Security Management Report

Executive summary

The report is about the assessment and analysis of the risk for Galaxy Corporation- A IT service provider. The scope associated with the current report is based on how an organization can respond to risks with the help of the risk mitigation plan. The main risk associated with the organization is cybersecurity issues, communication issues, health and safety issues, and lack of skills and knowledge. This can be overcome through the implementation of effective resource planning, training program, and selection of well-qualified employees. The finding also shows that a risks assessment plan has a significant impact on the organization's performance.

Table of Contents

Introduction

Introduction of organization

The report is about the assessment and analysis of the risk for Galaxy Corporation- A IT service provider. The role of CISO (Chief Information Security Executive Officer) of Curzon law firm is to conduct a security audit to determine the security and find out any kind of cybersecurity gap in Galaxy Corporation- A Information Technology service provider company that provides various digital services including digital marketing services, website design, database maintenance and other types of technical support. The company was established in the year 2017, since then the company has registered significant growth both in terms of revenue and number of customers.

Scope of assessment

The scope associated with the current report is based on how an organization can respond to risks with the help of the risk mitigation plan. Assessment, evaluation, and mitigating risk is one of the critical aspects that help an organization to identify the risk and take necessary measures to minimize the damage from the risk. Without a proper information security management system, it is difficult for an organization to organize digital information in a secure manner (Stevenson, 2018). In this regard, ISO 27001 provides a systematic guideline and examine the security risk of an organization.

Organizational structure

According to Jordan, and Murphy, (2009), the organization structure is the method that mainly represents how certain activities are associated to accomplish the objective of the business. These organizational activities mainly include roles, rules, and responsibilities. The organization structure associated with the business is a functional structure that benefited the management to focus on collective energies and executing their roles and responsibilities in proper ways. Galaxy Corporation organization structure is illustrated below figure;

The above figure shows that in this organizational structure CEO of the organization is the highest position and marketing, sales, and services directly communicated with them. This organization structure assists the employees to gain and understand their roles and responsibilities and improve performance.

Section2 Risk assessment and analysis

Risks assessment team: Roles and responsibilities

The role and responsibility of the Chief Information Security Executive Officer and the team members can be divided into several stages. The stages are mentioned below:

Stages	Roles and responsibilities
Risk identification	The role of the CIO or Chief Information Security Executive Officer is to identify the source of the risk that can from an information asset, or related to the other internal/ external issues.
Risk Analysis	The role of a project manager is to consider the possibility and impact of the risk. In this stage, the risk has segregated

	the risk into types based on the level of the impact.
Risk evaluation	The role is to include review of the HI and LI positioning is done through proper documentation using various tools and frameworks such as risk register. The criterion of investment depends on the possible impact of the risk. more investment is done for the risk having high impact and high occurrence probability. On the other hand, low investment and focus are given for the low impact risk.
Risk treatment	Risk treatment is done by the team lead by CIO or Chief Information Security Executive Officer which is done internally to mitigate the risk or could be done through transferring the risk. the risk can be transferred through outsourcing the specific task or transfer the risk to the suppliers. The best approach to risk treatment is to completely terminate the risk. ISO 27001 is highly useful as it provides specific sets of control objectives that can be used as the framework for the risk treatment that forms the backbone of the statement of applicability.
Monitor and Review	In this stage the roles and responsibilities of the Chief Information Security Executive Officer and the team members are to monitoring and review can be broken into several areas including staff engagement, staff awareness, management reviews, and improvement

Source [(Papastergiou and Polemi, 2018), (Hsu *et al.*, 2016), (Weil, 2020), (Aksu *et al.*, 2017), (Aksu*et al.*, 2017)]

