International Journal of Innovation and Research in Educational Sciences
Volume 7, Issue 4, ISSN (Online) : 2349–5219

Managing Risks of E-learning During COVID-19

Fouzia Shersad [1*] and Sabeena Salam [2]
[1] Dubai Medical College, Dubai, United Arab Emirates.
[2] Dubai Pharmacy College, Dubai, United Arab Emirates.
*Corresponding author email id: fouzia@dmcg.edu

Date of publication (dd/mm/yyyy): 04/09/2020

***Abstract* – During the unprecedented times of COVID-19 pandemic, globally all education providers have been subjected to a major shift to e-learning mode of study. This paper aims at structuring multiple facets of e-learning risks in a way that will be feasible for educators and education administrators to assess and plan countermeasures. We have superimposed the stakeholders of Wagner, different classifications of risk from the review of literature and the specific conditions posed by the COVID-19 pandemic. The outcome is a framework where the risks of e-learning are exemplified under two dimensions - general risks and specific stakeholders' risks. General risks are applicable to all stakeholders and are broadly classified under Non-availability, Illegitimate use /Theft, Integrity violation, Privacy violation, Deliberate attacks and Unintended/Natural threats. At the specific stakeholders' level, the way in which the general risks affect each stakeholder group are categorized as content developers' Risk, Instructors' Risk, Institutions' Risk, Administrative officers' Risk, System Developers' Risk, Students' Risk, Employers' Risk and Accreditation bodies' Risk. We proposed a framework of risk analysis in two different dimensions - the general risks faced by any e-learning program and the risks faced at each stakeholder level. New areas of risks specific for the COVID-19 situation were identified as the lack of readiness, unexpected overload on all stakeholders and increased risks of security breaches which could lead to damaged reputation and reduced enrollment. In addition, the sudden online shift of examinations, lack of practical skills, poor attendance due to excessive internet traffic, lack of student engagement, uncertainty of regulations and increasing cybercrimes can have a negative impact on credibility and validity of the learning. The mitigation measures are similar to non-Covid times except that there is more emphasis on training, motivation and additional awareness campaigns.**

***Keywords* – Risk Management, Cybersecurity in Education, Security System, Higher Education.**

I. INTRODUCTION

In 2020, COVID-19 has ushered in its own share of risks, due to the sudden onset of the unprecedented lockdowns and shift of education to the online arena. As educational institutions were taken by surprise at the enormity of change, risks associated with e-learning assumed greater significance. Rising cyber dependency has been quoted as the second highest risk factor in higher education in the Global Risk Perception Survey by the World Economic Forum 2020; the risks classified in the technological categories include breakdown, cyber-attacks and data fraud [1]. While the concept of e-learning has been increasingly adopted over the last three decades, e-learning became universally mandatory in 2020, due to the requirement of distancing dictated by the COVID-19 pandemic. The importance of readiness and motivation for e-learning was reported a decade ago [2] but their impact on e-learning in the current situation have escalated by several notches.

Due to the restrictions imposed by the COVID-19 pandemic, regulating bodies have set guidelines for a risk-based approach to education to protect the beneficiaries who are the students, faculty and other stakeholders. Even so, literature on e-learning risks is scarce, though e-learning relies heavily upon risk-prone internet applications. The few published papers on data security of e-learning rely on circumstances where the participation in e-learning is optional and exemplified that documentation of systematic measures to avoid risks have to be undertaken [3] [4] [5]. During COVID-19, the previously identified risks which tamper with

confidentiality, integrity and availability have emerged with force. We find that many elements of risks are different due to the mandatory nature of the shift to e-learning. For example, a relative lack of readiness of the participants posed additional challenges as universities scrambled to protect their data and resources. The escalation of cyber-crime risks in higher education is a 'global peril' which will be disastrous as it would lead to reduction of international students if not addressed immediately [5].

