Fundamentals of Data Security

Security Risk Assessment

IISC Consulting Company Information

Unit Code : ISEC5006

Name : Syed Muhammad Ahmed Zaidi

Student ID: 20972008

Table of Contents

EXECUTIVE SUMMARY

Security risk assessment is identifying and evaluating potential vulnerabilities and threats within an organization so that decisions can be taken to mitigate such risks. It is also a recondition and a key component of risk management (Sajko, Rabuzin, and Bača 2006). This document aims to conduct this assessment for IISC Consulting, a known consulting firm offering its services to various industries, including finance, health, power, utilities, retail, consumer, government, and more. This assessment not only identifies the possible vulnerabilities and threats the organization faces but also gives recommendations to solve them and reduce the chance of such risks.

This report takes a deep dive into the workings of the particular organization to determine its current security posture that can have a negative impact on its operations, assets, clients, and reputation. It follows the guidance of NIST SP 800-30 to evaluate each element of its operations and gives out an evaluation based on the FAIR (Factor Analysis of Information Risk) method of risk assessment. Over and above, it also highlights recommendations to to address each possible risk and finds solutions to reduce the overall risk to IISC Consulting.

INTRODUCTION

In today's world of modernization and extensive use of technology, information security is essential to safe keep a company's assets. In this report, we will be considering a consulting company, IISC. This company provides services to various industries, including Finance, Health, Power, Consumers, Utilities, Retail and even Government. The clients are dispersed over a ride range from medium to large organizations, which are both private and public.

Such Organisations are responsible for handling a vast quantity of susceptible data that can be very important for the running of any organization. This ranges from proprietary information, client data, financial records, and more. IISC must ensure that they are following the right protocols for securing each element of the information so that it does not get into the hands of others who may misuse it. They must guarantee that all data is handled with objectives in mind, which include confidentiality, integrity, and availability.

To effectively safeguard all data, organizations must conduct security risk assessments to identify if there are any vulnerabilities so that they can be evaluated fully to mitigate any risks for the future. The purpose for IISC to conduct this analysis is also to find and eliminate if there are any possible risks so that they can continue to commit to excellence in information security. The objectives for this risk assessment include

- To identify and study all potential security risks and vulnerabilities that can possibly become a threat to the company's operations, its IT infrastructure and its information systems.
- It must analyze and give actionable insights that can work as recommendations for IISC to apply such security measures to improve its capability to protect vital information.
- It should align the whole organization with the security practices that are being followed globally, specifically the industry in which the company is working in.
- It should be a guide for the board and the management of IISC consulting company to make timely decisions about resource allocation, security investments, and also implementation of risk mitigation strategies.

The scope of this analysis includes a range of topics that will be discussed by this report and also those that are beyond any discussion as they will be excluded to make it more relevant towards the risk assessment. This report explicitly highlights the analysis that is completed on the major elements of data security which includes

- Information Technology Infrastructure: This incorporates the discussion about the evaluation of the security measures that are undertaken by the company, which involves its infrastructure. This comprises servers, workstations, networking equipment, and storage data systems that are being used across the locations of its offices, including Sydney (Headquarters), Canberra, Melbourne, Brisbane, Adelaide, Perth, and Hobart.
- Data Storage: This will also cover extensively how the company is managing its resources for data in order to keep data confidential. It will answer the questions about how the data is being handled, stored, and protected to provide a service that is secure. It analyzes all data security facilities, backup procedures, and data access controls to understand how effectively data is being managed.
- Network Security: This assessment also takes into account both wired and wireless network infrastructure analysis. This includes examining network configurations, firewall settings, intrusion detection systems and also what measures are being taken by IISC to protect against any unauthorized access to such facilities.
- Access Control and Authentication: Evaluation of access control mechanisms and authentification procedures are also within the scope of this assessment. It reflects the policies being implemented at each office location to compare and contrast for betterment.
- Employee Traning and Practices: An analysis of employee awareness, training, and adherence to security policies is vital for any organization to achieve its objective for data security. Hence, this assessment takes a deeper look at what IISC is doing with respect to the organizational hierarchy. It also analyzes how employees are working from remote locations and ways to authenticate their control over organizational information.

The scope of this assessment is kept relevant to the topic, and for this reason, it will not be taking into account what security practices are being followed beyond the IT infrastructure. Also, it will not examine in-depth what the vendors of IISC are doing in order to protect data. This report exclusively focuses on the practices that IISC is following alone.

RECOMMENDATIONS

Being a consultation company, IISC has to be responsible for the safekeeping of vital information for all of its clients. As of now, they are trying their best, but there are still gaps that can be categorized as being vulnerable. As a security consultant, I have noted down some susceptibilities that can be rectified to improve the overall data security handling in the organization.