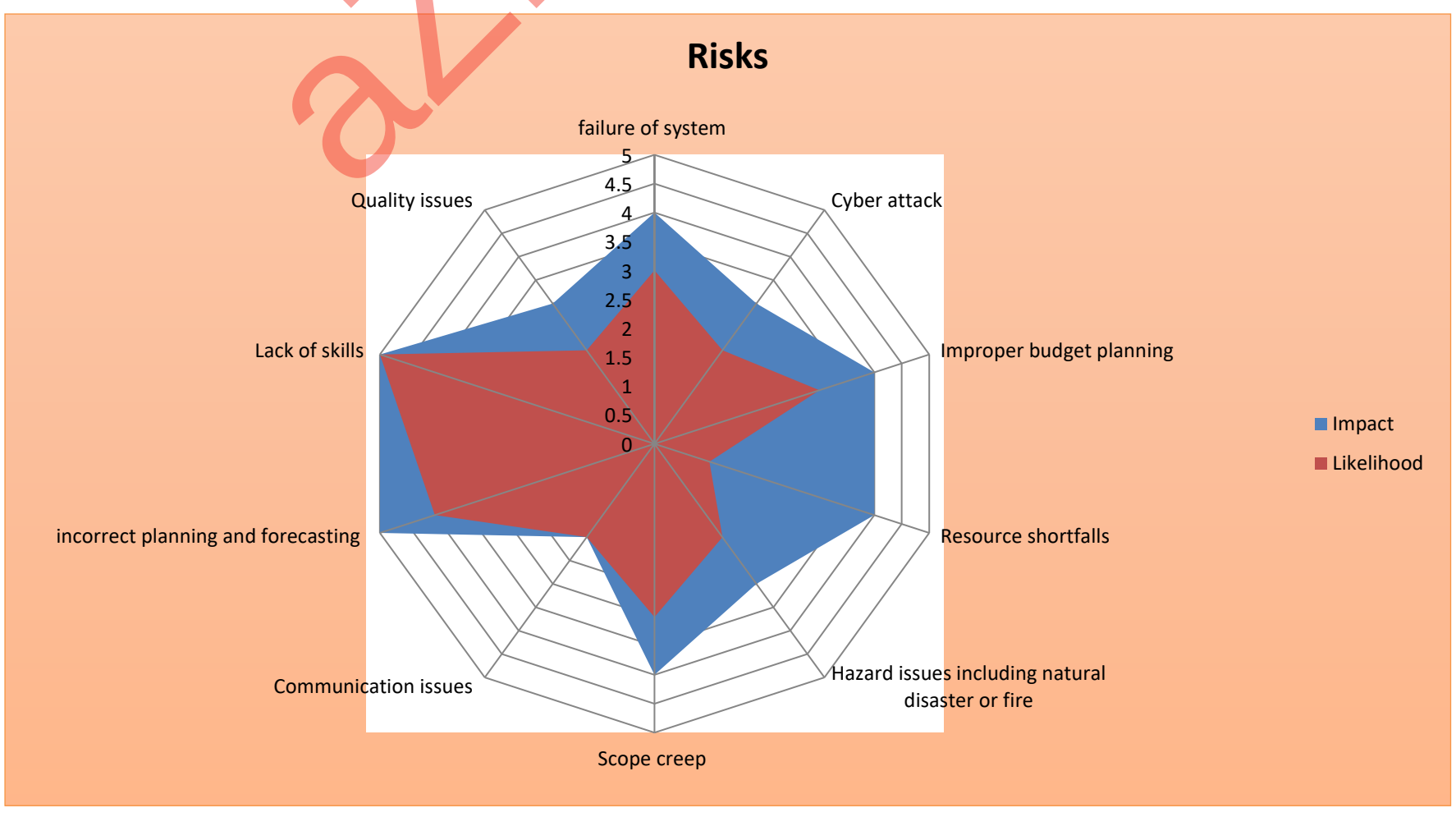
Asset identification and classification

In the risks management strategies risks asset identification and classification of the organization Galaxy Corporation is the starts with the process of self-evaluation and

examination. At this stage project manager of the organization is determine the Galaxy Corporation's information assets, as well as classified, categorizes them according to their effectiveness and usefulness into groups and prioritizes them by their overall effectiveness. The identification of the risks associated with the organization is illustrated in risks tables;

Risks Ref no	Risks assets	Risks explanation	Risks causes	Risks consequence
1	Information and technology	failure of the Computer system	The system is failed due to the failure of software and hardware functionalities	Workers or employees of the organization is not able to perform their task properly
2	Computer	Cyber attack	Improper security policies and vulnerabilities management	Brand values and work performance negatively impacted
3	Bad debt	Improper budget planning	Lack of efficient budgeting tools and techniques	delay business performance
4	Organization image and reputation	Resource shortfalls	lack of human resource planning or unexpected team or employees members leave	Organization performance hampered and business is not able to submit client requirement on time
5	Employees	Hazard issues including natural disaster or fire	Human and environmental accidents	The business running project will not be conducted
6	Cost of component increase	Scope creep	Lack of project scope planning	Both budget and schedule planning is hampered
7	Low customer satisfaction	Communication issues	Lack of communication due to improper communication plan among term members and groups	Delay in project performance
8	Difficult to sell products	Incorrect planning and forecasting	Decrease or increase in the demand for goods than predicated	Project planning and project scope might be impacted
9	Data security	Malicious software	Due to software loophole	Brand image and reputation negatively impacted
10	Completion: legal action	Quality issues	Lack of quality management planning	Quality of products does not fulfil the customer needs

