IS CONTROL

Student Name

Institute Name

**Contents**

[Introduction 3](#_Toc4365622)

[Literature review 3](#_Toc4365623)

[Threat mitigation technique 5](#_Toc4365624)

[General and application management controls with examples 6](#_Toc4365625)

[Security technique to achieve CIA 8](#_Toc4365626)

[Audit process 9](#_Toc4365627)

[Summery 9](#_Toc4365628)

[Reference 11](#_Toc4365629)

# **Introduction**

IS control being a procedure done to make sure that the set of standards as well as objectives of the functionality can be found in both real as well as being met. The education industry, quality control is a crucial challenge, as students, parents and teachers want to make sure that the students are getting right kind of training. There are so many methodologies of quality control and IS control in education industry, consisting standard level of testing, reviewing the teaching process along with right training (Bastid, 2017).

Education organization network constantly be ideal playground for number of cybercriminals. Since this is the time and interests of the so many educational consumers, such networks will tend to consist of some cutting-edge technologies along with diverse strategies. Also, students that tend to work hard against any kind of network limitations, looking for some kind of workaround to get data as well as applications that current IT administrators can be limited (Brauer, 2016). For this, an unequal number of consumers initiate cutting their teeth on facts that they are hacking.

# **Literature review**

Following is the detailed discussion:

* Frequency or intensity of cyberattacks: as a part of the largest cyber issues that face the education industry is with rising number of cyber attacks that have a goal to grab personal data, extort information for the sake of money or completely disrupting abilities of schools to function (Dalton, 2017). In the current time, schools are constantly targeting with three kinds of cyberattacks discussed below: -
	+ Phishing: this is the process where emails are sent out that seems like coming from trustworthy websites or comes with figures based on authority that attempt to get different kind of recipient in order to send personal as well as financial data (Bryson, 2018). The recent instances consist of cybercriminal pose as companies for student loan and officials also claims to require the W-2 tax data of workforces.
	+ DDoS: there are concepts like distributed denial of various services-based attacks are utilised to halt the operations by completely filling a bandwidth of school with so many requests, cause the system to completely crash or slow down, this is why keep students and faculty from getting the network. School have also raised the digital based offers as well as students are highly dependent on various connected machines, attacks from DDoS have the capacity to hinder all features every type of educational institute (Drahos and Braithwaite, 2017).
	+ Ransomware: education is the industry which is the soft target of ransomware. At the same time, six percent of government institutes have part of the target by ransomware as well as three percent healthcare people, thirteen percent of education organization have been experiencing ransomware attacks. This is a kind of malware that can be encrypted the files till the time a ransom has been provided (Fukuyama, 2017).
* Restricted IT-based resources: other kind cybersecurity issues schools usually face when saving the network from any kind of attacks is considered as a lack of varied IT resources. The present cybersecurity skill set hap actually means that there is immense shortage of present professional that are highly equipped to address that there is threat faced by landscape of the school. It is actually not possible at all for the restricted IT resources as well as personally at organization to supervise all the device as well as request for any kind of network (Hatch, 2018).
* Lack of Cyber aware culture: schools and other education institute are mainly lacking the basic awareness that is required by everyone who are at consuming end of technologies.

# **Threat mitigation technique**

Following are the threat mitigating techniques: -

* Use of technology in education will just continue to develop and this way, the attack can surface that makes the school premises highly vulnerable. In other to make sure technology using as well as the innovation further it gives without any kind of compromise any kind of safety, educational institute should be highly aware of as well as strategize so that it can be mitigated in a right manner (Hayhoe and Bastid, 2017).
* Therefore, more and more machines need to get the network, to carry application with changing degrees of safety and digital change moves infrastructure as well as sources towards the cloud, teams in IT will require to get security answers that give network visibility across so many cultures mixed with automation when they have to keep the speed with cybercriminals (Kerzner and Kerzner, 2017).

Legacy IT based infrastructure is considered as another field that can keep educational institute at high risk of any kind of attack. The team of IT have to make sure that older hardware along with answers have the recent level of updates, or when they are not highly supported by the vendors, should be constantly updated with modern level equivalents. In complicated and high distributed network, but improve as well as replace different kind of programs that can mainly resource intensive (Krantz, 2018).

* Teams of IT must motivate cybersecurity environment training to form every individual who can be connected with the network aware of cyber challenges, mainly phishing as well as ransomware. This can motivate the consumers to actually think carefully before actually clicking on any unknown field as well as the attachment, or to completely double the evaluation the sender of any email asking for personal or account data. In addition, educational institute can educate the students as well as the staff on the significance of regular updated machineries as well as applications to make sure that they are applying for the most current security-based patches to possible insecure level of codes (McDonald and Wilson, 2016).

# **General and application management controls with examples**

Educational institution is facing distinct type of security issues that range from tight budgets, to surprising number of many BYOD machineries, to number of e-learning initiatives, Fortinet functions with education sector in order to find the right answers for their distinct digital needs. All the issues in the cybersecurity sphere is that such attacks are not restricted to educational networks. Once it is properly refined, they will soon be part of the network (Newhouse et al., 2017).

This is why, all companies, not just education culture, need high-performance, comprehensive safety offers that are designed to function at one place for easier management as well as fast response. Concepts like Fortinet solutions are actually made to let people decrease the complex behaviour and save the consumers without actually compromise the overall network performance (O'connor, 2017).

General management control can be defined as internal level of control that can be assured with safe, stable as well as trusted performance of the current computer hardware, IT personnel and software attached to the finance-based structure. The concept impacts the capacity to depend on the application controls and IT reliance on manual level of control. without any kind efficient application and general management control, dependency can never be placed on any form of application level of control or IT depending on manual level of control until added processes are actually be part of performance. Even such added processes restrict the capacity to depend on more than one kind of application control at one time (Schön, 2017).