Educationists lack the much-needed competencies of risk management such as identification of the threats to intellectual property rights, which is as daunting as its mitigation strategies. It is important for universities to react and adapt according to the needs of technological advances. It has been well documented that risk management should incorporate the entire organization including all its parts and all levels to avoid detrimental impact on enrolment and reputation of education institutions [6]. The importance of risk assessment has elucidated that e-learning risk management gives a competitive advantage due to uninterrupted innovation and productivity in higher education institutions [7].

A 2018 report by Deloitte notes that breaches in e-learning security is a natural evolution of digitization and therefore should be top priority as it has been on top of the list quoted by leaders in this field such as EDUCAUSE [8]. This study is particularly relevant at this time as every governing authority across the globe has been requiring Higher Education Institutions (HEIs) to churn out new strategies to cope with the compromise of physical proximity. Distance education administrators face a steep learning curve as they have to quickly adapt into the realm of virtual reality. Additionally, increase in cyber threats and fraudulent activities raise strident concerns about the extent to which academia is geared to face the online surge. This study aims to provide a framework for a concise yet robust risk assessment and mitigation process that is required during mass-scale enforced distance learning instituted in higher education institutions.

II. Literature Review and Theoretical Foundation

Right from 2005, scholars in cyber security have classified operational risks into internal and external risks. Internal risks arise from people, process and system, while external risks arise from regulatory, political or fraudulent activities [9], [10]. Kritzinger has put forward four pillars of security measures as information security governance, policy formulation, countermeasure implementation and monitoring of these measures [11].

A. *Major Threats of E-Learning Prior to 2019*

A study by Alwi in 2010 has elucidated the serious risks as deliberate attacks, technical failures, human errors, theft, compromise of intellectual property, obsolescence and extortion [2]. A very useful list of different types of risks and the effects on the participants with remedies to be taken in an e-learning system have been provided by Barik and Karforma [12]. In 2017, Muqtadiroh has identified 24 risk factors related to delivery and support namely inability to install software at schools, non-usability of (inaccessible) features, resistance by users, non-compliance and non-attendance in training sessions [3].

B. *Risks of E-Learning Stakeholders*

In 2010, B Singh classified major threats which can affect the different players in an e-learning platform and has been endorsed by several researchers [13]. When we look at the risks faced by each participant, whether it is

the facilitator or the beneficiary of the electronic learning system, risk assessment and management are of utmost importance at every level. The key stakeholders have been identified as student, instructor, institution, content provider, technology provider, accreditation body and employer [14].

C. *Security Measures for Mitigation*

In order to mitigate these risks, several solutions have been recommended by researchers. For example, Alwi and Fan have proposed an Information Security Management (ISM) system. ISM includes policies, process, organizational structures, software and hardware viz. access controls, communication system, risk management and business continuity planning; policy, standards and organisation; computer architecture and system security; law, investigation and ethics; application program security; cryptography, operation security and physical security. These measures have to balance security with convenience and productivity [2]. They suggest that though the cost can be frayed by moving into a cloud-based platform and avoiding third party vendors might reduce the entry points. Experts recommend the use of new age tools for business continuity, security and crisis communication to help institutions maintain cyber-resilience [8]. The need for authentication, encryption, access control, managing users and their permissions have been purported as an essential security elements required in the e-learning environment [17].

D. *Major Threats of E-Learning Impacted by COVID-19*

A publication by QS rankings report that the major changes caused by COVID-19 lockdown has not been accepted by all students as 43% stated that they were not interested in online studying as it imposes greater demands on them [15]. Interaction related risks, highlighted in another study conducted at Eastern Mediterranean university, underpins the essentiality of such assessment and mitigation measures [4]. Another scholar vouches for the need of risk assessment as the degree of uncertainties and risks are very high and therefore, proper and systematic planning and designs for risk management are essential [3]. The risks of interruptions, malware, academic integrity issues and abusive communications are enormous while the complexity of security systems have escalated [16] particularly due to the sudden increase in number of students and programs using e-learning.

