iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 7 **Issue:** V **Month of publication:** May 2019

**DOI:** https://doi.org/10.22214/ijraset.2019.5238

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177*
*Volume 7 Issue V, May 2019- Available at www.ijraset.com*

# Research on Importance of Cyber Security Audit and Assessment in Bank

Vibhisha Ghodasara[1], Chandresh D Parekh[2]
[1]*M.Tech, Raksha Shakti University, Ahmedabad, Gujarat, India*
[2]*Assistant Professor, Raksha Shakti University, Ahmedabad, Gujarat, India*

***Abstract:*** ***Banks are facing an unprecedented challenge of data breach and thus enhancing their cyber security positions because of rising cyber-attack. The cyber-attack threat is substantial and continually evolves. Cyber-attacks that may lead to money and reputation losses. Many audit committees and boards have set expectations for internal audit to understand and evaluate the ability of the bank to manage associated risks. A cyber security audit focuses on cyber security standards, guidelines, and procedures and such controls are implemented. Other operational audits are also based on the audit of cyber security. The paper examines the role and importance of the bank's internal audit and internal controls.***
***Keywords: Internal audit and control, Framework and Policies Implementation, Risk identification and Assessment, Incident Management ,Compliance, business objectives, Security Considerations and Awareness, Solutions For Improvement***

## I. INTRODUCTION

Everyone is going cashless, using digital money, i.e. Debit and credit card. In this context, ensuring that all cyber security measures are in place, protecting your data and your privacy, becomes very important.

Data breaches can make it difficult to trust financial institutions. For banks, this is a serious problem. A weak cyber security system can amount to data breaches that can easily cause their customer base elsewhere to take their money. You often tend to lose time and money when a bank's data is infringed. Recovering from the same thing can be time-consuming and stressful. Cancelling cards, checking statements, and keeping complications open in your eyes would be involved.

Your private data can do much harm in the wrong hands. Even if you cancel the cards and immediately take care of fraud, your data is sensitive and can reveal a lot of information that could be used against you.

Banks need more than most firms to be on their guard. This is the cost of keeping valuable personal data that banks do. If not protected from cyber-crime threats, your bank data may be infringed.

### *A. Key drives for Investment in Cyber Security*

*1)* Sensitive information about customers
*2)* Fortify systems and IT processes
*3)* Customer Convenience and Payment Requests Security
*4)* Comply with regulatory requirements

### *B. What is the Role and Significance of Bank's internal audit and Internal Control?*

*1)* How to implement internal audit and internal control?
*2)* How does the case bank influence the implementation of internal audit and internal control?
*3)* What are the internal audit and internal control regulations to be complied with by the case bank?

### *C. An Audit In Three Parts*

*1)* *Management:* Ultimately, management owns the organization's risk decisions. It therefore has a vested interest in ensuring that there are cyber security checks and that they operate effectively. Typically, decisions are made on the basis of guidance received during the processes of risk management, the appropriate direction to take.
*2)* *Risk Management:* Risk assessments are typically conducted on the basis of guidance from an organization's security officer, and business management make decisions using processes of risk management. The objective is twofold in any risk assessment.First, it is critical to communicate the risk state so that the level of risk involved is easy to understand and clear. Secondly, and equally significantly, it is also necessary to identify ways in which to address this risk. This provides both a problem and a solution, and mitigates a bank's negative impact.

©IJRASET: All Rights are Reserved

3) *Internal Audit:* Auditing is a measure of security— not a disadvantage. Protecting a business in today's global digital economy is critical. In many organizations, the internal audit department plays a vital role in cyber security auditing and often has a dotted-line reporting relationship with the audit committee to ensure that an independent view is communicated at the bank's board level. Audit helps bank with the challenges of managing cyber threats by providing an objective assessment of controls and making recommendations for improving them, as well as helping senior management and board of directors understand and respond to cyber risks.

## II. WHAT IS THE CYBER SECURITY FRAMEWORK?

The Framework refers to this compilation of practices as "the core." This core consists of five concurrent and on-going functions—identifying, protecting, detecting, responding, and recovering — that provide a strategic view of the lifecycle of cyber security risk management by an organization. Furthermore, each function is divided into categories linked to programmatic needs and specific activities. Furthermore, each category is divided into subcategories pointing to informative references. These references refer to specific sections of standards, guidelines and practices which illustrate a method for achieving the results associated with each subcategory.