- Currently, IISC's physical access controls for server rooms are not up to the mark. They use swipe cards for authentication before letting anyone into the rooms. This can be a security risk as such cards can be lost or stolen, and someone else may use it to get inside. Hence, I would recommend using physical access controls such as biometric authentication or even face recognition through retina scans. This will make sure only the authorized personnel can get in and have access.
- Continuing with the last point, we see that IISC has not fully conducted a thorough review to assess and validate user access permissions. This means that this outdated check of who has the permission to view which data can cause wrong information to go into the wrong hands. Hence, the best practice would be to conduct regular audits and see which information was accessed by whom, where, and at what time so there could be proper tracking and if anyone is found to have unauthorized access, that should be immediately rectified.
- From the case, we got to know that IISC lacks a consistent vulnerability scanning procedure and it also does not process patch management. This could mean that known and unknown vulnerabilities within the systems are not fully addressed, which may become problematic in the future. In order to solve this, IISC should schedule routine vulnerability scans to identify known and unknown gaps, and they should also do process patching on a regular basis so that even if there is the slightest opening for attackers, they get eliminated. This allows the achievement of the desired level of security and minimizes tangible and intangible losses (Shedden, Smith, and Ahmad 2010).
- IISC has not been upgrading their technology. This is evident as they are still using Windows Server 2003 even though there are plenty of better options available in the market now. Using an old operating system that does not receive any security updates is also a vulnerability for the organization, as any malicious actors can exploit it at any time. In order to correct this, they should convert all of the legacy operating

systems to something that is modern and is receiving regular security updates. They should precisely convert their Windows Server 2003 to the 2019 model as it is comparatively a lot more secure and may even give additional features that may be helpful for the firm.

- IISC is still relying entirely on one single-factor authentication. This means any user who has permission to access their systems only needs to enter a password one time in order to gain complete control. This approach can be very threatening as it gives way to various attacks, such as password guessing, brute force attacks, and credential theft. The only way to solve this is to have a multi-tier approach, which is also referred to as the Multi-Factor Authentication (MFA). MFA requires any user to at least confirm their identity two ways. For example, after entering a password, an email will be sent with a four-digit code, which needs to be entered correctly before getting full access. This additional layer of security has a great impact on reducing risk of unauthorized even when the first layer of password protection is breached.
- From the case, we understand that IISC does not consider training employees about awareness of security as an important element for overall security. Without this, employees may not be able to identify common security threats such as phishing emails or social engineering attempts, which may result in data breaches and information leaks. Hence, my recommendation would be to establish routine training for all employees that would teach them about how they can recognize phishing attempts, how they can create stronger passwords, and also where in the organizational hierarchy is the best option for reporting if they find themselves in any situation that me cause risk to the firm. Well-informed employees act as the front line in a war again cyber threats. The better they are trained, the better the chances of the organization to uphold security standards for confidentiality, integrity, and availability.
- IISC also does not posses an ideal data backup and recovery system. This means if there is an event of failure of systems or data loss due to cyberattacks, the organization may never be able to recover it or even if it does it will take a lot of time and money. This could be rectified by introducing an efficient backup system that periodically backs up data to local or cloud storage which can help easy recovery if there is ever a chance of loss. The backups could also be kept in an offsite storage

apart from the offices that IISC already has as it will also protect IISC from potential data losses from physical disasters.

- Lastly, every organization thriving for success will know that there is always a chance of failure. Hence, it is important to have pre-plans to take action immediately if ever something happens. However, for IISC, there are hardly any incident response planning strategies created. If there is ever an incident of an attack of physical disaster of data systems, IISC would have to face huge losses as a result. They do not have a way to detect, report, contain or recover from such incidents. Hence, as a security consultant, I highly recommend that the firm brainstorm and set up a plan on how and which immediatem action would be taifided an event occurs. This plan should highlight responsibilities and roles, communication protocols, and guidelines for recovery. This will reduce costs and improve the performance of the company as a whole while tackling any security incident that comes in their way.

RISK ASSESSMENT APPROACH

Participants:

- Security Consultant (Syed Muhammad Ahmed Zaidi)
    - Lead security consultant who coordinates with all other stakeholders, making sure all inputs are taken into consideration to understand the current situation of the company.
      Email: smazaidi24@gmail.com
- IISC Consulting Management Team
    - The team of management that makes decisions and has complete information of what is happening in which section of the company.
      Emails :
        - John.Doe@iiscmanagement.com
        - Jane.Smith@iiscmanagement.com
        - Robert.James@iiscmanagement.com
- IISC IT Department
    - This department includes all IT related personnel who are expert in technical knowledge. They are responsible for all IT related implementations and posses all relavent information that can be used to implement security procedures.
      Emails:
        - Justin.imberlake@iiscit.com
        - tommy_shelby@iiscit.com
        - maya.claire@iiscit.com

Techniques:

A model for risk assessment can only be effective if it has adequate information as input. The more data a company can generate about relavant security topics, the better the chances are for identifying vulnerbalities in all systems. This requires data collection techniques to be implemented. Few of which are mentioned below

- There could be multiple intreriews being conducted with the IISC Consulting Management team and the members of the IT department. These interviews will focus on how we can gather extensive information about the running of the organization so we can understand it much better. It will to gain enough knowledge on the type of security processes that are being currently used. By talking to relevant people with

preferred topics, on-point information can be collected about each procedure. For example, IT-related employee Justin Timberlake is an expert who helped set up the IT infrastructure. He can guide us on the exact gaps in the system.