Source [Calder, (2017), Gerba, (2019), Rausand, (2013), Stevenson, (2018)]



Risks vulnerabilities, threats, and severity

According to Stevenson, (2018), risks vulnerabilities is the gaps or weakness in a security program that can be exploited by hazard to gain unauthorized to organization assets. Risks impact, likelihood, and risk rating are illustrated below the table. From the finding, it is obtained that the major risk related to the organization Galaxy Corporation is the failure of the system, improper budget planning, scope creep, incorrect planning and forecasting, and lack of issues(Rausand, 2013). Apart from that, it is obtained that medium risk associated with the organization i.e. Galaxy Corporation is cybersecurity risks, hazard issues including natural disaster or fire, and quality issues.

Risk Rank Matrix						
		IMPACT				
LIKELIHOOD	LEVEL	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Severe
Rare	1	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)
Unlikely	2	Low (2)	Low (4)	Medium (6)	Medium (8)	High (10)
Possible	3	Low (3)	Medium (6)	Medium (9)	High (12)	High (15)
Likely	4	Low (4)	Medium (8)	High (12)	High (16)	Extreme (20)
Almost Certain	5	Medium (5)	High (10)	High (15)	Extreme (20)	Extreme (25)

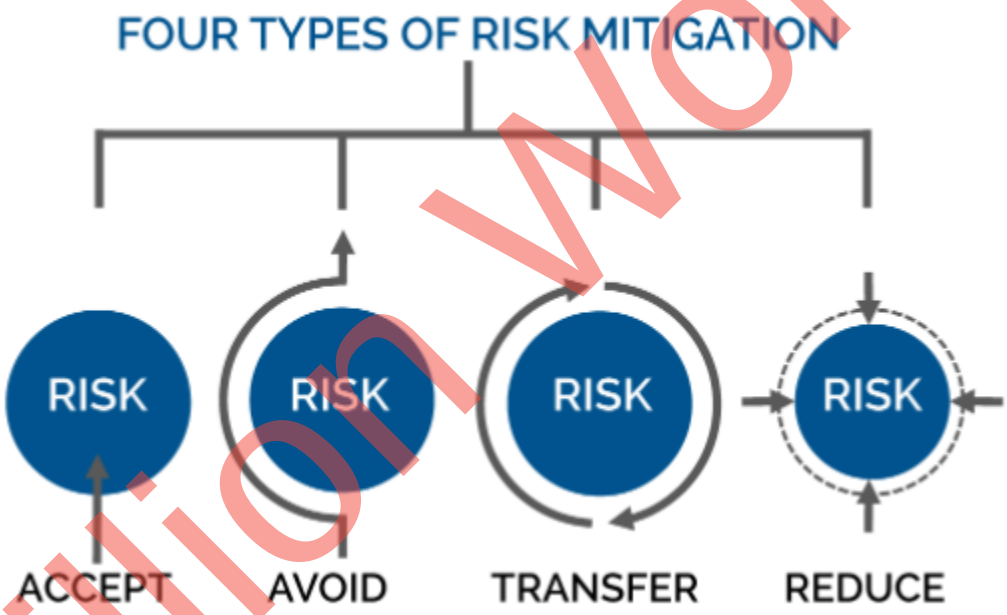
Risk Levels					
L	Low	1 - 4	H	High	10-16
M	Medium	5 - 9	E	Extreme	20-25

risk ref no	Risks description	Impact	Likelihood	Risk rating
1	failure of the system	4-Major	3-Possible	**High**
2	Cyberattack	3-Moderate	2-Unlikely	**Medium**
3	Improper budget planning	4-Major	3-Possible	**High**
4	Resource shortfalls	4-Major	1-Rare	**Low**
5	Hazard issues including natural disaster or fire	3-Moderate	2-Unlikely	**Medium**
6	Scope creep	4-Major	3-Possible	**High**
7	Communication issues	2-Minor	2-Unlikely	**Low**
8	Incorrect planning and forecasting	5-Catastrophi	4-Likely	**Extreme**
9	Lack of skills	5-Catastrophi	5-Almost Cert	**Extreme**
10	Quality issues	3-Moderate	2-Unlikely	**Medium**

Risk of existing control

Risk existing controlling plan and methods helps the management of the organization to manage risks associated with business entails the process of identification, subjugating, and evaluating these issues a defense planning to prepare for unexpected. In risk management strategies, four basic strategies to control the risks associated with

the organization mainly include risk avoidance, risk transferable, risk mitigation, and risk acceptance (Stevenson, 2018). Risk avoidance is the strategy implemented to safeguard and reduce the uncontrolled risk for threats. Risk avoidance strategies mainly accomplished with the help of using an effective training program, implementing efficient technical security protocol and safeguards. Apart from that a risk transferable is referred to as shifting risks to outside entries or other areas. Risk mitigation strategy helps the management of the organization to reduce or decrease the impact of threats. At last, risk mitigation strategies are focused on gaining an understanding of the risk's consequents and accept the risk without mitigating and controlling.