## III. POLICIS IMPLEMENTATION

Cyber security policies have been framed at Bank, taking into account the security requirements, based on a series of security principles. All policies on cyber security and their need were addressed below:

### *A. Inventory Management Of Business It Assets*

1) *Asset Management Policy:* Information assets are accounted for and have an asset owner nominated. Owners shall be identified *and catalogued for all information assets and assigned responsibility for maintaining appropriate controls. The owner may* delegate the implementation of specific controls as appropriate, but the owner remains responsible for proper asset protection.
2) *Risk Management Policy:* Detailed risk assessments for information risks (e.g. application risk assessment, Infra risk assessment) are undertaken to identify relevant threats, extent of vulnerability to such threats, likelihood and potential impact should the vulnerability result in a mature threat. This assessment will determine the acceptable, transferable and avoidable risk and the risk that risk treatments (control mechanisms) will reduce.
3) *Data Classification Policy:* A data classification scheme has been designed to ensure that the confidentiality, integrity and availability of information are maintained. The level of security to be given to the information will be directly dependent on data classification.
4) *Incident Management Policy:* Incident management is necessary and needs to be established to ensure a rapid, effective and orderly response to incidents of security. Depending on the sensitivity and size of the information systems being managed, such a policy would vary in scope. For all systems, a company-wide incident management policy has been developed.

### *B. Preventing Access Of Unauthorised Software*

1) *Internet & Intranet Security Policy:* Bank should use the Internet as an important information and knowledge resource to more efficiently carry on the business. Users also need to understand that any Internet connection gives unauthorized users the opportunity to view or access corporate information. In this direction, bank has developed systems and procedures to ensure that a uniform code of conduct is used only for business purposes in a secure manner (without jeopardizing the security of the network of the bank).
2) *Control Of Software Installations:* Bank Must Have Full Control on all Software (OS and Application Software), Utilities Etc. Installed, To Be Installed on all IT Devices of the Bank. In The Beginning Bank Will Delete, Un-Install, Remove all Unauthorised, Pirated, Unlicensed Software, Utilities From All Its Devices And Shall Put In Place Adequate Control So That Any One Not Having Authority Can Not Install Any New Such Software / Utility Without Written Permission From The Authority.
3) *Web Browser Configurations:* Since All Major Software (including CBS) Run In The Web Browser And Web Browser Are The Primary Entry Point For Malware And Viruses, Bank Shall Put In Place Controls In Every PC / Laptop / Mobile Device (In Its Control). All web browsers will run as suggested by RBI and CBS provider under a standard configuration. Users are not going to have rights to change the settings.

©IJRASET: All Rights are Reserved

4) *Password Policy:* Passwords must be strong, complex and long, Passwords must not be shared with anyone, Passwords must not be inserted in email messages, does not use the "Remember Password" feature of applications, any user who suspects that his / her password might have been compromised must report the incident and change all passwords.

*C. Environmental Controls*

1) *Physical & Environmental Security:* To prevent unauthorized physical access, damage and interference to Banks premises and information, critical or sensitive information processing facilities must be housed in a secure area, protected by secure parameters, with appropriate entry controls.

*D. Network Management And Security*

1) *Network Security Policy:* To ensure data security in private and public networks and to protect connected services from unauthorized access, appropriate controls should be established. It is necessary to protect the network infrastructure of the Bank from unauthorized access. To protect these environments, a variety of security controls are required in computer networks. The network security policy has been framed for the bank, taking into account the above.
2) *Wireless Security Policy:* Local Wireless Area Networks (LANs) are part of the corporate network infrastructure of the bank. The wireless network must meet the same level of security employed by the rest of the infrastructure to protect the bank's business needs. This policy is designed to ensure that wireless networking deployment is controlled and managed in a centralized manner to deliver functionality and optimum service levels while maintaining network security.

*E. Secure Configuration*

Firewall configurations should be set to the highest level of security and configurations should be performed periodically to evaluate critical devices (such as firewall, network switches, security devices, etc.). Dedicated use should be made of systems such as network, application, database and servers for the purpose for which they were set up.

*F. Anti-Virus And Patch Management*

1) *Anti-Virus Management:* Viruses, Trojans, worms, etc. are malware programs that are called malware and may corrupt or destroy data or distribute confidential information to unauthorized recipients, resulting in loss of confidentiality, integrity, information availability. Detection and prevention of malware should be implemented as appropriate. Protection against malware should be based on good awareness of security and adequate controls of system access. For the above reasons, the anti-virus policy was framed.
2) *Patch Management Policy:* To reduce the likelihood of a serious business impact, a patch management process must be in place to address technical system and software vulnerabilities quickly and effectively.