We identified a huge gap in the risks of e-learning reported in literature with the actual risks faced by HEIs during the large-scale shift with no time for preparation due to COVID-19. Many of these gaps are due to the mandatory nature of the shift to e-learning. The mitigation strategies for ISM remains relevant with the addition of more efforts towards acceptance and motivation by participants are required in the current situation of COVID-19 pandemic. The identified gaps are summarized below:

- Lack of readiness of administrators, instructors and students.
- Financial burden on educational institutions due to withdrawals and increased student debts.
- Barriers imposed by the infection control such as reduced access to important files and absence of crucial staff who are sick/quarantined.
- Poor availability and connectivity during peak times due to unprecedented internet traffic as the entire schooling system shifted to e-learning.
- Tendency to use poorly secured sites out of desperation to fulfill the requirements of the course and its deli-

-very.

- Sudden overload and adaptation to distance mode of work leads to increase in human errors, which may lead to breach of confidentiality or privacy.
- Risk of the credibility and validity of highly valuable degrees being questioned.
- Skills gap due to lack of practical skills puts employers at risk of getting low skilled employees.
- Sudden shift of examinations on a large scale to online mode and software increased the risks of security breaches.
- Unexpected overload on faculty could increase human errors with legal, intellectual property, and privacy lapses.
- Ambiguity of rules and regulations leads to damage to reputation.
- The unprecedented increase in the use of digital platforms led to increase in cyber attacks.

III. PROPOSED FRAMEWORK

Based on the review of literature and the identified gaps which will be particularly useful during the COVID-19 pandemic, we have attempted to create a framework (Figure 1) which includes multiple facets of an educational institution. In order to help educators and education administrators to analyze the risks holistically, we have superimposed the stakeholders of Wagner, and different classifications of risk from the review of literature noted above. According to this framework, which can be easy for educators to document, the risks of e-learning can be classified under two dimensions - general risks and specific stakeholders' risks (Figure 1).

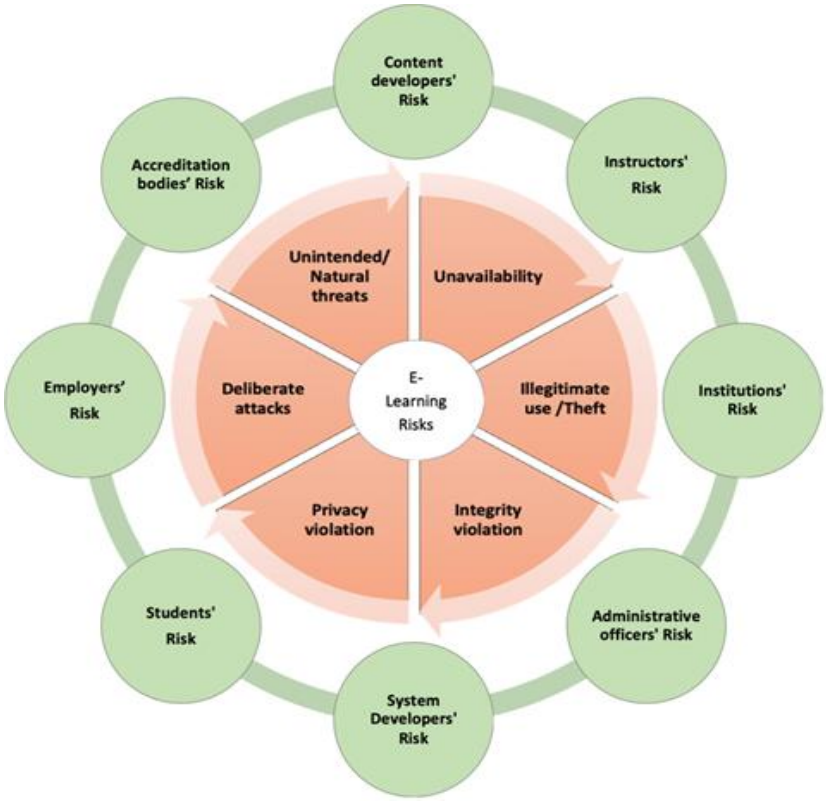

Fig. 1. Framework of two dimensions of E-Learning risks- general risks and stakeholder risks.