Overall risks calculation

Overall organization risks score is calculated in form of a number that shows the severity of the organization risk due to some factors. Risks score is computed through different factors based upon ranges in impact and probability. Risk rating from 1-4 shows low risk, 5- 9 shows medium risks, 10-16 indicates high and 20-25 shows extreme risks.

Risks description	Impact	Likelihoo	**Risk ratir**
failure of the system	4	3	12
Cyberattack	3	2	6
Improper budget planning	4	3	12
Resource shortfalls	4	1	4
Hazard issues including natural disaster or fire	3	2	6
Scope creep	4	3	12
Communication issues	2	2	4
incorrect planning and forecasting	5	4	20
Lack of skills	5	5	25
Quality issues	3	2	6

Risks assessment method selection

Risk assessment procedures are implemented to execute a risk assessment for a business's information security. Presently there are several risk assessment procedures from which to select, exhibiting a different of issues. The impact and likelihood are rated on a scale of 1-5, but the organization's overall risks assessment score of particular issues is computed to anywhere from 1-5. According to Gerba, (2019), the Management of the organization also implemented what-if analysis, checklists, hazard, and operability study, use a failure mode and effect analysis, and fault tree analysis. Implementation of the above risks assessment helps the management to effectively determine and identify the issues.

THREAT	VULNERABILITY	LIKELIHOOD	IMPACT	RISK EXPOSURE	CONTROL TO BE IMPLEMENTED	HOW LIKELY NOW CONTROL IS IN PLACE?	IMPACT WITH CONTROL IN PLACE	OVERALL MANAGE RISKS EXPOSURE
Failure of the Computer system	The system is failed due to the failure of software and hardware functionalities	4	3	12	Mitigate	Ensure that organization need to train their employees and working on the improvement of skills through training and providing information to reduce confusion	2	1
Cyber attack	Improper security policies and vulnerabilities management	3	2	6	Avoid	To implement proper network security protocol and firewall techniques.	3	1
Improper budget planning	Lack of efficient budgeting tools and techniques	4	3	12	Avoid	To implement efficient budget planning tools and techniques	1	1
Resource shortfalls	lack of human resource planning or unexpected team or employees members leave	4	1	4	Transfer	To ensure that organization created proper backup	2	2
Hazard issues including natural disaster or fire	Human and environmental accidents	3	2	6	Mitigate	Get all project paperwork and stored in cloud computing	3	1
Scope creep	Lack of project scope planning	4	3	12	Accept	Ensure that proper scope is created during project designing and planning	2	1
Communication issues	Lack of communication due to improper communication plan among term members and groups	2	2	4	Accept	Ensure that proper communication plan and strategies are implemented	1	1
Incorrect planning and forecasting	Decrease or increase in the demand for goods than predicated	5	4	20	Mitigate	Ensure that proper analysis and reporting system utilized to and provide accurate information	1	1
Malicious software	Due to software loophole	5	5	25	Mitigate	Ensure that proper training and development is implemented and also recruited well-qualified skills workers	2	1
Quality issues	Lack of quality management planning	3	2	6	Transfer	ensure that proper quality plan and monitoring technique is implemented	1	1

Table 1 Probability impact matrix

		IMPACT				
Likelihood	LEVEL	1	2	3	4	5
RARE	1	2	2	3	Resource shortfalls 4	5
UNLIKELY	2	4	Communication issues	The cyberattack, Hazard issues including natural disaster or fire, Quality issues	8	10
Possible	3	6	6	9	failure of the system, Improper budget planning, Scope creep	15
Likely	4	8	8	12	16	incorrect planning and forecasting
Almost certain	5	10	10	15	20	Lack of skills

Section 3 Risk mitigation- ISO 27001

Proposed of mitigating control ISO 27001

The policy of the access control should be established, documented, and reviewed at regular based on the business requirement for the assets in scope. The control rules, restrictions, and rights including the depth of the controls need to reflect information security risk based on the organization's appetite and information for managing them. Risk mitigation control according to ISO27001 is based on risk management of the following criteria (Sicari*et al.*, 2018).