*G. User Access Control / Management*

1) *Access Policy:* The Access Policy's intention is to provide guidance on the confidentiality, integrity and availability of data / information by applying various access controls and tracking the incident and ensuring that the person knowingly / unknowingly does not infringe any cyber security policy.
2) *Audit Logging And Monitoring Policy:* Audit Logging and monitoring policy addresses the operating system events framework, application events, local area network database events and network events framework.
3) *Security Monitoring:* A Security Operations Centre or a process for the security monitoring of critical IT asset logs shall be established like CCTV logs.
4) *Remote Access Policy:* This policy is intended to define standards for connecting from any host to the bank network. The purpose of these standards is to minimize potential bank exposure from damage that may result from unauthorized use of bank resources. Damage includes loss of confidential data, intellectual property, public image damage, damage to critical internal banking systems, etc.

*H. Secure Mail And Messaging Systems*

1) *E-Mail Security Policy:* Bank shall implement effective systems and procedures to ensure that e-mails are used as an efficient business communication mode and control procedures are implemented so that users do not misuse the e-mail facility. It also needs to be ensured that e-mail service and operations remain secure, efficient during intranet and internet communication.

©IJRASET: All Rights are Reserved

*I. Removable Media Policy*

1) *Usage Of Removable Media And Scanning Before Use:* The easiest way to compromise a system and to introduce malware and viruses is through USB devices. Bank Shall use of USB devices severely restricted. Only the authorized Devices of Bank will work on the network and will also be limited to one or fewer computers. All such devices will be scanned before they are used for viruses and malwares.
2) *Policy On Secured Discard Of It Assets:* Discarding a critical IT asset must be done in a systematic and secured manner that does not permit any information leakage. All server hdds, USB storage devices and storage devices from other critical systems must be systematically destroyed and documented for audit purposes.

*J. User/Employee/Management Awareness*

All bank employees and, where appropriate, contractors and third-party users will receive adequate awareness training and regular updates in bank policies and procedures as relevant to their job function.

*K. Customer Education And Awareness*

Customer awareness should be addressed for both retail and commercial customers and, at a minimum, should include a list of suggested cyber security mechanisms that customers may consider implementing to mitigate their own risk(s). Educate customers to keep their card, PIN, etc. safe and not share it with third parties.

*L. Backup And Restoration*

To protect information and computing resources from various business and environmental threats, systems and procedures have been developed to back up all business data, related application systems and software for operating systems on a scheduled and standardized basis across banks. Whenever possible, the backup and recovery procedures must be automated using the system features and regularly monitored.

*M. Vendor/Outsourcing Risk Management*

When bank relies on or has to deal with third-party services, it is essential to ensure that the same level of cyber security protection is implemented in the third party as in the bank. It describes how to organize, implement and monitor the cyber security requirements between the bank and third parties. In this framework, third parties are defined as providers of information services; outsourcing providers, providers of cloud computing, vendors, suppliers, government agencies, etc.

1) *Contract And Vendor Management:* The bank should define, approve, implement and monitor the necessary cyber security controls within the processes of contract management and vendor management. To ensure that the approved cyber security requirements of the bank are adequately addressed before the contract is signed and compliance with cyber security requirements is monitored and assessed during the life cycle of the contract.

*N. New Technology Adoptions*

The introduction of new technology and application & infrastructure deployment shall be carried out through risk assessment and sign-off process prior to production implementation. Procedures and guidelines are to be developed for new technologies such as cloud computing, social banking, etc.

