Predict | Protect | Prevent

BSP Circular 982

mandates Security Compliance for Banking, Financial Services & Insurance (BFSI) industry in Philippines

arcon

introduction

With the growing menace of IT security hazards, Far East Asian countries turned out to be highly lucrative for information hub. Cyber criminals target every industry in this region, especially Philippines, since it is enriched with sensitive and confidential information. In order to curb any further damage, BSP (Banko Sentral NG Pilipinas) issued Circular 982 on November 2017 to strengthen cyber security policies among the organizations. This has helped the organizations from Philippines to stay compliant to BSP Circular 982.

In this backdrop, BSP Circular 982 closely monitored the massive data breach incident of one of the leading remittance companies in Philippines, in January 2019. This incident affected personal information of more than 9,00,000 people. These information include name, date of birth, personal identification number, email ID, mobile number etc. Few even lost the privacy of their income details which again proved to be fatal in terms of digital security.

which organizations should be complied to bsp circular 982

BSP Circular 982 mandates compliance of every organization from banking and other financial industry in Philippines. BSP normally notifies all the every company from BFSI sector about the effectivity of the Circular with a reasonable timeline. This regulation remains unchanged and effective until further notice by BSP. As mentioned in the circular -

> *“This assessment and classification process of BSP should not preclude BFSIs from assessing their own IT classification on an on-going basis. All BFSIs are required to have periodic and rigorous self-assessment exercises using more robust data sets and variables as part of their information security risk management system.”*

requirements/ standards/ guidelines of this act and how arcon can help

There are several basic requirements the organizations need to follow regarding the standards of BSP Circular 982. Also, it might be an opportunity for the organizations who are looking for the mandates but are not able to justify their role in implementing the guidelines. Let us see how the session acts can make an impact on the overall security of the network atmosphere:

section 2. subsections x177.3 and 4177q.3, 4196s.3, 4177p.3 and 4196n.3

Section 2 of Circular 982 speaks about the several standards that are mandatory for maintaining security standards in any organization from BFSI sector. Let us see the factors that are checked while mitigating insider threats and data breaches:

a] it infrastructure & operations:

The basic IT infrastructure of any organization is highly crucial to assess their IT operations policies and how it can be utilized for maintaining the security of the overall privileged accounts' access policies, their limitations and opportunities.

ARCON | PAM (Privileged Access Management) can provide comprehensive security to the privileged accounts in any enterprise network and mitigate malicious insider threats.

b] digital/ electronic financial products & services

Digital or electronic financial products include bank ATM cards, debit/ credit cards, ATM terminals, Point-of-Sales (POS) terminals, internet banking, mobile banking etc. BFSI industry, mostly banks provide all these facilities and thus invites bigger security risks because of being vulnerable to security threats. Each information in this industry is processed, accessed, transferred and managed through privileged accounts which are always prone to malicious threats.

ARCON | PAM with the help of multi-factor authentication provides complete security to these privileged accounts by validating the user and protect all the confidential financial information from external malefactors and malicious insiders.

c] it projects and initiatives:

The nature of BFSI's IT projects incur severe security risks and complexities. It happens while implementing/ developing/ transforming the existing banking systems into core banking systems in the entire network. This invariably affects the current organization network structure if not taken adequate measures. The risk factor of this transition makes BFSI industry vulnerable to security breaches.

ARCON | PAM nullifies this threat vector with adequate granular level access control mechanism and monitoring the privileged activities happening in the enterprise network.

d] outsourced services:

Outsourcing is one of the most time saving and energy saving formula organizations follow to lower their operations and employee expenses and time required for the work. The responsibility of any work which has been given to some third party expecting timely accomplishment asks for access permission to all the privileged accounts existing in the entire network. As a result, this pose as a huge security threat of the confidential information.

ARCON | PAM with regards to this security postre, have got the mechanisms like user authorization, granular level access control, multi-factor authentication, session monitoring, audit trails etc. in place. These mechanisms ensure that the malicious third party activities are monitored in real-time.

e] threats:

The extent and severity of cyber threats especially in BFSI industry is getting sophisticated day by day. Some organizations are more prone to attacks depending on the size of their digital assets, vastness of customer base and definitely the network infrastructure and systematic importance that can ensure how prepared the organizations are to shield various digital threats.