A. *General Risks*

General risks are applicable to all stakeholders and therefore are applicable for all users and administrators (Table 1). General risks are broadly classified under Non-availability, Illegitimate use /Theft, Integrity violation, Privacy violation, Deliberate attacks and Unintended/Natural threats.

Table 1. General Risks, Description and Countermeasures.

	General Risks	Description	Countermeasures
1.	**Availability** a. Internet Traffic (specific for COVID-19) b. Loss of data processing capability	- Loss of accessibility at any time and place. - Poor connectivity at peak times due to overuse of communication channels. - Quality of hardware and infrastructure	- High speed internet connection. - Well-paced live sessions avoid internet peak-time. - Internet speed guidelines for participants - Back-up platforms. - High quality of hardware components e.g. server, high bandwidth internet, high quality LMS and infrastructure capable of sustaining multiple users and networked applications.
2.	**Illegitimate use /Theft**	- Illegally accessing E-Learning information stealing intellectual property.	- Access control using a multiple-tiered security network and Firewall. - Clear Policy for use of shared materials. - Updated operating system with security patches and service packs. - Password protection and guidelines to administrators.
3.	**Accuracy/Integrity**	- Illegal access with obstruction of activities of legitimate user's protection of data from unauthorized changes, both intentional and accidental. - Integrity depends on access control by robust mechanisms to confirm unique identity of all persons who attempt access.	- Firewall, File storage & Data recovery system. - System administrators with knowledge and skills to implement firewall & troubleshoot firewalls.
4.	**Privacy/ Confidentiality**	- Illegitimate use of another user's electronic resource protection of one's private information from unauthorised persons leakage of sensitive information.	- Advanced level of access control. - High level of data security with encryption.
5.	**Deliberate attacks**		
	a. Repudiation	- Students may deny acceptance of information or disagree to participate in any transaction of documents.	- Student training to motivate participation. - Monitor activities of students on the LMS. - Counseling of students who are having less participation
	b. Masquerade	- Hackers, masqueraders, unauthorized user activity, unprotected downloaded files, local area networks (LANs), and	- Maximize use of internal LMS and servers - Restrict the use of external public platforms.

	General Risks	Description	Countermeasures
		Trojan horses.	- Effective Firewall & System security. - Warn the staff about the cyber security and password protection.
	c. Malicious program	- Intruders using malicious codes	- Appropriate protective equipment. - Antivirus and firewalls. - Endpoint Security software updated regularly with auto-scanning and filters.
	d. Brute-force attack	- Attack by miscreants using different modalities to breach security.	- Create awareness among staff and students to protect themselves against Phishing and hacking. - Password protection guidelines and secure internet and email policy. - Filters and Physical security to protect vulnerable data contingency & IT equipment. - Pre-validation of data entry into the network. - Fault tolerance system; Efficient back up system.
6.	**Unintended/ Unavoidable**	- Natural disasters. - Unavoidable threats like Computer bug, power outage, handling error etc.	- Efficient back up system and document management system. - Adequate Physical protection - Insurance.

Adapted from Alwi & Fan, 2010 [2], Barik & Karforma, 2012 [12], Muqtadiroh et al., 2017 [3], Ilkan et al, 2017 [4], Schroeder, 2019 [16].