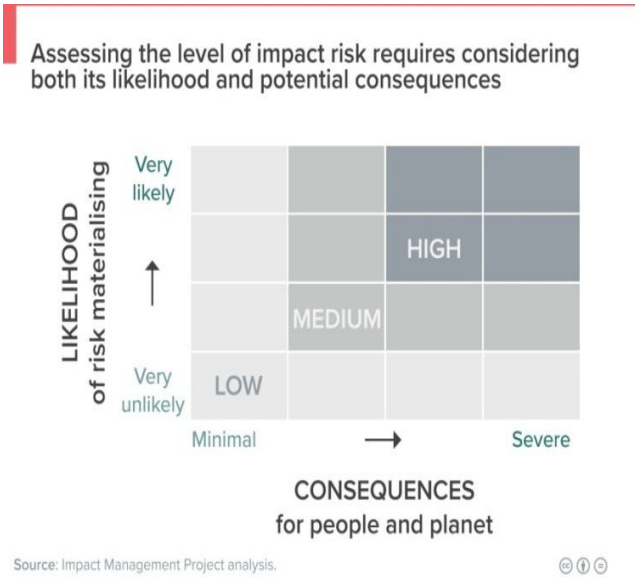
1) *Internet Banking:* It is possible to consider security controls such as multi-factor authentication, strong password creation, adaptive authentication, image authentication, etc.
2) *Mobile Banking:* Mobile applications should be ensured to be up-to-date and tested. The latest standards of hardening could be applied.
3) *Wallet Transactions:* Awareness material should be incorporated on phishing, malware attacks, vishing and social engineering, password security, etc.
4) *ATM Security:* Banks should introduce biometrics such as eye-retina, voice scan or fingerprint scan.
5) *UPI (Unified Payment Interface):* Banks and PSPs need to think through their security strategies, governance models and predictive controls in order to create a secure UPI environment that ensures a seamless user experience while balancing security risks.

©IJRASET: All Rights are Reserved

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177*
*Volume 7 Issue V, May 2019- Available at www.ijraset.com*

## IV. RISK MANAGEMENT

1) *Identify the Risk:* You and your team are uncovering, recognizing and describing risks that may affect your project or its results. There are a number of techniques that you can use to identify project risks. You will start preparing your Project Risk Register during this step.
2) *Analyse the Risk:* Once you identify risks, you determine each risk's likelihood and impact. You develop an understanding of the risk nature and its potential to affect the goals and objectives of the project. This information will also be entered in your Project Risk Register.
3) *Evaluate or Rank the Risk:* By determining the magnitude of risk, which is the combination of probability and consequence, you evaluate or rank the risk. You decide if the risk is acceptable or if it is sufficiently serious to warrant treatment. You will also add these risk rankings to your Project Risk Register.




4) *Treat the Risk:* Also known as Risk Response Planning. You will evaluate your highest ranked risks during this step and establish a plan to treat or modify these risks in order to achieve acceptable levels of risk. How can you minimize the likelihood of negative risks and increase opportunities? In this step, you create strategies for risk mitigation, preventive plans, and contingency plans. And you are adding risk treatment measures to your Project Risk Register for the highest ranking or the most serious risks.
5) *Monitoring And Reviewing The Risk:* This is your step in monitoring, tracking and reviewing your Project Risk Register. Risk is an issue of uncertainty. If you put a framework around this uncertainty, you de-risk your project effectively. And that means that you can move much more confidently to achieve your goals for your project. It is possible to reduce unpleasant surprises and barriers by identifying and managing a comprehensive list of project risks and discovering golden op port units. Also, the risk management process helps to solve problems when they occur because these issues have been planned and plans have already been developed and agreed upon. You avoid impulsive reactions and go into "fire-fighting" mode to correct anticipated problems. This makes project teams and stakeholders happier and less stressed. The end result is to minimize the impact of project threats and capture the occurring opportunities.

## V. INCIDENT MANAGEMENT

The first step of the incident response process is the detection and identification of a suspected incident. Four phases characterize the response process:

1) *Identification*- Recognition, reporting and confirmation of the incident.
2) *Assessment*- Assessment of the incident and assignment of an initial severity rating.
3) *Response*- Appropriate strategy shall be implemented and revised as necessary.
4) *Follow-up*- Damage shall be corrected, vulnerabilities identified and remedied, summary reports shall be prepared.

©IJRASET: All Rights are Reserved

*A. Reporting Information Security Events*

Security events, such as a virus infection, could spread rapidly throughout the bank and cause data loss. All users need to understand that any unforeseen or unusual behaviour on the workstation could potentially be a malfunction of the software. If users are detected an event, they must:

*1)* Note the on-screen symptoms and error messages.
*2)* Disconnect the workstation from the network if an infection is suspected (with IT Support Staff's assistance).
*3)* Do not use removable media (such as USB memory sticks) that may also have been infected.

The Information Services Helpdesk should immediately report all suspected security events. If the information security event relates to paper or hard copy information, such as personal information files that may have been stolen from a filing cabinet, this must be reported to the IT Senior Management for assessment of the impact.

