The Role of IT Governance During COVID-19 and Beyond:

Keeping the Momentum

This is an extremely critical and dangerous period in everyone's lives. A single message is heard from every corner of the world: "Stay home." This is a vastly different situation from how the world has functioned for the last five decades.

The World Health Organization (WHO) declared the novel coronavirus outbreak a public health emergency of international concern (PHEIC) on 30 January 2020.[1] According to a WHO situation report, the number of deaths has reached 229,971 and active cases exceed 3,267,184 at the time of this writing.[2]

Global Reaction to the Outbreak and the Use of IT

Many organizations have had to transition to remote workforces indefinitely or closed their doors completely. Governments around the world face the major challenge of maintaining the basic functions of society and preserving their economies.

The work-from-home (WFH) transition has impacted millions, from office workers to world leaders. Governments have encouraged enterprises and essential services to use available technologies to drive their operations, and many organizations have started applying technologies as much as possible to enhance their online presence and facilitate communication and business. Online commerce has become vital. The need for IT solutions has reached its peak.

IT Incidents and the Need for IT Governance

This new reality has resulted in an increased risk of cybercrime and phishing attacks. Criminal actors are taking advantage of changing working conditions to commit fraud and steal sensitive information. Fear, uncertainty and doubt enable criminals to target users still trying to fully understand their new way of working.

The WHO reports a fivefold increase in cyberattacks and urges vigilance:

> *…[S]ince the start of COVID-19 pandemic, the WHO has seen a dramatic increase in numbers of cyberattacks directed at its staff, and email scams targeting the public at large…Some 450 active WHO email addresses and passwords were leaked*

Lionel Jayasinghe, CISA, COBIT5 Foundation, PMP
Is an independent IT consultant with 15 years of experience in IT audit. His prior experience includes software engineering, quality management (Capability Maturity Model Integration [CMMI] standard) and project management. Jayasinghe is a past president of the ISACA® Sri Lanka Chapter. He has served as a senior IT auditor for the Central Bank of Oman, a board member of a public sector bank in Sri Lanka, and the Information and Communication Technology Industry Skill Council (ICTISC) in Sri Lanka. Jayasinghe has written conference papers and articles and has conducted workshops on IT audit, IT governance and software engineering standards for national conferences and professional associations. He can be reached at lionel.jay@gmail.com.

> BECAUSE OF THE UNFORESEEN CIRCUMSTANCES OF THIS PANDEMIC, PRACTITIONERS WORLDWIDE CONTINUE TO FOLLOW IT PRACTICES IN HETEROGENEOUS WAYS.

online along with thousands belonging to others working on the novel coronavirus response.[3]

There is also concern with collecting personal information and tracking the movements of people. It has become a topic of open discussion based on privacy concerns and the possible use of data for purposes other than those for which they have been collected.[4]

Spreading misinformation via various applications such as social media is harmful to the global community. Some countries have experienced delays in dealing with such situations because of a lack of rules and regulations such as the EU General Data Protection Regulation (GDPR) and the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada.

Although business continuity planning (BCP) is an established concept, that does not mean that the majority of organizations around the world have established BCP to deal with situations such as COVID-19. Many of the underlying BCP or disaster recovery planning (DRP) assumptions, such as availability of people to manage necessary operations, does not hold during this pandemic.[5]

Increasing information security incidents, inadequate BCP processes, and issues related to information sharing and IT infrastructure can be triggered by the absence of proper principles, policies and processes in areas such as information security and disaster recovery at the global level. Because of the unforeseen circumstances of this pandemic, practitioners worldwide continue to follow IT practices in heterogeneous ways. IT principles, policies and processes are major components of the IT governance process.

However, it is difficult to find a single IT governance framework that has been established at a global level to govern IT to achieve global objectives. Many institutions and individuals are voluntarily helping by producing various IT devices, software and tools to fight against the threat associated with the pandemic. It might not be possible to realize the full benefit of the effort in the absence of a proper IT governing mechanism within necessary laws.

Beyond Boundaries

The IT governance process is not new to many organizations. IT governance is a process that is defined at the enterprise level. Related frameworks have evolved over time.