B. *Specific Stakeholders' Risk*

Specific stakeholders' risks are applicable to internal key stakeholders, for instance; course content developers, teachers, institution, system developers and importantly end-users viz. the students and employers (Table 2). It can be classified based on the proposed framework delineated (in Figure1) as Content developers' Risk, Instructors' Risk, Institutions' Risk, Administrative officers' Risk, System Developers' Risk, Students' Risk, Employers' Risk and Accreditation bodies' Risk.

Table 2. Stakeholder's risks of E-learning.

	Stakeholders' Risks	Description	Countermeasures
1.	**Content developer's risk**	Faculty members who prepare their own content have authorship rights over the content. **a. Teaching content** could be passed on and processed without the authors' knowledge. **b. Hackers** may modify/destroy content like lecture notes, class test papers, home assignments etc.	- Educate content developer and instructors on responsibilities. - Involve educational technologists in the content developing process - Install access controls & encryption. - Electronic Watermarking of lecture notes. - Regular data backup. - Create plan of action in case of a breakdown of certain

	Stakeholders' Risks	Description	Countermeasures
			components (e.g. hard disk, network connections). - Use of secure sites only so that Students receive the content unaltered and that the users can check the integrity of the text.
2.	**Instructor's risk** .	Instructors are responsible for providing support to students in academics. **a. Content Delivery:** Risks in events such as delivering lecture, sending notes and assignments, accepting and marking answer sheets, preparing and distributing mark sheets. **b. Privacy:** Digitally stored data of Student and faculty contributions. **c. Content of examinations:** Standardization of examination questions may restrict the academic freedom of individual teachers. **d. Conduct of examinations:** Risk of cheating, non-availability and non-repudiation or altered question papers of examinations & impersonation.	- Instructors should keep another platform as back up. - Risk for the privacy to digitally stored data of student and faculty contributions to a discussion. - Discussion forum data needs robust security mechanism and encryption of data. - Avoid deviations from the existing plans used in face to face examinations. - Use of examination software can eliminate restrictions by providing wide range of formats. - Proctoring tools and Lockdown browsers. - Effective guidelines and monitoring. - Improve student communication and support to gain acceptance. - Perform mock exams before the final exams. - Increase security by strong passwords. - Robust security mechanisms.
3.	**Institution's Risk**	**a. Lack of readiness,** non-compliance and lack of skills of leadership and participants could be a major threat specific for COVID-19. **b. Financial risk** specific for COVID-19 due to withdrawal and reduced paying capacity of students. **c. Ambiguity in rules** laid down by authorities specific for COVID-19. **d. Legal aspects** specific for COVID-19**:** Faculty members, students & staff tend to neglect legal aspects. **e. Natural threats** may be by natural disasters like fire, storm, earthquake, floods etc. (See Table 1 point 6)	- Training and support to faculty, students, administrative staff. - Communication with all stakeholders. - Ensure that the employers are informed of the credibility of the teaching methods in transcripts. - Reduced enrolment. - Student financial debt and withdrawals. - Employee benefits. - Legal threats are because faculty and students are motivated to ignore legal restrictions as they are usually more interested in academic field. e.g. copyright, sending official documents etc. - Conduct awareness sessions on professional use of citations for faculty, staff and students.
4.	**Administrative officer's Risk**	**a. Adaptation** for distance work and increased workload due to COVID-19. **b. Lack of Access to documents** for Training, Processing and documentation due to Interruption to	- Efficient administrative software and information systems. - Distribute responsibilities for maintaining passwords of all servers and routers .