The Information Services Helpdesk will require you to provide additional information that will depend on the nature of the incident. The following information must be provided, however.

*a)* Contact name and number of person reporting the incident.
*b)* The type of data, information or equipment involved.
*c)* Whether the loss of the data puts any person or other data at risk.
*d)* Location of the incident.
*e)* Inventory numbers of any equipment affected.
*f)* Date and time the security incident occurred.
*g)* Location of data or equipment affected.
*h)* Type and circumstances of the incident.

*B. Learning from Information Security Incidents*

Incidents must be recorded and a Post Incident Review conducted to learn from incidents and improve the response process. It is necessary to retain the following details:

*1)* Types of incidents.
*2)* Volumes of incidents and malfunctions.
*3)* Costs incurred during the incidents.

Information Services and any patterns or trends identified must collect and review the information on a regular basis. Any changes to the post-incident review process must be formally noted.

If necessary, the information should be shared with the Warning, Advice and Reporting Point (WARP) to assist the region's alert process.

## VI. FOR CONTINUOUS IMPROVEMENT REFER PDCA CYCLE

The recommended approach for long-term continuous imbalance is still the PDCA cycle, which forms the basis of numerous management systems.

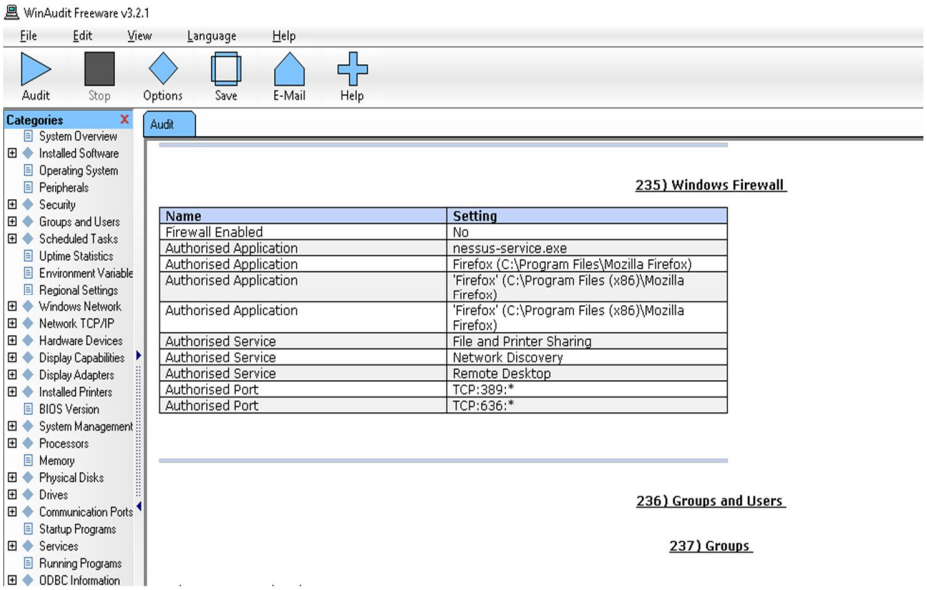
*1) Plan:* Setting control goals and defining who is responsible for ensuring that they are achieved Establish safety measures to achieve control goals and identify the individuals responsible for the operational process behind these measures.
*a)* Defining performance indicators capable of measuring performance against control targets.
*b)* Definition of the performance measurement process, including measurement points, calculation methods and normal and tolerance ranges.
*c)* Definition of corrective measures to keep the safety measure within the normal range.
*2) Do:* Continuous measurement of the achievement of objectives in the implementation of corrective actions provided that defects or non-conformities are identified.
*3) CHECK:* Monitoring of individual safety measurement indicators and comparing individual performance with the objectives of control. Monitoring the countermeasures implemented and the individuals responsible for them if a safety measure exceeds the normal effective range. Drawing up security reports with key management performance indicators based on oversight objectives and safety goals. These reports should include recommendations for action for the management decisions required; they should reinforce security measures that exceed the normal range but remain within tolerance or exceed the threshold values and become ineffective.

©IJRASET: All Rights are Reserved

*4) ACT:* Making the management decisions necessary to restore the effectiveness of security measures or all of the measures ' objectives. Decisions are handed down for implementation to day-to-day operations. Decisions are properly documented (e.g. through security control), including explanations.