- Another essential technique to gather insights about the security practices being used is the reviewing of necessary documentation. This includes all the official policy and procedures that are currently being followed by IISC. The review may also take into account all the incident reports that are lodged, which may in turn be a great way to understand the gaps in the system.
- As a security consultant. I will also consider visiting each office at a time and try to break into things that are not authorized. A system that is able to defend its own will also be able to defend against attacks from outside. Hence, by visiting the premises, any vulnerabilities that are present in regards to access controls, physical security systems and server rooms can be identified and rectified before anyone from outside misuse it.
- Questionaries and surveys are also a way to find answers to hidden questions. There are times when employees do not want to show their identity while recognizing a vulnerability. Hence, providing them a platform where they can anonymously point out where the security risk lies can help find problems that might be hard to figure out by the management working by their own.
- Comparisons and experiences of other firms can also act as a good way to see the problems within. Any recent or relevant security breaches within and outside the industry can also provide ways to search if they exist in IISC as well. If they do, catching them early can allow IISC to build stronger walls that attackers might find more challenging to breach.

Risk Model:

A risk management model is a sequence of activities based on a published standard (Faris et al. 2014). For this risk assessment, the model that will be used for valuation of a security risk is called FAIR. This is an abbreviation for FACTOR ANALYSIS OF INFORMATION RISK. In the field of data security, this model is highly recognized and often used to find more insights about a risk in financial terms. It provides a structured approach that converts the risk into money terms that can be easily understood. The criticality of each risk is rated

according to potential impact and likelihood of occurrence (Shedden et al. 2011). The model will quantify a categorical concept, which would aid in recognizing how impactful a security risk can be in the future.

A few key components of this model include the **Asset**. This primarily refers to the information assets of a company. System, hardware, software, intellectual property, and more. Then, we find the **Threat Events**, which are the likely scenarios that could be impactful for these information assets. These threat events are after the vulnerabilities in an organization, which are mainly gaps in the system that could be due to software or even human ways. We then figure out with domain knowledge or past data the **Loss Event Frequency(LEF**). This refers to the likely chances that a threat event might occur. Lastly, the terminology of **LM refers to the Loss Magnitude**. This quantifies the potential financial impact of a specific threat, even if it will occur. Combining both LEF and LM gives us the **Annualized Loss Expectancy** which is also referred to as the ALE.

Impact Assessment Scale :

Scale Level	Description
1	Negligible
2	Low
3	Moderate
4	High
5	Very Hight

Likelihood Assessment Scale

Scale Level	Description
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

Below is a simplified equation for this concept explained above.

Risk = Threat Event Frequency (TEF) × Threat Event Magnitude (TEM)

This quantitative analysis is typically done by professionals who have access to specialized software and tools. For this report, we will be considering only the most relavant variables and find results with the basic equation.

Risk Assessment Matrix:

Risk Level	**Impact (1-5)**	**Likelihood (1-5)**	**Risk Level**
Very Low	1-2	1-2	Minimal risk
Low	1-2	3-5	Low risk
Moderate	3-4	1-2	Moderate risk
High	3-4	3-5	High risk
Very High	5	1-5	Very high risk

SYSTEM CHARACTERISATION

Hardware:

- **Server Infrastructure**: IISC makes use of both modern and legacy systems in their approach to providing a service. The modern system includes servers that are top-notch. They fall on the criteria required by the industry. However, they also have a blend of legacy servers as well that only have the capacity to run the outdated Windows Server 2023.
- **Diversity in Workstations**: Interms of hardware, IISC does not restrict their employees to use only a particular brand or model of any equipment. They have given them complete freedom to choose among themselves if they want to use personal laptops or tablets if it suits them well. They are mainly concern with output and ease of employees which is why such permissions are pre granted.

Software:

- **User-Centric Application Stack:** As mentioned earlier, IISC is more output-driven driven, which is why they've also allowed stackholders to use software they find best in terms of productivity. Hence, most of the employees use what seems more friendly and productive rather than sticking to one particular software to perform specific tasks.
- **Server OS Diversity:** IISC also continues with the same thinking when it comes to the operating systems. As understood by the case, they use multiple operating systems. Mainly within the organization systems, there is the use oif Windows and Linux. However, as they have no restriction on using personal gadgets, employees may also be making use of MacOS.