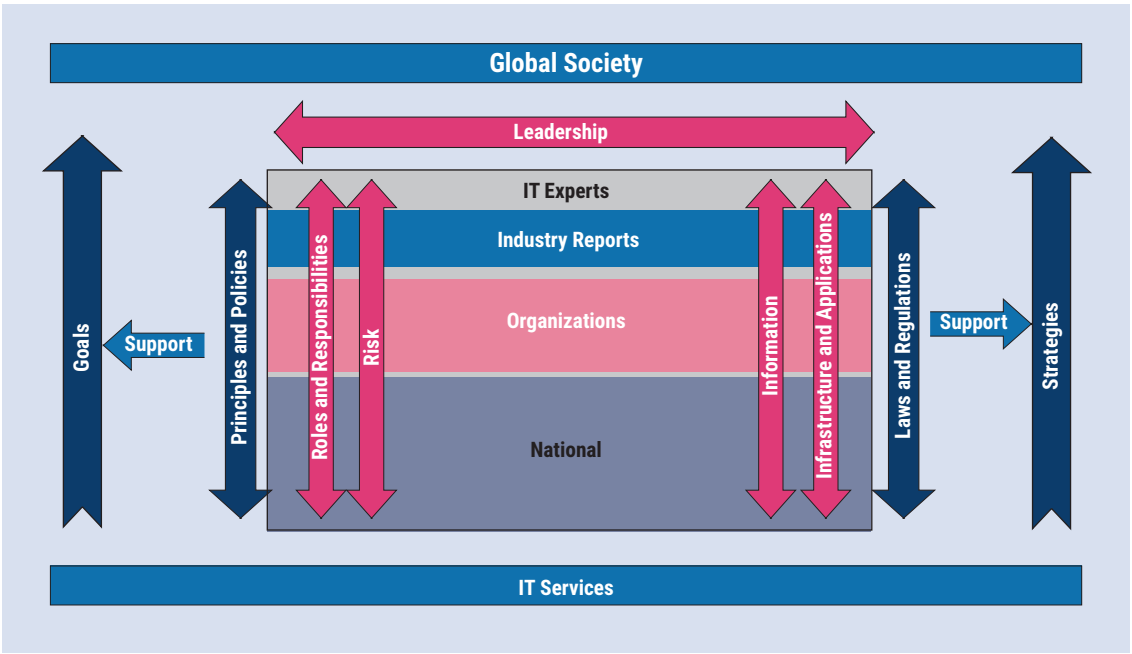
IT governance has been described as a structure of relationships and processes to direct and control in order to achieve enterprise goals by adding value while balancing risk vs. return over IT and its process.[6]

According to the IT Governance Institute (ITGI), IT governance is the form of leadership, organizational structures and processes that ensures that an organization's IT department sustains and extends the organization's strategies and objectives.[7]

The scope, process and boundaries of IT governance are very clear in these definitions. The need to integrate IT skills with other expertise to perform IT activities effectively, securely and ethically in this pandemic is clear.[8, 9]

Many changes to the IT governance process may be needed when shifting from an enterprise level to a national or global level. One major change is shifting goals and objectives. Connecting the IT governance process on a national level with a global level is a fairly complex process. Many aspects need to be considered such as policies and principles and related laws. These aspects are already addressed in the IT governance framework, COBIT®. Organizational Structures, Principles, Polices and Frameworks, Service Infrastructure and Applications, and Information are some of the seven components defined in COBIT®.[10] **Figure 1** shows the organizational structure and sharable, vital aspects of IT governance on a global level.

Figure 1—Governing IT on the Global Level



The organizational structure consists of four teams that represent the core governance team. Governments of individual countries in the world represent the national level. Various organizations in multidisciplinary environments such as the WHO, the United Nations, the European Union and the International Telecommunication Union (ITU) are some examples of the representation of global organizations. Industry experts can be in various industries such as healthcare, financial, international law and IT. IT experts can consist of individuals to experts who are a part of major independent IT institutions such as universities and community emergency response teams (CERTS). All these teams/stakeholders need to work together to achieve goals at a global level, such as providing support to eradicate global healthcare issues such as pandemics. Agreed-on principles and policies are the vehicles to communicate organizational values across the governance structure. These principles and policies can spread over different areas of IT such as information sharing, information security, IT emergency response, business continuity and IT infrastructure maintenance. The core team is responsible for providing directions within agreed-on laws and regulations for all activities such as sharing information and mitigating IT risk at the global level.

IT strategies will be reformulated from time to time according to changing goals. Relevant IT services are developed to support the strategies and goals of the governance process. Members of society across the globe are stakeholders of the IT governance mechanism. Leadership rests with the core governance team.

IT Governance Processes

Some national-level strategies and objectives can be relevant at a global level, while some are only relevant at a national level. For example, IT initiatives to support eradicating the pandemic are a shareable objective. Leadership and organizational structures are vital to the success of the whole exercise.[11] When the pandemic started, several organizations started working together. WHO started working with ITU to send text messages to people to help protect them from COVID-19. WHO is expecting "these text messages to reach billions of people that aren't able to connect to the Internet for information."[12]

Policies of IT governance processes may vary from the national level to the global level. For example, some policies related to information sharing,

Enjoying this article?

- Read *COBIT® 2019 Framework: Introduction and Methodology. www.isaca.org/cobit*
- Learn more about, discuss and collaborate on COBIT® and frameworks in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

security and confidentiality may be specific to the national level and some may be valid at a global level. However, it is essential to have valid and binding (sharable and non-sharable) policies able to work with all stakeholders at the global level. Stakeholders may act locally and globally with assigned roles and responsibilities.