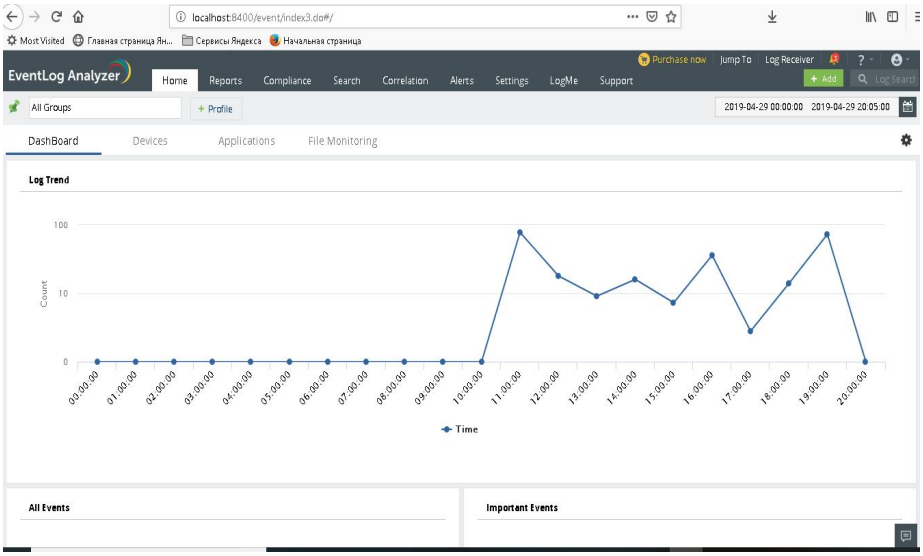
## VII. SOME TOOL USE FOR AUDIT AND SECURITY:

### A. *Win Audit*




Win Audit is a Windows computer inventory tool. It creates a full report on the configuration, hardware and software of a machine. Win Audit is free, open source, and anybody can use or distribute it.

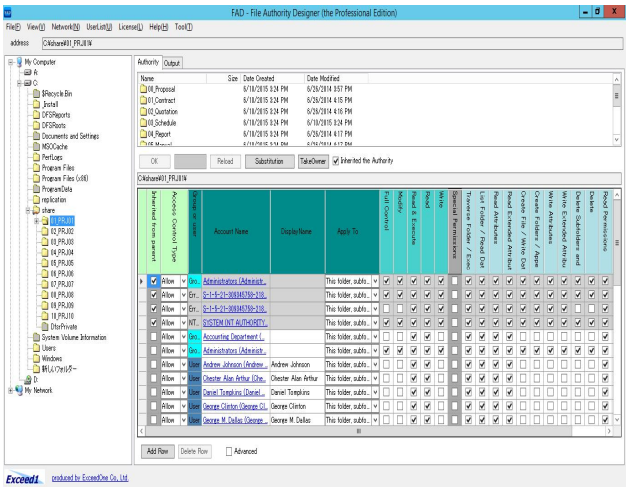
### B. *SIEM (Event Log Analyzer)*




Security information and event management solutions (SIEM) have entered the market to provide security intelligence and automate the IT security management of log data terabytes. SIEM solutions monitor network systems, devices and applications in real time, provide IT professionals with security intelligence to mitigate threats, correlate events, identify the root cause of security incidents, and meet requirements for compliance.

