LOOKING FOR MORE?

- Read *Bridging the Digital Risk Gap.* *www.isaca.org/bridging-the-digital-risk-gap*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

The Effectiveness of the Control Beyond Standards and Good Practices

The definition and operation of organizational controls has been evolving as the environment becomes more brittle (associated with vulnerability), anxious (created by uncertainty), nonlinear (derived from complexity) and incomprehensible (the result of ambiguity) (BANI).[16] Traditional controls are in crisis because they operate using a static vision based on practices and standards that respond only to known situations and operations based on the reduction of uncertainties to ensure proper decision making.

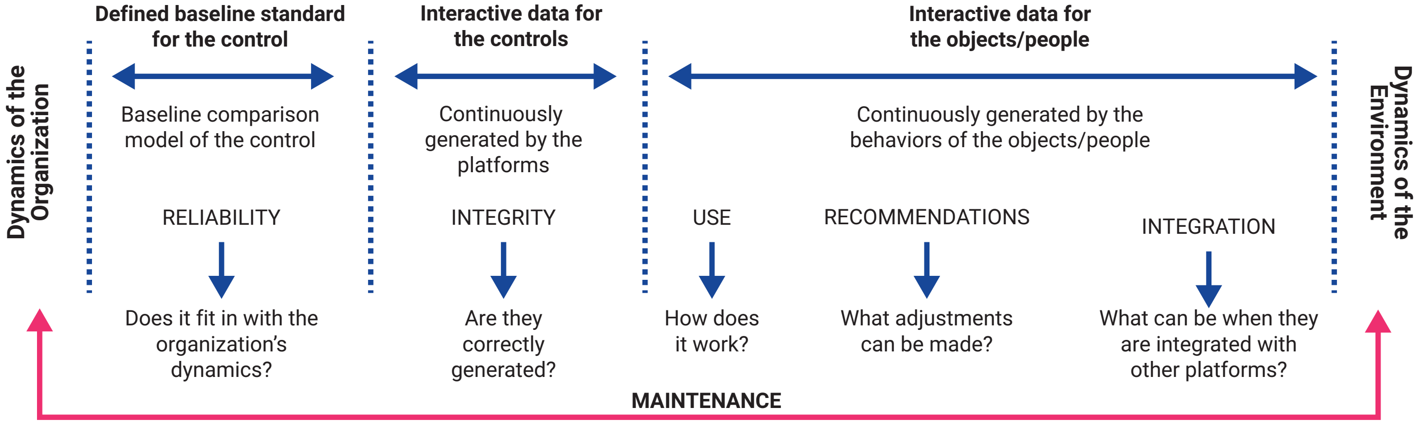
Understanding the effectiveness of controls in BANI scenarios helps ensure that certain conditions detailed in the known frameworks are fulfilled and that the control's sensor is up to date and equipped to handle the variations and instabilities that can occur. The effectiveness of a control in a BANI world is determined by whether it:

- Understands the dynamics of the organization and its purposes
- Understands the dynamics of the environment
- Contributes to the reduction of the risk covered
- Calibrates the sensors in accordance with the use and adjustments of the dynamics of the organization and its environment
- Identifies and analyzes relevant changes in the environment

Figure 1 illustrates the effectiveness of the control in a changing scenario.

FIGURE 1

Understanding the Effectiveness of the Control in Dynamic Contexts


Dynamics of the Organization
Defined baseline standard for the control
Baseline comparison model of the control
RELIABILITY
Does it fit in with the organization's dynamics?
Interactive data for the controls
Continuously generated by the platforms
INTEGRITY
Are they correctly generated?
Interactive data for the objects/people
Continuously generated by the behaviors of the objects/people
USE
How does it work?
RECOMMENDATIONS
What adjustments can be made?
INTEGRATION
What can be when they are integrated with other platforms?
Dynamics of the Environment
MAINTENANCE

The first step to understanding control effectiveness in a dynamic context is to establish the baseline models and the characteristics intended to be compared and measured. This initial exercise defines the reliability of the model the organization wishes to implement, which involves determining whether the defined baseline standard fits with the organization's dynamics and challenges. Then, the control mechanisms are deployed in the relevant areas established by the organization, such as information systems, industrial control systems or any automated system. At this point, whether they are correctly activated and consistent with the established conditions needs to be determined. If an event happens that does not meet the defined standards, it should be reported.

The next phase is understanding the dynamics of the control's operation, including the behavior of both the people and the objects over which the control mechanisms have been defined. It is important to determine the controls' use (do they work as they should?), what adjustments should be made based on how the controls operate and what other trends can be seen when integrating the controls with other platforms. This phase should generate enough information to calibrate the control and update the baseline models that were previously defined during design.