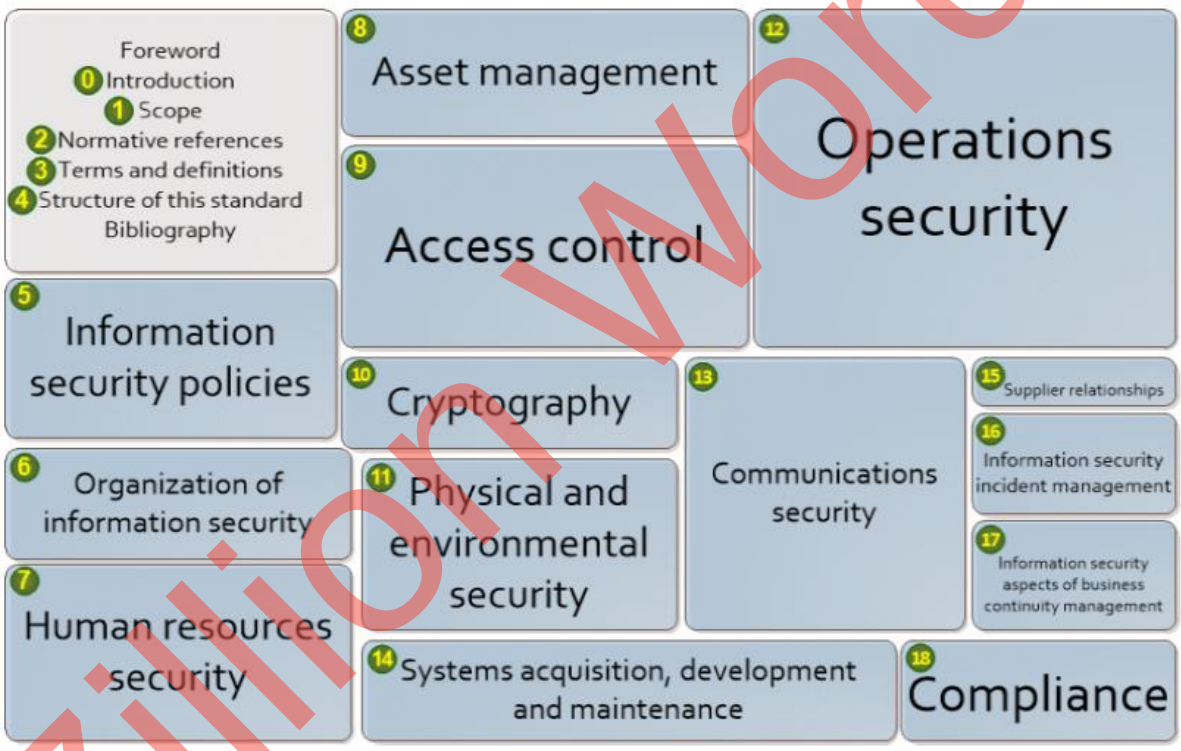


Figure 1mitigating control ISO 27001

Source (Sicari*et al.*, 2018)

The principle based on the network access and network services is the approach favored for protection, rather than superuser rights or unlimited access without proper consideration. To secure the network, it is important to allow access to the network to the people who know about their role and responsibility, Managementcontrols, procedure, authorization procedures (Radanliev*et al.*, 2019). The control of access is a vital aspect of cybersecurity that can be both physical and digital. For instance, the permission restrictions are based on the user accounts as well as the limitations on the

person who can access a certain physical location. The policy needs to be account including security requirement such as the business applications that can be aligned with the information, the control of the access of the rules should be supported by formal procedures as well as defined responsibilities. *Network services and access to networks:* The access principles in the general approach is favored for protection, instead of that unlimited access without careful consideration. As such a person should get access to the services of the network. *User deregistration and Registration:* A user registration and deregistration procedures are required to be implemented and at the same time, a good process for the ID management associate with responsible people(Faris *et al*., 2014).