Data:

- **Data Storage**: IISC has multiple storage of data as they are spread throughout the land with multiple offices in different cities. They have different repositories that meticulously safeguard sensitive information. They have rules and regulations aligned for data classification and access control which allows this data to be kept in a secure environment. They also keep a good synergy between the types of data collected. This allows data driven decisionmaking also a competitive landscape in the consulting enviorment.

- **Data Abundance**: They collect and retain any data that comes in so that if they have any issue that is related to that data, they would abundance of it to find a solution out of it.

Procedures:

- **Proactive Security Protocols**: IISC also does not only count on having proper reporting of incidents report but also they have continuous monitoring and threat intelligence integration which allows timely response in order to lessen the impact of any risk event.
- **Long-term Planning:** The company works in a way to continue the business for a longer time. This is reflected in most of their policies and procedures showing a thirst towards success in competition. Minimizing downtime during incidents and disruptions highlights their commitment.

People(Users):

- **Dynamic Employee Roles:** Within the company, there is diversity in the background of all employees which reflects how dynamic the whole workforce is. They also have well-defined job descriptions so each worker knows what exactly the requirements are from each of them. Such an environment promotes cross-functional and cross-premises collaboration.
- **Contractor Collaboration:** The clientage for such a company is also very diverse. IISC mainly focuses on welcoming a more comprehensive range. They also work on collaborations with contractors. This actually results in seaming less integrations, which helps in learning more from each other in terms of knowledge about the industry.'

Networks:

- **Cyber-Resilient Connectivity:** As due to the nature of the business, IISC cannot afford to have slow internet speeds as they must need access to information as quick as possible. Hence, by having a quick turnaround for speed, they are able to make their connection cyber-resilient.
- **Guess Network Experience:** They also have a system for guests who would like to visit the organization. They feel safe and protected as they have enough security procedures and protocols that make their experience very satisfactory.

- **Network Infrastructure:** As IISC has multiple locations, they've made use of both wired and wireless networking solutions. Their seamless connection between each other ensures how effectively the infrastructure is performing.

VULNERABILITY STATEMENT

From the case study of IISC we understand that company operating in such a nature industry must be on its toes to be able to protect the information, as any leaks may cause huge impacts on the clients. Hence, As security consultant for them, ive taken a deep look into their scenario and have joined together a few points that can be potential vulnerabilities based on the above mentioned system characterizations. These are as follows:

Hardware:

- **(V1) Legacy Windows Server (Windows Server 2003):** First and most important is the use if Windows Server 2003 in their heritage office. This is regarded as a huge vulnerability as this software has already reach the end of its lifetime with no more updates coming along the way. Microsoft has officially announced that they are working towards the latest models of the software and hence this older version will no longer be getting any security updates and patches. This leads to the organization being exposed to numerous security vulnerabilities as attackers can anytime try to exploit it by gaining access to information that can be misused. Once they have access, their agenda may also be different; for example, they may even try to disrupt critical services to damage the reputation of the company.
- **(V2) BYOD Policy**: As mentioned earlier, the business has given a lot of freedom while giving the employees the satisfaction they ask for. However, too much freedom can also go against the standards of data security. For example, the way the company has allowed anyone to use their personal phones or laptops to log into company information may mean that they are letting an important door open for attackers to come in. As these phones and personal laptops are not fully encrypted like the company assets, it may mean that it will be much easier for attackers to get in using these gadgets. Computer theft and the loss of computers is one of the major security concerns for companies (Bernard 2007).

Software:

- **(V3) Unified Endpoint Management (UEM) Absence:** The company, like other functions of the organization, is still considering this important element to be diverse as well. They have not implemented a Unified Endpoint Management (UEM) solution, which would allow all devices to be controlled from one point. Having access to vital data from different sources may expose the whole system to vulnerabilities like Malware and unauthorized access.
- **(V4) Insider Threat Detection:** IISC consultancy also does not have a dedicated system that detects insider threats. As of now, the company is operating without auditing itself to know if there are any potential vulnerabilities that can be identified. They do not have a way to detect user activities, detect suspicious behavior and also identify potential insider threats that can potentially cause extreme harm to the organization.

Data:

- **(V5) Inadequate Data Retention Policies:** IISC does not currently posses a clear policy on what data they should be collecting and retaining. As a result, they are accumulating unnecessary data which takes up a lot more space in their storage systema and also ultimately increasing costs and time of handling. From security point of view, this also increases the chances of potential exposure of sensitive information.
- **(V6) Data Backup/Recovery Procedures:** Similar to retention, they also do not have a clear backup and recovery plans set up for the firm. They have multiple locations plus data storage respositories, and even then no proper backup and recovery policy applied to them. If any unforeseen circumstance arises and they somehow lose the data, they will not be able to recover it

Procedures:

- **(V7) Guest Network Token:** Anyone who comes as a guest has a Guest Network Token for the next 24 hours. If this token is somehow misplaced or gets in the hands of someone who does not think well for the company, they may end up using it against IISC. This vulnerability could be exploited by malicious actors seeking to infiltrate the internal network, compromising confidentiality and integrity.
- **(V8) Incident Reporting:** Another vulnerability within this whole case is the non-use of incident reporting. As they have not planned out well about what to do in case a

security incident occurs, it means the facts about a breach may not be properly documented. This means IISC Consulting can not use its past experience to improve its standards in the future. Decision-making would also be all over the place in such scenarios as there has never been a documented incident that top management could learn from and do not make mistakes that were previously done.