	Stakeholders' Risks	Description	Countermeasures
		power supply to the server and other network devices. **c. Communication failure** due to Virus through disruption to email, Remote access, LAN, WAN damages.	- Enhance authorization of access multimedia databases of E-Learning materials. - Adequate protection for uninterrupted power supply for server and for faculty who conduct virtual classes in college. - Antivirus updated and maintained. - Enhance safety measures and Physical security of the building. - Maintain adequate back up and IT personnel to trouble shoot.
5.	**System Developer's risk**	**a. All general risks** have to be predicted, prevented and mitigated (specific for COVID-19). **b. Leaking of confidential material:** An intelligent learner may be able to access the source code of the script and get access of the password of the databases. **c. Attackers** may change/steal users' password.	- High quality of hardware components and infrastructure. - Hardware components such as high ended web server & database server, high bandwidth internet leased line and a quality LMS. - Robust infrastructure capable of sustaining multiple users and networked applications. - System developer must be aware of SQL injection, Cross-site scripting (XSS) attacks to maintain multimedia database. - Instruct faculty and staff to avoid storing passwords in clear text in the application code. - Increase password security.
6.	**Student's risk**	**a. Intruders** could edit the question papers or other important documents. **b. Lack of acceptance** of online learning. **c.** Students' **lack of skills** to engage in online learning. **d. Misinterpretation** of what was meant on electronic platform. **e. Phishing** by fake web sites which look like a real E-Learning website to steal confidential information.	- All students must be aware of misuse of log-in information, otherwise attacker may attempt to prevent authorized learner from accessing the e-learning server. - Counseling and motivation. - Train students to work independently without the assistance of teachers. - Improve writing and communication skills through e-learning devices. - Awareness of phishing: They should be trained never to provide confidential information.
7.	**Employers' Risk**	a. Employees with **poor skill-sets.** b. Validation of **credentials.**	- Collaborate with e-learning institutions. - Pre-appointment Competency testing.
8.	**Accreditation bodies' risk**	**a. Credibility and validity** of the degree programs offered.	- Clear guidelines and regulations to ensure validity. - Continuous monitoring and inspection for institutions.

Adapted from Alwi & Fan, 2010[2], Barik & Karforma, 2012[12], Wagner et al, 2008 [14], Jorion, 2007 [9], Patomviriyavong, 2006[10] Syed et al, 2020 [18]

C. *Key Role of Faculty in COVID-19 Specific Risks*

Building competencies of cyber-risk management among faculty members is of prime importance to safeguard intellectual property, accuracy of teaching content, content delivery, confidentiality, password security, privacy, examination security, disruptions and integrity (Table 2). Faculty members serve as content-developers and instructors, and at the same time can positively influence students to accept safe practices. Several countermeasures to overcome student risks are strict adherence to protocols for back-up, confidentiality, use of secure sites, improved communication with students and increased security with strong passwords. If faculty members are adequately trained to identify risks and take countermeasures, this will help the other stakeholders to prevent damage to reputation.

IV. DISCUSSION

The relevance of a such a framework implies that systematic planning is crucial to mitigate risks [3]. In 2014, Dimitrijevic proposed that a framework for risk assessment is needed for higher education institutions as it is a very sensitive area which needs expertise; their proposed framework is based on working processes, assets which are at risk, and mitigation measures [6]. Expanding on this study, the risks exclusive to e-learning have been laid out by our framework (Figure 1) in a single diagram showing two dimensions. The more elaborate description in the tabular form (Table1 and Table 2) is anticipated to be a guide for educationists who are struggling to ensure security for the mass-scale conversion of education to the online mode. For instance, it has been noted that operational risks can be due to faculty inexperience in eLearning, resistance to change or poor system performance [18]. This may be mitigated by involving educational technologists who will embed safe practices. Moreover, many researchers had mentioned that use of third party vendors should be curbed, but this was ignored due to the urgency dictated by the onset of COVID-19 pandemic [2]. It has been clearly shown that universities have to invest time and resources to ensure that faculty members, system administrators, educational technologists and other support staff are adequately trained and equipped to perform risk assessment and manage them systematically. Being front-liners in the Teaching-Learning-Assessment process, faculty members are strongly positioned to counter student risks such as lack of acceptance of online learning, students' lack of skills and misinterpretation (Table 2).