Risk related to information and technology should be well balanced, optimized and managed in applying IT in this process.[13] Information security, disaster recovery and business continuity are indispensable processes in this mechanism.[14] The risk of cyberattacks and inadequately implemented BCP can be considered as high risk. The risk can be minimized by implementing necessary security policies, training employees on security principles, and applying, detecting and immunizing tools. There have been recent disturbances because of inadequate capacities of communication networks and some information security threats. One such critical infrastructure that needs to be available at all times is the Internet. Infrastructure, applications, services, skills and competency are essential to run the mechanism.

Sharing information is vital to control the spread of a virus and find a solution to end a pandemic. Many institutions around the world hold information related to COVID-19 and similar epidemics. Sharing that information for research on the life cycle of the virus including origin, symptoms and manner of spreading are essential to dealing effectively with a pandemic. The use of innovative technology such as artificial intelligence (AI) and big data analysis techniques on shared information can be effectively used to eradicate the pandemic.

Compliance with applicable laws, regulations and standards, and contractual agreements is another essential aspect in governing IT at both the national and global levels.[15] There are many mobile applications that are used for gathering personal information. There are social implications and risk related to the privacy and security of personal information gathering during the pandemic. Personal information should be used only for the purpose for which it has been obtained. Enforcement of proper information security laws and rules can minimize undesirable activities.

> "A WIDER DISCUSSION AMONG GOVERNMENTS OF INDIVIDUAL COUNTRIES IS ESSENTIAL TO ESTABLISH THE NEED FOR IT GOVERNANCE AT A GLOBAL LEVEL."

Conclusion

Now is the time to redefine and enhance the IT governance process to consolidate and integrate all required IT skills, expertise and necessary stakeholders to perform IT activities with necessary binding legal and ethical parameters to effectively deal with present and future global health and economic crisis situations. A wider discussion among governments of individual countries is essential to establish the need for IT governance at a global level. It may be possible to initiate action through existing organizations such as the Commonwealth of Nations, the European Union and the G20. The representatives included in the IT governance structure (**figure 1**) can be identified when the need is established. Objectives may change according to the criticality of global needs such as pandemics, natural disasters and threats to global society. Strategies can be formulated to deal with the objectives when principles, policies and processes are defined. Establishing governing laws and regulations, information sharing, information security, BCP and IT infrastructure risk mitigation are some of the vital areas to consider in a scenario such as a pandemic. The most important need is the commitment and contribution from all countries and stakeholders to actualize an IT governance process at a global level.

Endnotes

1 World Health Organization, "2019-nCoV Outbreak Is an Emergency of International Concern," Switzerland, 31 January 2020, *www.euro.who.int/en/health-topics/health-emergencies/international-health-regulations/news/news/2020/2/2019-ncov-outbreak-is-an-emergency-of-international-concern*

2 World Health Organization, "Coronavirus Disease (COVID-2019) Situation Report 105," 4 May 2020, *https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200504-covid-19-sitrep-105.pdf?sfvrsn=4cdda8af_2*

3 World Health Organization, "WHO Reports Fivefold Increase in Cyber Attacks, Urges Vigilance," Switzerland, 23 April 2020, *https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance*

4 Datta, A.; "Data Privacy Worries as Govts Collect Location Data to Track Coronavirus Spread," Geospatial World, 25 March 2020, *https://www.geospatialworld.net/blogs/data-privacy-worries-as-govts-collect-location-data-to-track-coronavirus-spread/*

5 McConnell, P.; "Planning for a Pandemic: Is Your Business Prepared?" BCS, 25 February 2020, *https://www.bcs.org/content-hub/planning-for-a-pandemic-is-your-business-prepared/*

6 Lainhart IV, J. W.; Z. Fu; C. M. Ballister; "Holistic IT Governance, Risk Management, Security and Privacy: Needed for Effective Implementation and Continuous Improvement," *ISACA® Journal*, vol. 5, 2016, *https://www.isaca.org/archives*

7 Lankton, N.; J. Price; "Board Investment With IT Governance," *ISACA Now,* 25 April 2016, *https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2016/board-involvement-with-it-governance*

8 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 38500, *Information Technology—Governance of IT for the Organization*, Switzerland, 2015, *https://www.iso.org/standard/62816.html*

9 ISACA, *COBIT® 2019: Framework: Governance and Management Objectives*, USA, 2018, *https://www.isaca.org/resources/cobit*

10 *Ibid.*

11 *Op cit* Lankton and Price

12 World Health Organization, "ITU-WHO Joint Statement: Unleashing Information Technology to Defeat COVID-19," Switzerland, 20 April 2020, *https://www.who.int/news-room/detail/20-04-2020-itu-who-joint-statement-unleashing-information-technology-to-defeat-covid-19*

13 *Op cit* ISACA 2018

14 *Ibid.*

15 *Ibid.*