People(Users):

- **(V9) Employee Training:** Server Room Security:From what we learnt about the employees, we can see that IISC does a great job in keeping them motivated and also satisfied by giving them a lot of freedom. However, they must at the same time ensure that they are properly trained. As of now, any employee who is gullible to a security attack can easily be a source of phishing emails and can cause significant data breaches because of their lack of understanding about the importance of this matter.
- **(V10) Contractor Offboarding Process:** In terms of Contractor Offboard, IISC is also having a weak point that has the potential of getting exploited. Whenever contractors offboard, there is not a proper system to revocate all the access privileges that were previously given. This means even after offboarding, they may still have some access to company information that may actually allow former contractors to exploit critical systems, data, and even network resources.

Network:

- **(V11) Server Room Security:** Server rooms being of the most critical in terms of how crucial is to its security, IISC has been taking this very lightly. They do not possess the right ways to ensure that only the right personnel can get into it. As they have kept it just like any other room, there's a big gap that can be exploited by anyone with the wrong intentions for the organization. Once accessed, the attacker can potentially theft, service disruption, or sabotage the entire company.
- **(V12) Fallback Internet Connetion:** IISC is a consulting company and is heavily dependent on Internet. This is one reason why they have installed high speed internet, however, they do not have a fallback policy incase the internet stops working. This may mean they have to halt processes which may cause huge losses and even chacnes of data breaches while their systems are completely down allowing opportunity of vulnerability.

THREAT STATEMENT

Basic Threats:

- **(T1) Thefts and Break-ins:** There is always a chance of people getting into areas where they are not allowed. This opens up possibilities of thefts as if not properly survailanced, they may take from the organization. There are also chances of people for their reasons breaking into areas where they are not allowed.
- **(T2) Malware and Ransomware:** These attacks are done to exploit or infiltrate computer systems without consent. Malware may include viruses, spyware, adware and much more. On the other hand ransomware may include an attackers demand for something in exchange of the security that has been breached.
- **(T3) Distributed Denial of Service(DDoS):** This is a type of cyberattack that aims to make service unavialble. In the case of IISC it is very important to provide a consistent service to their extensice clientage. However, such attacks limit the usage of the users making them restricted to entertain the requests of their clients.

External Threats:

- **(T4) Hackers:** One of the most critical threats for any organization including IISC is the widespread of External hackers. They could have any agenda behind their hacking that may range from financial gains, notoriety, or even just personal satisfaction. With this hacking, they may aim to gain unauthorized access to the organization's secrets, which may also include essential data of IISC's clients. They may employ different techniques ranging from spear-phishing attacks, Distributed Denial of Service(DDoS), or even just sabotage the whole company.
- **(T5) Competitors:** Another group that may interested in damaging the working/reputation of the company could be the direct competitors of IISC. As this industry is highly saturated, competitors may take wrong steps to ensure they remain or become the giants of the industry. Hence, it is highly possible that they may be bribing any of the employees in the organization to fetch them a piece of information that they have no authorization over. The tactics may also include social engineering attacks that may cause sensitive data leakage.
- **(T6) Social Groups:** At times, there are social groups that may work towards hacking of a company just to make them either accept their terms or prove a point. For example, it might be possible trade unions may form up as a hackactivists to voice

their view about the mistreatment of employees and they take the route of threatening the company by hacking into their system and warning for disclosure unless their terms are met. They may use tactics like Distributed Denial of Service or even data sharing on the web to raise awareness about their cause or to make the company accept what they ask.

Internal Threats:

- **(T7) Internal Employees:** Another threat to the company could be from within a company. Any employee who wants a type of revenge or wants something more out of the company may intentionally compromise data integrity. As employees are the ones that are working within, they understand the company a lot better than any external person. They might be able to damage the company a lot more compared to someone from outside. They could possibly take threatening actions to get unauthorized access and leak information that is highly confidential, causing chaos in the company.
- **(T8) Negligent Employees:** Some employees may do it intentionally, while others may only do it due to their negligence. If employees are not well trained about security matters, they may unwanting create security risks. As they do not know how people are dragged into such matters, they may become victims of threat actions like phishing emails. They may also with their lack of care, send confidential information to the wrong recipient or may accidentally download some malware into the company's system that can cause data breaches.