Justification for selection of control (SOA)

The statement of Application (SOA) creates a fundamental portion of the organization's information security management system which is one of the most vital documents regarding organizational security and risk management. ISO 27001 is one of the comprehensive approaches that apply to all kinds and sizes of organizations including SMEs, large enterprises, private companies, and public sector organizations. SoA and ISO standards are entirely about developing a comprehensive system for the management of information security risk(Bamakan and Dehghanimohammadabadi, 2015). The SoA is a requirement to get ISO certification including with the scope will be one of the first aspects that an auditor will look for in their audit work. The document related to SoA required to be available for review during the certification Stage-1 audit, however, will tend to be drilled into during the Stage-2 audit, when the authority or auditor well be testing some of the ISO 27001 controls to ensure that it not only describes but adequately demonstrate the control aims tend to achieve. (Radanliev*et al*., 2019)The objectives of SoA are to cover the organization's services and products, its information assets, processing, systems in use, facilities, people involved, and the process of business, whether that is a virtual one person business or a multinational operation with a large number of staffs. It is not expectable having an ISO certification with the SoA and a scope for a UK head office when the basic information processing risk tends to take place in an offshore office without the scope of resources. Therefore, certification authorities are now encouraging the 'whole

organization' concept or scope, which creates a much deeper and broader statement of applicability is a need.

Effect of proposed control –risks reduction

There are four options available when there is the list of unacceptable risks for an organization there are four options that reduce the risk, avoid the risk, share the risk, and retain the risk. ISO 27001 describes the risk six major risk assessment and treatment in six steps including assessment of risk and its methodology, proper implementation of risk assessment, risk treatment implementation, reporting of risk assessment, statement of risk applicability, and most importantly risk treatment plan. The first phase of the risk reduction process is a planning process that involves laying out the detailed groundwork for the Chief Information Security Executive Officer has to ensure achievement of Information security management system and its intended outcomes towards reducing the unwanted results (Radanliev*et al*., 2019). The second phase of the risk reduction is an assessment of risk that includes establishment and maintain particular information criteria of risk, the phase also includes repeated risk assessments, identification of risk associated with confidentiality loss, ensuring integrity and availability regarding for information related to the scope of the information management security's security. The third phase of the risk reduction process is the treatment of the risk that is elaborately mentioned in RTP (Risk treatment plan) that provides a summary of the particularity of the risk identification, the responses that been mentioned for an individual risk, the parties involved or responsible for the available risks(Faris *et al*., 2014).

Risks treatment plans

The risk treatment plan is an effective element for ISO 27001 implementation procedures as it helps the management to effectively document the ways the organization will respond to determine issues. ISO 27001 recommended that management of the organization i.e. Galaxy Corporation needs to implement one of the four actions such as risk treatment, risks migration, risk avoidance, and risk acceptance. The risks treatment plan for risks identification is illustrated in the following table;

Asset ID	Risk Description	Risk Value	Type of Treatment	Controls already in place	Controls to be implemented	Date	Responsible for applying the controls	Comments/ Additional information
ASOO1	failure of the Computer system	High	Mitigate	Monitoring tools	Ensure that organization need to train their employees and working on the improvement of skills through training and providing information to reduce confusion	20.12.2020	supervisor	Completed
ASOO2	Cyber attack	Medium	Avoid	Antivirus install	To implement proper network security protocol and firewall techniques.	20.12.2020	Information management	Completed
ASOO3	Improper budget planning	High	Avoid	Communicate with manager	To implement efficient budget planning tools and techniques	20.12.2020	Financial manager	Completed
ASOO4	Resource shortfalls	Low	Transfer	Monitoring tools	To ensure that organization created proper backup	20.12.2020	HRM	Completed
ASOO5	Hazard issues including natural disaster or fire	Medium	Mitigate	Monitoring tools	Get all project paperwork and stored in cloud computing	20.12.2020	IT	Completed
ASOO6	Scope creep	High	Accept	Monitoring tools	Ensure that proper scope is created during project designing and planning	20.12.2020	project manager	Completed
ASOO7	Communication issues	Low	Accept	Training	Ensure that proper communication plan and strategies are implemented	20.12.2020	HRM	Completed
ASOO8	incorrect planning and forecasting	Extreme	Mitigate	Monitoring tools	Ensure that proper analysis and reporting system utilized to and provide accurate information	20.12.2020	PM	Completed
ASOO9	Malicious software	Extreme	Mitigate	Antivirus install	Ensure that proper training and development is implemented and also recruited well-qualified skills workers	20.12.2020	HRM	Completed
ASOO10	Quality issues	Medium	Transfer	Monitoring tools	ensure that proper quality plan and monitoring technique is implemented	20.12.2020	QA	Completed

Source [Calder, (2017), Gerba, (2019), Rausand, (2013), Stevenson, (2018)]