Finally, it is necessary to read, analyze and explore any new trends or signs of weakness observed in the environment to perform maintenance and update the organizational dynamics, which demand the amplification of variety so as to ensure the organization's viability in the short and long term.[17]

The Inevitability of Cybersecurity Control Failure

Many of the controls that are currently used in information security and cybersecurity respond to variety attenuation, looking for certainties and trying to eliminate uncertainties. Executive reports identify known risk as a way of indicating that the measures implemented respond to the dynamics of the organization's environment, which can lead to a false feeling of security through excessive reliance on standards and technological tools.[18]

From a cybersecurity perspective, the controls seek to delay, dissuade or confuse any adversary who may be attempting to gain access to a system. These controls should always validate and recognize emerging patterns in the environment based not only on the behavior of the infrastructure and users, but also on the conditions of event time, mode, place and context. The baseline model should always be learning about correlating events to establish signs of weakness, which may lead to early alerts.[19]

Cybersecurity controls must be balanced between the attenuation of variety (reports and known alerts) and amplification based on patterns of events, unforeseen situations and surprises that enable the protection dynamics defined by the organization to be updated. Consequently, possible detected and undetected vulnerabilities become basic inputs for the necessary creation of a culture of learning and flexibility in the face of the inevitability of failure.

When a cyberrisk arises or a security breach is generated, it implies that the failure of a control has occurred. The effect on the organization can vary depending on the sensitivity of the process and information. Understanding effectiveness in this way means going back to the basic operational and mechanistic model of the control, where error is a result and not part of the process.[20]

Due to the evolving nature of society, a security breach or failure arising through either a vulnerability or an unforeseen event is common. Therefore, the effectiveness of the control must not be linked to the reduction of uncertainty but rather to the ability to maintain alerts, take concrete actions based on known risk, and develop scenarios and forecasts for patterns and signs of latent and emerging risk. Organizations should be continuously questioning and validating risk and strengthening their practices and resilience through simulations and prototypes.[21]

The effectiveness of cybersecurity controls should be measured based on the ability to learn and develop when faced with challenges and instability, not as a technical benchmark that does not consider the dynamics of the business. Organizations should be proactive in discovering and warning of unforeseen and adverse events (which reveal gaps in the current security and control model) to develop watchful, efficient and flexible postures that fit with the organization's operating thresholds, even when a threat becomes reality.[22]

Conclusion

The world is experiencing tremendous changes and tensions that create ongoing instability, leading to challenges for even the most prepared and sophisticated control and management systems. Understanding and assessing the effectiveness of controls is an uncertain and complex challenge that demands the development of skills that reduce the variety of known risk and amplify latent and emerging risk patterns, enabling employees to take action and be flexible and efficient in accordance with the operating thresholds of their organization.[23]

The notion that a best practice for controls is to simply reduce uncertainty widens the gaps in security and control models, because it perpetuates the idea that everything that is not recognized by the defined standards can be ignored, creating a false sense of security that can be taken advantage of by adversaries. Given the cascading effects of cyberrisk, it may be clear where risk starts but not where it might end.[24]

From a cybernetic perspective, controls are a balance between the amplification and reduction of variety. Expanding this definition enables them to have their own dynamics and adjustments that can relate to the relevant organizational variety and its long-term permanence.[25] In this way, the effectiveness of the control seeks to find new points of stability in the organization's dynamics and the environment to create an equilibrium that can change over time and prepare the organization to respond to tensions and instabilities that arise.

> The effectiveness of cybersecurity controls should be measured based on the ability to learn and develop when faced with challenges and instability, not as a technical benchmark that does not consider the dynamics of the business.

Cybersecurity controls should follow this expanded definition and demand the recognition and validation of the reliability and integrity of the platforms that said controls materialize. Controls should also generate the necessary calibration based on their use, adjustments and integration with other systems. Finally, setting up a maintenance strategy that, by consulting the dynamics of the environment, can quickly learn and unlearn to make adjustments (in real time as much as possible) to the standards and baseline models on which it generates its early warnings and emerging patterns.

Understanding the effectiveness of controls includes:

1. Changing the mechanistic view under which the controls were initially designed to create opportunities for learning that establish operating thresholds that are adjusted in accordance with the evolution of the environment and its challenges
2. Quickly learning and unlearning the instabilities and challenges of the organization's operating environment to develop efficient and flexible responses to possible adverse events

It is necessary to accept the inherent vulnerabilities of infrastructure, processes, people and standards as opportunities to learn that the control is not only a mechanism that reveals failures and adverse behaviors, but it is also an opportunity for the ongoing calibration of a sensor to create a resilient, vigilant posture that is capable of responding to and warning of latent realities and events still not visible.