Threats Beyond Human Control:

- **(T9) Natural disasters:** Lastly, the threats may be beyond human control as they may come in the form of natural disasters threatening the complete physical embodiment of a system. Threat actions like floods, earthquakes or fires can lead to prolonged power outages or even the destruction of the complete infrastructure, which may wipe out the data completely. Without proper backup, the data is no longer restoreable, causing harm to the company as the services may halt.

RISK ASSESSMENT RESULTS

As discussed earlier, each vulnerability has a worth of its own. Each of them can effect the business in different aspects of its working and those effects may range from the impact they can have on it. In this section, a thorough discussion of all the vulnerabilities listed above will be discussed. For ease of referencing, click on the hyperlinks while holding “CTRL” or “Command” (example ((V1) and (T1)) to go directly to the designated details within the report..

- According to the list of vulnerabilities, one that was mentioned at the top and, as a security consultant, which seems to be worth much importance is [V1] the presence of legacy servers within the data infrastructure that are running on an outdated software, Windows Server 2003. The **Consequent Risk** to such an activity may cause numerous attempts of exploitation as it opens up gates ot many vulnerabilities. Any unauthorized access to this may impact the overall confidentiality and the integrity of data as anyone can view or make changes to what they are not permitted to do. The **Impact** of such a risk could be huge to IISC as there are likely chances of data breaches. As IISC handles critical data for many other organizations, it may also lead to their data secrets being breached [T4], which may harshly damage the reputation and trust of IISC as this issue can move onto a bigger scale. It may also lead to regulatory non-compliance due to the use of unsupported software. For Fair, the Loss Magnitude (LM) is 5 which is high. The **Likelihood** of this happening is Likely as attackers are after such vulnerabilities that are easily exploitable. Another Justification for this could be that as Windows are no longer issuing security updates for this software, there is a high chance that the last patch for this software has already been through by any hacker and the instructions to do it again are widely available. Hence, this may ensure that the chances of this happening may be substantially high. For Fair the Threat Event Frequency (TEF) 4 which is refered as Likely on the scale. Hence, The **Overall Risk** risk of this particular vulnerability would be considered as Very high risk as due to the equation Risk = 5 (Impact) × 4 (Likelihood). The **Existing Controls** for this particular vulnerability are not clearly defined. They have not made any movements towards solving the issue. However, from the case, we can see that they have a combination of Legacy and Modern Servers. Hence, there could be a possibility that they are in the middle of a transition and will soon substitute all legacy servers with modern ones. Due to this reason, the **Residual Risk** would be

categorized as moderate. For **Recommendation**, I would suggest they continue this transition if it is in effect. However, they should do it as soon as possible as with the ease and speed increasing of attackers, it is vital to do it quickly so they can mitigate the chances of this risk taking place as an event.

- The next point for hardware is related to BYOD Polcies [V2]. The **Consequent Risk** of allowing employees to use their personal gadgets may cause data leakage. The **Impact** once again can be high as people can literally use their personal laptops/mobiles and sit at home while they access critical confidential data. With such leakages, this vulnerability will be given 4 LM as there are high chances to face threats like [T7] and [T8]. And as all employees can use their personal gadgets with no restriction the **Likelihood** of this happening is also high with a TEF of 4. The **Overall Risk** with FAIR equation would be High Risk. The **Existing Control** is set to freedom, which actually means they have none at all, causing the **Residual Risk** to also be null. The **Recommendation** I want to give to IISC regarding this is to atleast give employees the training to have strong passwords just so third-party people can not get access to the system. They should also install a monitoring app within their personal gadgets so IISC knows who is trying to access which data while not on the premises.
- The next mentioned vulnerability was for Software and was about the lack of use of a Unified Endpoint Management System(UEM) [V3]. The **Consequent Risk** for this is that IISC does not have a way to centrally manage and provide security for multiple devices that are being used in the organization. These included devices like laptops, tablets, mobile phones etc. The **Impact** if this vulnerability becomes an incident would also be high and according to FAIR the LM would be rated as a 4 as there is a high chance of data breaches with threats like [T2] Malware attacks and [T4] Hackers. For such an event, if anyone gets into the system by using their personal device, they can have access to the company's data for a long while without the company knowing as this is not centrally managed. The **Likelihood** of such an event is also Likely, and hence the TEF would be rated as 4. This is because it was discussed in the case that IISC does not restrict their employees from using personal gadgets. Hence, with no UEM on these personal laptops and mobiles, it's just like the data can wander anywhere. The **Overall Risk** for this event would also be categorized as high due to both the impact and likelihood being on the upper scale. The **Existing Control** for

this particular vulnerability is nearly non-existent as everything is decentralized. Therefore this also means there is **Residual Risk**. My **Recommdenation** for IISC for this would be to first find out all the devices that are connected to the system. Once they know, they should implement the UEM system on all of them. If there are new users or new devices, they must first come under the permission and then be used. This would lead to a centralized control with not anyone accessing data on every device.