The framework (Figure 1) takes into account the internal and external risks and further classifies the risks at two dimensions for each stakeholder and general risks including regulatory, political or intentional activities [9], [10], [17]. The four pillars of security measures suggested by Kritzinger have been exemplified at each level [11] with additional input from COVID-19 related risks. The major threats for each player elucidated by B. Singh and levels of risks and their countermeasures classified by other researchers have been successfully incorporated in our proposed framework [13] [2] [12] [3].

One of the components in our framework is on student acceptance and is aligned with the report on student perception reported by QS ranking [15]. The risks caused by sudden increase in e-learning which pose a threat to confidentiality, availability and integrity have been incorporated [16]. The mitigation measures to preserve interaction related risks have been classified for each stakeholder level [4]. The recommended measures for mitigation in the information security systems are carefully recommended so that security measures do not hinder productivity and autonomy [2].

The unprecedented increase in the use of digital platforms due to restrictions imposed by COVID-19 has led to the need for energetic countermeasures using several strategies (Table 1 and Table 2). This study shows that universities have to invest time and resources to build competencies among faculty members to assess and mitigate risks in their day-to day activities and then embed them in the processes used for e-learning.

V. CONCLUSION AND LIMITATIONS

We proposed a framework of risk analysis in two different dimensions - the general risks faced by any e-learning program and the risks faced at each stakeholder level. New areas of risks specific for the COVID-19 situation were identified as the lack of readiness, unexpected overload on all stakeholders and increased risks of security breaches which could lead to damaged reputation and reduced enrollment. In addition, the sudden online shift of examinations, lack of practical skills, poor attendance due to excessive internet traffic, lack of student engagement, uncertainty of regulations and increasing cybercrimes can have a negative impact on credibility and validity of the learning. The mitigation measures are similar to non-Covid times except that there is more emphasis on training, motivation and additional awareness campaigns.

The main steps to be taken by institutions are to increase training and support of faculty, staff and students. Clear communication of policies and regulations and collaboration with employers and community partners will help to ensure credibility and validity of degrees. A great proportion of countermeasures specific to COVID-19 pandemic requires a well-informed faculty about the perils and countermeasures for managing risks of e-learning. Ensuring access security and availability at the same time poses a challenge. Adequate investment in software, competent human resources and infrastructure is essential to provide a secure platform to ensure reliable access and to protect against human errors and privacy lapses.

Our study is limited to the risks of E-learning during a pandemic which necessitated a sudden and mandatory move to distant learning mode. The mechanism of grading of risk using probability and importance is beyond the scope of this paper.