ARCON | PAM with its innovative and comprehensive technology have made sure that these security worries are kept at bay. Be it a malicious insider, external hacker or even suspicious third party, privileged access management solution monitors every activity and notifies the administrator about any suspicious move.

section 3. subsections x177.5 and 4177.5, 4196s5, 4177p.5 and 4196n.5

Section 3 speaks about the several standards that are mandatory for maintaining security standards of MORB (Manual of Regulations for Bank) and MORBNBF (Manual of Regulations for Bank & Non-bank Financial Institutions). Let us see the factors that are checked while mitigating insider threats and data breaches:

a] apt (advanced persistent threat):

This sophisticated form of attack involves any unauthorized user gaining access to the critical systems of any organization without any specific time frame and exploits their vulnerabilities to steal confidential information.

ARCON | Privileged Access Management (PAM) monitors each user activity in real time and notifies the administrator about any suspicious behaviour. Eventually it stops unauthorized users from accessing privileged accounts in any shared and distributed environment.

b] cyber threats:

This is a deliberate act of any cyber criminal/ hacker to conduct fraudulent transactions, obtain sensitive data illegally, communicate false promises, hacking official enterprise servers/ accounts etc. This normally happens due to unmonitored privileged accounts, absence of adequate security measures to protect official data, no mechanism to check user activities happening in the network etc.

ARCON | PAM does all the activities that is required to protect sensitive and confidential information from being hacked by malicious insiders or tainted third party user. These include user authorization, multi-factor authentication, one admin control, password vaulting, granular access control, session monitoring, text & video logs and customized reporting etc.

c] cyber security:

It is actually the technology or mechanism to secure digital assets from external malefactors or malicious insiders. It happens only when the Anti-Virus software is not updated or Privileged Access Management (PAM) solution that monitors user activities seamlessly, are not in place.

ARCON | PAM mitigates all risks associated to the privileged accounts and prevents the malicious actors from doing any digital damage to the organizations.

d] information security risk management:

The process of analyzing, identifying, assessing, mitigating, monitoring and managing the overall information security risks is known as ISRM (Information Security Risk Management). In order to manage the cyber risk involved in protecting the critical information from hackers or malicious insiders, BFSI and other industries control their risk management system with the help of a robust Privileged Access Management solution.

ARCON | PAM controls the overall user activities happening in the enterprise network with the help of authorization, authentication, virtual grouping, fine grained access control, one-admin control, password vaulting, session monitoring, customized reporting and more. With this, the overall security landscape of the enterprise network receives a complete security vigilance round the clock.

e] threat intelligence:

The process of gathering and analyzing information about the motives, proficiencies and tactics of the malicious actors helps organizations to take preventive measures beforehand and protect their digital assets from external/ internal malefactors.

ARCON | PAM with its enterprise-level risk preventive solutions can offer best possible threat matrix to the administrators and continuously monitor the user activities to detect any erratic behaviour of any employee/ third party and notify the administrator accordingly.

section 4. item 3. a of subsections x177.7 and 4177q.7, 4196s.7, 4177p.7 and 4196n.7

Section 4 speaks of the amendments of MORB (Manual of Regulations for Bank) and MORBNBF (Manual of Regulations for Bank & Non-bank Financial Institutions) which deals with IT Risk Management System (ITRMS):

a] information technology:

In broader terms, Information Technology deals with computing, hardware, software, telecommunications and networks. Today, most of the global organizations have transformed their operations into digitized way, thanks to the global wave of digitization. Many times, it is observed that organizations give least importance to the cyber security aspects leading to information, financial and face loss. Most of the times, this loss is irrecuperable and eventually it leads the organization to take a holistic approach towards evaluating the overall threat landscape.

Among all the industries, BFSI is the most targeted industry by the cyber criminals. This industry holds the treasure of sensitive and confidential information and thus it is always the “most sought after” zone for the cyber crooks. Today, most of the breaches happen due to sophisticated hackers, malicious insiders, unmonitored privileged accounts, inadequate employee knowledge & training and too much of a risk exposure. To rescue, Privileged Access Management (PAM) plays a crucial role in mitigating the risks incurring from the enterprise network structure every now and then.

ARCON is the pioneer of risk management solutions including Privileged Access Management (PAM), User Behaviour Analytics (UBA) and Security Compliance Management (SCM). The management if looking for an integrated and clinical approach towards information security, banks on the overall risk management in IT systems of the entire network infrastructure.

b] information security risk management framework (isrm):

The ISRM framework consists of six major phases which creates the entire cycle of information risk prevention. Let us see how these six steps contribute in organization’s overall security structure:

i. identify

The ISRM cycle starts with identification of information security risks. In this stage, the management identifies the risk factors existing in the network, the security vulnerabilities attached to the IT operations. This helps the organization to assess the risk areas and take immediate necessary steps to mitigate these modern threats.

ii. prevent

There is a say “Prevention is better than Cure.” It goes to the Information Security industry as well. In this stage of the cycle, organizations sit with the security team to discuss about the loopholes in the overall network infrastructure and chalk out threat prevention strategies. The management restructures the organization policies starting from the grassroots level to advanced tools so that the extent of security defense is strengthened.