- Next comes the another vulnerability about software which is of insider threat detection systems [V4]. The **Consequent Risk** about this issue is that IISC consulting does not have a single system to detect existing or upcoming threats. They do not have the ability to Audit themselves to know if they need improvements. Hence, the **Impact** of this could be High as the threats might be bundled up and may come to a point for it gets out of hand for IISC. Once done, data breaches, financial losses, reputational damage, and legal consequences are inevitable [T2], [T3] and [T4]. Therefore the Loss Magnitude for this would be 4. The **Likelihood** of this happening is 3 on the scale for TEF as the possibility of such threats occurring would always be there. By using the equation for FAIR, the **Overall Risk** comes out to be High risk. The **Existing Control** for this does not exist as there is a complete absence of any detecting mechanism. Hence, the **Residual Risk** is none. The **Recommendation** I would give to them would be to understand that this is a High Risk situation; hence it should be treated as a priority. An advanced insider threat system should be implemented that monitors user activities, accesses, and behaviors to identify unusual or suspicious patterns and hence reduce the chances of threat actions.
- The Vulnerabilities mentioned for Data are very similar as they both deal with the lack of policies regarding Data Retention [V5] and also data backup/restore [V6]. The **Consequent Risk** of not having usch policies is that the losses can be huge in amount. With such inadequate considerations about the circumcstances, threats like Natural Disasters [T9] can put the organization in a very serious situation. The **Impact** can be as huge as losing the business as there would be chacnes of data leakage also a complete loss of it. As per FAIR, the LM would be 4 and the Threat Event Frequency would be 2. Therefore the **Overall Risk** for such incidents would be Moderate. The **Existing control** apart from having good storage repositories is none, hence there is no **Residual Risk.** My **Recommenation** would be to have an emergency meeting in

which the top managemen decide alongside the data handlers to see what data to keep and what to dispose of and how. They should also immediately invest in backup and restore systems so that with any event, they are left with a backup.

- Next is the treatment by IISC for guest access [V7] which falls under the Procedure characteristic. The **Consequent Risk** to such an event of providing any guest with a 24-hour access token to visiting clients means they have access to the company's wireless network for the whole day. Most of them may genuinely be used for general purposes; however, as security consultant we must be cautious about everyone. Therefore, giving 24-hour access to a guest who has wrong intentions may mean that we are letting the door open for them to walk in. The **Impact** of this could be that they may be able to access the system data and may even flood malware into it, causing disruptions and halting of service [T2] and [T3]. For FAIR, the rating for LM would come out as 3. The **Likelihood** of this happening may be rare as guests may only come for a limited time hence a TEF of 1. Therefore, the **Overall Risk** would be categorized as Moderate Risk. The **Existing Control** for the organization is currently dependent on the token-based access which eliminates most people who can connect it as a free network. The **Residual Risk** remains as those who are connected may still exploit it. My **Recommendation** would be to reduce the amount of time they are given to access the network. Secondly, additional authentication should be applied so that not everyone as a guest can access it.
- IISC does not have an incident reporting system [V8]. This actually opens the gates to **Consequent Risks** that incidents and breaches may happen but may go without proper documentation [T2] and [T4]. The **Impact** of this would be moderate that is LM of 3 as IISC will not able to improve on this in the future. The **Likelihood** can be high (TEF 4) as there may be many incidents happening but nobody would be aware of it due to the lack of reporting. Hence, the **Overall Risk** for such an incident would rank in the middle which would be moderately risky. **Existing Control** could be Verbal communications about such incidents which makes the **Residual Risk** moderate. However, I would **Recommend** the management to brainstorm and find ways how such incidents can be easily documented. Also, such documentation needs to be retrievable so that whenever another threat action takes place, IISC should know what they did earlier and how to deal with it now.

- The vulnerability of employee training [V9] is another essential door that IISC is not closing. The **Consequent Risk** of not training the employees is easy access for attackers to get into the system by using practices like Phishing emails [T8]. The **Impact** of such an incident would not only affect the business but also the employee as they will be held accountable for it. Hence, according to the Loss Magnitude, this vulnerability would be categorized as 5, which is very high. For **Likelihood**, the chances of such attacks for consulting companies companies like IISC are also high as they possess confidential data for more clients. Therefore the TEF would be 5 which is almost certain. The **Overall Risk** due to very high impact and alsmot certain likelihood would come out to be high risk. The **Existing Contol** may include that employees are being trained on different things and they may also be given some general training for data security. Therefore, the **Residual Risk** is moderate as work is already being done. But, as a security consultant for this company, I would **Recommend** them to have this eradicated as soon as possible. Give employees routine training about how attackers can effect them. They may also send some template phishing emails randomly just to see if any body responds so that they can be trained further.
- Next mentioned vulnerability is about the Contractor Offboarding [V10]. The **Consequent Risk** about this is that IISC does not have an official way of how they will be offboarding a contractor. Anyone may offboard while still having leftover connections with the organization, which they can use to access data [T4] and [T5]. The **Impact** of such an event occurring would mean they can continue to view unauthorized documentation which can cause potential exposure to sensitive data. According to the FAIR method, the Loss Magnitude (LM) would be 4 and on the other hand the **Likelihood** of such an event occurring is possible as not all contractors who offbaord are interested anymore nor would have a reason why they want to exploit the company. There on the scale the Threat Event Frequency would be 3. Hence, the **Overall Risk** to this is also High risk according to the scale for FAIR. The **Existing Control** for such an event is not in existence which is why there is no **Residual Risk**. However, as my **Recommendation**, the process may not take too long but may benefit them enormously. Hence, they should think over the terms and conditions and close this vulnerability once it for all by making every offboarding standardized.