> The notion that a best practice for controls is to simply reduce uncertainty widens the gaps in security and control models, because it perpetuates the idea that everything that is not recognized by the defined standards can be ignored.

Endnotes

[1] Sheffi, Y.; *The New (Ab)Normal: Reshaping Business and Supply Chain Strategy Beyond COVID-19*, Massachusetts Institute of Technology (MIT) Center for Transportation and Logistics, Cambridge, Massachusetts, USA, October 2020, *https://sheffi.mit.edu/book/new-abnormal*

[2] Mejía, R.; *Administración de riesgos. Un enfoque empresarial*, Universidad EAFIT, Medellín, Colombia, 1 May 2020

[3] Sieber, S.; J. Zamora; "The Cybersecurity Challenge in a High Digital Density World," *The European Business Review*, 18 November 2018, *https://www.europeanbusinessreview.com/the-cybersecurity-challenge-in-a-high-digital-density-world/*

[4] Subramanian, M.; "The Four Tiers of Digital Transformation," *Harvard Business Review*, 21 September 2021, *https://hbr.org/2021/09/the-4-tiers-of-digital-transformation*

[5] Avizienis, A.; J.-C. Laprie; B. Randell; C. Landwehr; "Basic Concepts and Taxonomy of Dependable and Secure Computing," *Institute of Electrical and Electronics Engineers (IEEE) Transactions on Dependable and Secure Computing*, vol. 1, iss. 1, 4 October 2004, p. 11–332

[6] Kast, F.; J. Rosenzweig; *Organization and Management: A Systems and Contingency Approach, 3rd Edition*, McGraw-Hill College, USA, 1 January 1979

[7] Reason, J.; *Managing the Risks of Organizational Accidents*, Routledge, UK, 20 January 2016

[8] Beer, S.; *Decision and Control*, John Wiley and Sons, UK, 1994

[9] Beer, S.; *Cybernetics and Management*, John Wiley and Sons, UK, 1964

[10] *Ibid*.

[11] Beer, S.; *Diagnosing the System for Organizations*, John Wiley and Sons, UK, 1995

[12] Espejo, R.; R. Harden; *The Viable System Model: Interpretations and Applications of Stafford Beer's VSM*, John Wiley and Sons, UK, 1989

[13] *Op cit* Beer 1995

[14] *Op cit* Espejo and Harden

[15] Espejo, R.; "Giving Requisite Variety to Strategic and Implementation Processes: Theory and Practice," Proceedings of the JAIST Conference, Ishikawa, Japan, September 2000, *https://www.researchgate.net/publication/228772758_Giving_Requisite_Variety_to_Strategic_and_Implementation_Processes_Theory_and_Practice*

[16] Cascio, J.; "Facing the Age of Chaos," *Medium*, 29 April 2020, *https://medium.com/@cascio/facing-the-age-of-chaos-b00687b1f51d*

[17] Schrader, R.; M. McConnell; "Security and Strategy in the Age of Discontinuity: A Management Framework for the Post-9/11 World," *Strategy+Business*, 9 January 2022, *https://www.strategy-business.com/article/11439*

[18] Cano, J.; La 'falsa sensación de seguridad'. El reto de incomodar las certezas de los estándares y tratar de 'domesticar" 'os inciertos. *Revista SISTEMAS. (SYSTEMS Journal)*, Asociación Colombiana de Ingenieros de Sistemas. (Colombian Association of Systems Engineering), vol. 159, p. 82–95, 2021, *https://doi.org/10.29236/sistemas.n159a6*

[19] Day, G.; P. Schoemaker; *See Soon, Act Faster: How Vigilant Leaders Thrive in an Era of Digital Turbulence*, The MIT Press, USA, 1 October 2019

[20] Schoemaker, P.; *Brilliant Mistakes: Finding Success on the Far Side of Failure*, Wharton Digital Press, USA, 2011

[21] *Op cit* Day and Schoemaker

[22] *Op cit* Cano

[23] Espejo, R.; W. Shuhmann; M. Schwaninger; U. Bilello; *Organizational Transformation and Learning: A Cybernetic Approach to Management*, John Wiley and Sons, UK, 1996

[24] Martin, P.; *The Rules of Security: Staying Safe in a Risky World*, Oxford University Press, UK, 2019

[25] *Op cit* Espejo and Harden