Risks communication plan

Risk	Timing	Sender	Audience	Key message	Desired outcome	Methods
failure of the Computer system	Anytime	IT manager	Project team members, sponsors	False monitoring	Improved system performance	Workshops and training
Cyberattack	First quarter in 2021	IT manager	Project team members, sponsors	False security awareness	Improved security protocol	IT training
Improper budget planning	First quarter in 2021	Finance manager	The project sponsor and project manager	False budget planning	Improve budgeting tools	Implement monitoring tools
Resource shortfalls	Second quarter in 2021	HRM	Project stakeholders, sponsor, and team members	False Resource planning	Implement monitoring tools	Implement monitoring tools
Hazard issues including natural disaster or fire	Anytime	PM	Project team members	False monitoring	implement proper monitoring tools	Implement monitoring tools
Scope creep	First quarter in 2021	PM	Sponsor	False planning	implement proper planning	Proper communication plan
Communication issues	Anytime	PM	Project stakeholders, sponsor, and team members	False communication plan	implement proper communication plan	Proper communication plan
incorrect planning and forecasting	First quarter in 2021	PM	Project stakeholders, sponsor, and team members	False monitoring	Implement proper monitoring tools	Proper monitoring tools
Malicious software	First quarter in 2021	IT manager	The project sponsor and project manager	False security awareness	Improve security	IT training
Quality issues	Fourth quarter in 2021	QA	The project sponsor and project manager	False quality awareness	Robust quality plan	Quality training

Section 4: Business continuity plan

Formulate business continuity plan

Formulation of the business continuity plan for Galaxy Corporation organization is included the following steps;

Critical Asset/ Function	BIA Owner	Assessment date	Review Date	Recover Time Objective	Maximum Tolerable Period of Disruption	Impact Recovery Point Objective
Information and technology	IT	21-Dec-20	22-Dec-20	4-10 hours	High	1-2 days
Computer	IT	22-Dec-20	23-Dec-20	5-9 hours	Medium	1-3 days
Bad debt	Financial manager	23-Dec-20	24-Dec-20	1 days	High	1-3 days
Organization image and reputation	HRM	24-Dec-20	25-Dec-20	6-12 months	Low	1 years
Employees	IT	25-Dec-20	26-Dec-20	10 hours	Medium	1-2 days
Cost of component increase	PM	26-Dec-20	27-Dec-20	10-12 hour	High	1-2 days

Low customer satisfaction	HRM	27-Dec-20	28-Dec-20	9-11 hours	Low	1-2 days
Difficult to sell products	PM	28-Dec-20	29-Dec-20	7-9 hours	Extreme	1-2 days
Data security	HRM	29-Dec-20	30-Dec-20	11-12 hours	Extreme	1-2 days
Completion: legal action	QA	30-Dec-20	31-Dec-20	2-5 hours	Medium	1-2 days

Source [(Sicari*et al.*, 2018), (Radanliev*et al.*, 2019), (Faris*et al.*, 2014)]

Performance business impact analysis

Determine RTO (recovery time objective)

In the context of business, RTO or Recovery Time Objective is the duration and level of time within which the process of a business organisation should be restored after a disaster to avoid risk or unacceptable consequence related to the break in continuity. The term is designates the variable amount of information that will be erase or need to re-entered during the downtime of the network. The "real time" can pass before the disruption starts to unacceptable result that impacts the flow the business operations (Radanliev*et al.*, 2019). While calculating the ROT, there are two aspects Recovery Time and Recovery point that needs to introduced by different manual and automated steps to starts the enhancement of business application. A set of tools, policies and procedures are implemented by the organisation to recover or continuation of necessary technology infrastructure within the targeted duration of time. RTO is established during the time of Business Impact Analysis by the designated person to the technology and process, including recognizing options time frame for manual workaround. The determination of RTO should be done as a part of BIA (business impact analysis) along with the continuity planner of the business.

Determine RPO (recovery point objective)

An RPO is the systematic measurement of duration of time from the failure or comparable loss-causing event. RPO is the measurement process back in time to when the data of the organisation used to be preserved in a format. The processing of recovery normally preserves any data changes the made before the failure or disaster. The measure of the RPO is done to evaluate several factors including the limit of IT that could be stretching back in time from the disaster to the point where data is in normal format, the measurement of RPO also done to frequently backup the data, although the RPO doesn't shows extra IT requirement(Faris*et al*., 2014). It is also measure to calculate the amount of data is lost due to the disaster or even that caused loss. The calculation of RPO is expressed backward in time from the time of failure, and can be specified in minute's details including seconds, minutes, or days. Therefore, it can be a important consideration in disaster planning for recover of data. When the RPO of given for a system, network or computer has been defined that determines the minimum frequency with the recovery process or backup must be made. RTO assists the administrators to select recovery technologies and processes.