- The vulnerability of the server room security [V11] is also a serious one related to network. **The Consequent Risk** with not restricting the number of people getting into the room may cause problems to the data's confidentiality, integrity and availability [T1]. The **Impact** of such an intrusion may be categorized as high as if someone gets access to that can actually get to the potential to breach any data they want or may even halt the service by causing disruptions. Hence, the LM for this would be 4. On the other hand, the **Likelihood** of such an event occurring would be possible. With no restrictions, people may go in, but not necessarily with the wrong agenda in mind. Hence, the TEF score would be 3. When putting them into the FAIR equation, the **Overall Risk** comes out to be Moderate. The **Existing control** for this is rarely present as the room is treated as any other room, which is why the **Residual Risk** also comes out to be zero. However, Considering the importance of this room, I would **Recommend** them to make sure only the relevant people are let in. This could be implemented by using facial recognition or a biometric system through which only the people who have authorized access can get in.
- Lastly, network vulnerability about fallback of internet connection [V12] can also be found vital for any consulting company especially IISC which deals with so many clients. The **Consequent Risk** with such an event is that lack of connection may lead to system haltage which may given an open door to hackers to walk in and corrupt the system [T4] and [T3]. The **Impact** could be huge as haltage may not only cause loss of clientage due to slowness in services but may also cause loss of data if hacked. There the LM score according to FAIR would be 4. The **Likelihood** of this happening can be seen as with the TEF score of 3. The **Overall Risk** coming out to be High. There is no **Existing Control** as the company has no other internet network to fall back on. Therefore there will also be no **Residual Risk**. My **Recommendation** would be to keep a backup internet network, preferably from a different provider so that any halt in the service can be tallied out by the backup internet.

CONCLUSION

This report undertakes a comprehensive approach to do a security risk assessment for IISC Consulting to analyze the organization's security landscape in current times. As it is systematic use of information to identify sources to estimate the risk (Wangen 2017), it identifies vulnerabilities and possible threats that could have a negative impact on the organization. It reveals various facets of IISC's operations which may be considered as open doors for security risks that may impact the confidentiality, integrity, and availability of organization's data resources. It uses the quantitative model of FAIR (Factor Analysis of Information Risk) to provide an in-depth assessment of all identified vulnerabilities. These include inadequate insider threat detection mechanisms, unsecured server rooms, a lack of standardized contractor offboarding procedures, the potential risks associated with employees using personal laptops for work, and much more. The results emphasize the need for immediate attention to high risk issues and to prioritize them so that all possible security attacks can be mitigated in the future. The report also gives out relevant recommendations for each vulnerability so that IISC can use them as a guide towards correction and protection of their vital data assets.

In conclusion, this report serves as a vital resource for IISC consulting to be used as a guide towards improvement and enhancing their overall security posture. It will require the company to take immediate actions, but once done, they can continue to provide excellence in their service, but this time while having resilience against all possible threats. Implementing these recommendations would ensure the mitigation of the above-mentioned risks and A healthy, secure environment for IISC to grow further. However, IISC must continue to perform such risk assessments on a regular basis to understand what new threats might have recently evolved that require further actions for complete protection.

REFERENCES

Bernard, Ray. 2007. "Information Lifecycle Security Risk Assessment: A tool for closing security gaps." *Computers & security* 26 (1):26-30.

Faris, Sophia, Mohamed Ghazouani, Hicham Medromi, and A Sayouti. 2014. "Information security risk Assessment—A practical approach with a mathematical formulation of risk." *International Journal of Computer Applications* 103 (8):36-42.

Sajko, Mario, Kornelije Rabuzin, and Miroslav Bača. 2006. "How to calculate information value for effective security risk assessment." *Journal of Information and Organizational Sciences* 30 (2):263-278.

Shedden, Piya, Rens Scheepers, Wally Smith, and Atif Ahmad. 2011. "Incorporating a knowledge perspective into security risk assessments." *Vine* 41 (2):152-166.

Shedden, Piya, Wally Smith, and Atif Ahmad. 2010. "Information security risk assessment: towards a business practice perspective."

Wangen, Gaute. 2017. "Information security risk assessment: a method comparison." *Computer* 50 (4):52-61.