©IJRASET: All Rights are Reserved

*C. FAD (File Access Designer)*




*D. Sequite Endpoint Security*

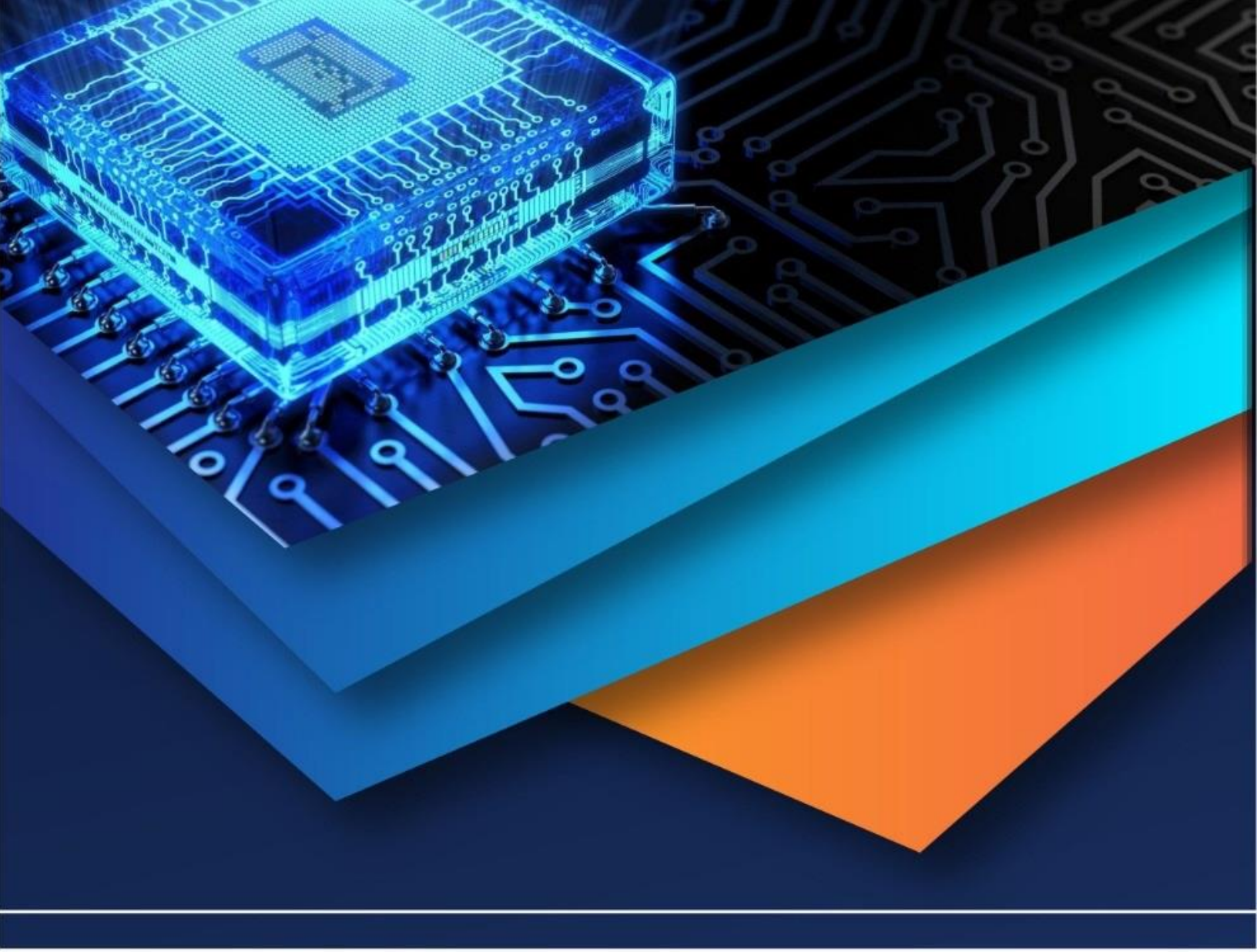

## VIII. CONCLUSION

Some point conclude that is 1) Always lessons learned from security incidents 2) Results of (internal) audits 3) Evaluation by management (management assessment) 4) Bank suggestion program (suggestions for improvement) 5) Risk analyses carried out on a regular basis 6) Performing Audit and VAPT Assessment periodically 7) Maintain clock synchronization 8) For change management using forms and template 9) Maintain Active Directory 10) High Availability for Critical device like firewall11) Always monitoring network traffics and logs etc. that all points are recommended for better security.

## REFREANCES

[1] M. Apata, the Essence of Information System Security and Audit. Retrieved January 2010, from Jidaw.com,http://www.jidaw.com/security1.html
[2] The National Institute of Standards and Technology's (NIST) Special Publication 800-53 provides controls for federal information standard. https://nvd.nist.gov/800-53
[3] Calder, Information Security Based on ISO 27001/ISO 27002 - A Management Guide (2nd ed.), Zaltbommel: Van Haren Publishing, 2009
[4] The Payment Card Industry security council's Data Security Standard https://www.pcisecuritystandards.org/
[5] NSAA and GAO. (2001, December). Management Planning Guide for Information Systems Security Auditing. Retrieved January 2010, from U. S. Government Accountability Office, http://www.gao.gov/special.pubs/mgmtpln.pdf
[6] The Information Systems Audit and Control Association offer the COBIT framework for information security. http://www.isaca.org/COBIT/pages/default.aspx
[7] Networks, 3., Security Audit. Retrieved 2010 February, from Scribd, http://www.scribd.com/doc/12734608/ Security-Network-Audit Steps

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)