Following are the areas that typically can be dealt as a part of such kind of controls:

* Accessing to different programs as well as data which means control that save wrong and unauthorized usage of the system all over the layers of the systems, operating structure, applications along with database. Elements like security-based policies, unique kind of IDs, authorized administrators, consumer access provisioning, consumer level of access review, firewall and physical safety are part of the whole analysis (Skopik et al., 2016).
* Changes in program may consist of needed authority of transformation level of requests, reviewing the transformations, approval, evaluation, documenting and assessing the changes on other IT elements as well as executions protocols. Change management procedure for constant as well as emergency transformations are also covered her.
* Program growth: it is important to have control on the growth-based processes, consisting designs of systems and execution, that can be outlined particular stages, need of documentation, management of change, checkpoints and approvals to completely control the growth or maintaining the projects (Starbuck, 2015). Also, control on the efficient acquisition, execution and maintaining the system software, management of database, software as a part of telecommunication, safety software as well as utilities.
* Application management control also covers software development life cycle. Operations of control over the efficient job actually configure and also scheduling, data centre functionalities, backup of data as well as recovery of data of processes.

The perfect example which can be taken here issues that the educational institute face and need of different types of control is crucial, is by studying Beaverton School District were constantly experiencing disruption right after an errant where the alarm set off for the fire level of suppression structure in the town’s data centre, harming hard devices along with various servers. As per the chief technology officer at the company all forms of systems that staff required to do the jobs (Starbuck, 2015). They were not able to utilise email or get access of class lists, schedules of students as well as textbooks on internet. The technology at the company operated for several days in order to patch as well as the repurpose structures, and in the end managing to get all structures back on internet. But the district is losing all the information that enter in one of its structure in a short amount of time right before the incident and staff had to again enter into it.

# **Security technique to achieve CIA**

**Confidentiality:** This is for the measures that needs to be ensuring about preventing the sensitive information from reaching the wrong people. Here, the access needs to be restricted for the authorisation of the different view of the data. The data needs to be categorised depending upon the damage in the unintended hands. The data confidentiality holds the special training for the privy of the documents. The training includes the security risks which can lead to threatening of information

**Integrity:** The integrity involves the consistency, accuracy and the planning of data over the time. The data must not be changed and so there is a need to take the steps so that the alteration is not by any unauthorised people, in breach of confidentiality. The additional changes could be detected through backups and the redundancies which affect the data.

**Availability:** It includes maintaining hardware, performance as needed, depending upon the functioning system. The communication bandwidth is to prevent the occurrence of Redundancy, failover and even high available clusters to mitigate any serious consequences issues that tend to occur.

# **Audit process**

The auditing is about the procedures which includes different verification, confirmation, observation and the verification processes. It includes the carrying out of procedures depending upon how the evaluation is made to judge the reliability with drawing any type of conclusion. The compliance is set with the code of conduct to find the evidence that tends to justify the opinions. Auditing includes the recognition with quality of education that helps in processing with the self-assessment and planning on the quality based standards to produce a wealth with the richer insights.

# **Summary**

In the end, there are so many methods, such network is part of canary as a part of coalmine for the sake of cybersecurity that organizations must all be paying some amount of attention to.

The team of IT is accountable for saving such environments must be at the top of the game also. All the number in various computer devices get connected to the networks, so in classrooms, office of administration, research laboratories or such bringing the students, combined with legal level of mandates to save the students and also make sure that the ware against all cyberthreats is considered something that any sector of education security professionals requires to take things in serious manner (Wilensky, 2015). However, to know where to pay attention on restricted security resources is not very easy.

# **Reference**

Bastid, M., 2017. Servitude or liberation? The introduction of foreign educational practices and systems to China from 1840 to the present. In *China's Education and the Industrialised World* (pp. 3-20). Routledge.

Brauer, R.L., 2016. *Safety and health for engineers*. John Wiley & Sons.

Bryson, J.M., 2018. *Strategic planning for public and nonprofit organizations: A guide to strengthening and sustaining organizational achievement*. John Wiley & Sons.

Dalton, M., 2017. *Men who manage: Fusions of feeling and theory in administration*. Routledge.

Drahos, P. and Braithwaite, J., 2017. *Information feudalism: Who owns the knowledge economy*. Routledge.

Fukuyama, F., 2017. *State building: Governance and world order in the 21st century*. Profile Books.

Hatch, M.J., 2018. *Organization theory: Modern, symbolic, and postmodern perspectives*. Oxford university press.

Hayhoe, R. and Bastid, M., 2017. *China's education and the industrialised world: Studies in cultural transfer*. Routledge.

Kerzner, H. and Kerzner, H.R., 2017. *Project management: a systems approach to planning, scheduling, and controlling*. John Wiley & Sons.

Krantz, J., 2018. Dilemmas of organizational change: A systems psychodynamic perspective. In *The systems psychodynamics of organizations* (pp. 133-156). Routledge.

McDonald, M. and Wilson, H., 2016. *Marketing Plans: How to prepare them, how to profit from them*. John Wiley & Sons.

Newhouse, W., Keith, S., Scribner, B. and Witte, G., 2017. National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Special Publication*, *800*, p.181.

O'connor, J., 2017. *The fiscal crisis of the state*. Routledge.

Schön, D.A., 2017. *The reflective practitioner: How professionals think in action*. Routledge.

Skopik, F., Settanni, G. and Fiedler, R., 2016. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, pp.154-176.

Starbuck, W.H., 2015. Organizations as action generators. *Available at SSRN 2708094*.

Wilensky, H.L., 2015. *Organizational intelligence: Knowledge and policy in government and industry* (Vol. 19). Quid Pro Books.