The prevention mechanism can be categorized into three types. They are:

a) Administrative Controls: It refers to the policies and procedures which articulate organization’s expectations and directions on Information Security. It includes security trainings and awareness programs to stop erratic employee behaviour.

b) Physical & Environmental Controls: It refers to those security controls and measures that are incorporated to protect the physical infrastructure (like data centers) from unauthorized access and other environmental hazards.

c) Technical Controls: It refers to those logical security tools and technologies to maintain confidentiality, integrity and availability of information assets as and when required.

iii. detect

Prevention mechanism alone is never sufficient as far as information security is concerned. Threat detection mechanism should also be in place to find out anomalous activities happening in the network and reducing the scope of malicious threats within the enterprise network.

iv. response

Response refers to the response of any occurance of cyber attack or any incident of compromise that has already affected the digital assets of any organization. With the growing incidents of cyber crime, every organization should develop a comprehensive, updated and apt response plans supported by well-trained administrators, experienced investigators, cyber security experts and forensic data collectors. With the help of adequate response capabilities, the organizations should minimize the impact of any breach incident by investigating on the root cause.

v. recover

The recovery phase is nothing but coming out of the impact of any breach incident happened with the organization assets. It encompasses both the resumption activities and back-up facilities. During the recovery phase, the organization should ensure that information processed with back-up facilities should meet the required level of security.

vi. test

Testing is nothing but checking, re-checking and continuous verification of all the above parameters in regular intervals to ensure everything is in place. Organizations, especially from BFSI sector, need to enhance situational awareness and proactiveness during emergencies so that organizations can actually rely on the team, operational policies and business models. Hence, ISRM can be implemented successfully if appropriate level of layered testing is done to commensurate security needs.

how ARCON can contribute?

ARCON | Privileged Access Management (PAM) suite enables any BFSI organization to overcome all the above mentioned challenges. Trusted by more than 250 enterprise customers across the globe, this highly scalable enterprise-class solution helps in integrating all the IT elements under a single centralized IT policy framework. The solution reinforces an organization's IT operations through real-time monitoring and controlling end user activities around privileged accounts.

security: mitigate threats of unauthorized access

- Strong multi factor authentication
- Robust password vaulting with AES-256 bit encryption to manage, secure, and rotate privileged credentials

efficiency: centralized administration of all privileged activities through one admin control

- The secure gateway server serves as a centralized policy engine to restrict, control and monitor privileges to target devices
- Single-Sign-On (SSO) administrative access to all underlying devices

access control: restriction and elevation of commands to control activities

- The solution enforces deepest levels of granular control over privileged users based on time, day and role of the team
- Privileged Elevation and Delegation Management (PEDM) enables to control and monitor non-admin users having temporary elevated access rights to systems
- Enforces the principle of least privilege

threat alerts: real-time monitoring, recording, and dashboarding of all privileged activities

- Advanced capabilities such as customized reporting, real-time alerts and analytics enables IT security team to improve upon privilege actions and decision making
- Each and every activity performed by end user is captured in a text and video format

c] cyber threat intelligence & collaboration

In the middle of a growing cyber-threat landscape, BFSI industry has been the most targeted sector worldwide. In order to enhance situational awareness and keeping the business models and organizations' IT policies in mind, it is highly imperative to deploy a security solution that can offer seamless monitoring of the privileged accounts and notify the administrators immediately if any suspicious behaviour is detected. This is the only way organizations can ensure information security in the entire network infrastructure.

ARCON | PAM holds the key to protecting the official network from unauthorized access, mitigating malicious threats, offering fine-grained access control for better management of the privileged accounts, monitoring each and every privileged sessions and even generating user report for the administrators. Hence, ARCON can largely contribute in providing robust security to the data assets.

conclusion

In a nutshell, BSP Circular 982 information security standard obtains and monitors the norms associated with the compliance, but the rapid technological advancements happening in Philippines is forcing organizations (especially BFSI sector) to count on robust security solutions a lot. It is strongly recommended that any enterprise in Philippines must comply with BSP Circular 982 compliance and set off for the most recommended security assurance programme. There are organizations that are complied with this regulatory standard by adopting the relevant parts of the standard to secure the data from baseline cyber-attacks. This is how BSP Circular 982 is responsible for the overall progress of Philippine's cyber security, expansion of cyber awareness and creation of a culture that collaborates information security and technological innovation.

arcon

about ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us