Propose a disaster recovery plan

The discovery recovery plan process includes the five steps mainly includes the identification of critical assets, lists of possible disaster, assess risks, action plan and test pan and modify. The process of identification of critical assets includes the findings main asset that is important for organization (Hsu, Wang, and Lu, 2016). Moreover lists of possible disaster includes the natural and manmade disaster and assess risks helps to indentify how much it impacted the performance of business. Additionally action plan helps to resolve all risks in proper ways.

The proposed disaster recovery plan for business Galaxy Corporation organization is following;

Critical Asset/ Function	Proposed DR Solution	Responsibility
Information and technology	Backup system	IT Team
Computer	Regular backup	IT Team
Bad debt	Alternative budgeting tools	Finance manager
Organization image and reputation	ERP	HRM Team
Employees	Forecasting tools	PM
Cost of component increase	MS project management tools	PM
Low customer satisfaction	Use face to face	PM
Difficult to sell products	Planning software	PM
Data security	Install antivirus	IT Team
Completion: legal action	CCTV	QA Team

Conclusion

From the above finding, it is concluded that risk assessment planning and technique is the vital strategies for organization and helps to business to overcome the problem before occurrence. It is concluded that to overcome the risks the management of the business needs to implement proper planning and strategies. From the evaluation, it is found that the main risks asscoatied with the organization is a lack of communication skills and knowledge and this can be reduced through the implementation of an effective training and development program.

References

Papastergiou, S., and Polemi, N., 2018. MITIGATE: A dynamic supply chain cyber risk assessment methodology. In *Smart Trends in Systems, Security and Sustainability* (pp. 1-9).Springer, Singapore.

Hsu, C., Wang, T. and Lu, A., 2016, January.The Impact of ISO 27001 certification on firm performance.In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4842-4848).IEEE.

Weil, T., 2020. Risk Assessment Methods for Cloud Computing Platforms. *IT Professional*, *22*(1), pp.63-66.

Aksu, M.U., Dilek, M.H., Tatlı, E.İ., Bicakci, K., Dirik, H.I., Demirezen, M.U. and Aykır, T., 2017, October.A quantitative CVSS-based cyber security risk assessment methodology for IT systems.In *2017 International Carnahan Conference on Security Technology (ICCST)* (pp. 1-8).IEEE.

Sicari, S., Rizzardi, A., Miorandi, D. and Coen-Porisini, A., 2018.A risk assessment methodology for the Internet of Things. *Computer Communications*, *129*, pp.67-79.

Radanliev, P., De Roure, D., Nurse, J.R., Nicolescu, R., Huth, M., Cannady, S. and Montalvo, R.M., 2019. Cyber risk impact assessment. *University of Oxford*.

Faris, S., Ghazouani, M., Medromi, H. and Sayouti, A., 2014. Information security risk Assessment—A practical approach with a mathematical formulation of risk. *International Journal of Computer Applications*, *103*(8), pp.36-42.

Hoy, Z. and Foley, A., 2015. A structured approach to integrating audits to create organisational efficiencies: ISO 9001 and ISO 27001 audits. *Total Quality Management & Business Excellence*, *26*(5-6), pp.690-702.

Bamakan, S.M.H. and Dehghanimohammadabadi, M., 2015.A weighted Monte Carlo simulation approach to risk assessment of information security management system. *International Journal of Enterprise Information Systems (IJEIS)*, *11*(4), pp.63-78.

Calder, A., 2017. *Nine steps to success: An ISO 27001 implementation overview*. IT Governance Ltd.

Faustman, E.M. and Omenn, G.S., 2008. Risk assessment. *Casarett and Doull's toxicology: The basic science of poisons*, pp.107-128.

Gerba, C.P., 2019. Risk assessment. In *Environmental and pollution science* (pp. 541-563). Academic Press.

Rausand, M., 2013. *Risk assessment: theory, methods, and applications* (Vol. 115). John Wiley & Sons.

Stevenson, M., 2018. Assessing risk assessment in action. *Minn. L. Rev.*, *103*, p.303.

Li, W., 2014. *Risk assessment of power systems: models, methods, and applications*. John Wiley & Sons.

Jordan, R.G. and Murphy, P.A., 2009. Risk assessment and risk distortion: finding the balance. *Journal of Midwifery & Women's Health*, *54*(3), pp.191-200.

Latessa, E.J., Lemke, R., Makarios, M. and Smith, P., 2010. The creation and validation of the Ohio Risk Assessment System (ORAS). *Fed. Probation*, *74*, p.16.