REFERENCES

[1] E.G. Franco, “The Global Risks Report 2020,” World Economic Forum, Geneva, Switzerland, Insight Report 15th Edition, 2020. Accessed: Aug. 16, 2020. [Online]. Available: https://www.weforum.org/reports/the-global-risks-report-2020/.
[2] N.H.M. Alwi and I.-S. Fan, “E-learning and information security management,” Int. J. Digit. Soc. IJDS, vol. 1, no. 2, pp. 148–156, 2010.
[3] F.A. Muqtadiroh, E.W.T. Darmaningrat, and R.N. Savira, “Risk assessment and risk mitigation of E-Learning Implementation in the middle school using failure modes and effects analysis (FMEA),” Semin. Nas. Teknol. Inf. Komun. Dan Ind., vol. 0, no. 0, Art. no. 0, May 2017.
[4] M. Ilkan, M. Beheshti, M. Behendish, E. Atalar, and M. Ilkan, “Managing interaction related risks on the development of E-Learning it Projects: A Case Study of a Language Institute E-Learning Platform Design in Iran,” vol. 5, no. 2, p. 9, 2017.
[5] J. Demchak, “Global risks abound for higher education institutions,” https://www.marsh.com, Aug. 22, 2019. https://www.marsh.com/us/insights/risk-in-context/global-risks-higher-education.html (accessed Jun. 20, 2020).
[6] L. Ruzic-Dimitrijević and J. Dakić, “The Risk Management at Higher Education Institutions,” Online J. Appl. Knowl. Manag., vol. 2, no. 1, p. 16, 2014.
[7] M.J. de Bozinoff, M. Tankosic, Megatrend, 19000 Zajecar, and G. Delceva, “E-Learning risks Management as Competitive Advantage in Institutions of Higher Education,” 2014.
[8] Deloitte, “significant risk in higher education - Google Search,” 2018. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-top-risks-higher-education.pdf (accessed Jun. 20, 2020).
[9] P. Jorion, Financial risk manager handbook, vol. 406. John Wiley & Sons, 2007.
[10] S. Patomviriyavong, B. Samphanwattanachai, and T. Suwannoi, “E-Learning operational risk assessment and management: A case study of the M. Sc in Management Program,” Int. J. Comput. Internet Manag., vol. 14, pp. 44–1, 2006.
[11] E. Kritzinger and S. H. Von Solms, “E-learning: Incorporating information security governance.,” Issues Informing Sci. Inf. Technol., vol. 3, 2006.
[12] N. Barik and S. Karforma, “Risks and remedies in e-learning system,” ArXiv12052711 Cs, Feb. 2012, Accessed: Jul. 24, 2020. [Online]. Available: http://arxiv.org/abs/1205.2711.
[13] B. Singh, “Network security and management,” in 2010 IEEE International Conference on Computational Intelligence and Computing Research, 2010, pp. 1–6.

[14] N. Wagner, K. Hassanein, and M. Head, "Who is responsible for E-Learning Success in Higher Education? A Stakeholders' Analysis," J. Educ. Technol. Soc., vol. 11, no. 3, pp. 26–36, 2008.
[15] S. Linney, "How Universities are embracing online learning during the Coronavirus Outbreak," QS, Mar. 26, 2020. https://www.qs.com/how-universities-are-embracing-online-learning-during-the-coronavirus-outbreak/ (accessed Jun. 20, 2020).
[16] R. Schroeder, "Identifying and mitigating the most important risks in online learning (opinion) | Inside Higher Ed," Inside Higher Ed, Mar. 20, 2019. https://www.insidehighered.com/digital-learning/blogs/online-trending-now/identifying-and-mitigating-most-important-risks-online (accessed Jun. 20, 2020).
[17] J. Iacob, "Information security management in E-Learning," Knowl. Horiz., vol. 5, no. 2, pp. 55–59, 2013.
[18] A.M. Syed, S. Ahmad, A. Alaraifi, and W. Rafi, "Identification of operational risks impeding the implementation of E-Learning in higher education system," Educ. Inf. Technol., Jul. 2020, doi: 10.1007/s10639-020-10281-6.

AUTHOR'S PROFILE

First Author
Fouzia Shersad is FRCP (Glasg.), FAIMER fellow and PhD (medical education). She is currently Director of Institutional Effectiveness and Associate Professor at Dubai Medical College, Dubai. She is certified in EFQM as senior assessor of Dubai Quality Award. She served as project leader of Annual Dubai Medical Education Symposium for 10 years and led the college to win the DQA and MRM Excellence Awards. Her research interests include, quality in medical education, program evaluation, professionalism and student assessment.

Second Author
Sabeena Salam (B.Ed, CELTA, MA, MPhil- English Literature and Linguistics). With over two decades of experience, currently she heads the institutional effectiveness of Dubai Pharmacy College and Faculty of general education require--ments. Her area of principal interest is teaching, learning and assessment with a recent emphasis on transitions from 'Quality' to 'Qualification Frameworks.' This led to inclusion in the Member Directory issue of NQA Qualifications Frameworks and Systems Community (NQA-QFSC) UAE, December 2016. For the past years, she has been actively involved in Collaborative Action Research (CAR). Her interests are strategic planning, organizational and program effectiveness, and curriculum design.