SALINAWATI SALEHUDDIN

PROFILE

To contribute to the overall success of a progressive, growth-oriented organization in an entire level position corresponding with my qualifications and job duties. Professional accreditation in a computer-related field.

CONTACT

PHONE:
017-2395600

LINKEDIN:
https://www.linkedin.com/in/salinawati-salehuddin

EMAIL
ezselena@gmail.com

CERTIFICATIONS

- Control Objectives for Information and Related Technology (COBIT)
- Comptia A+
- MCSA
- MCSE 2003
- Kepner-Tregoe
- ITIL V3
- ITIL V2
- CCNA

PUBLICATIONS

- Code of Practice for PDPA - Insurance industry
- Effectiveness of Gap analysis and assessment
- Supply chain solutions for cafe and company owner
- Awareness effectiveness
- Big Data Driving Business - Leveraging Data and Paperless Innovation in Insurance Sector

25 August 2021 until now, Agrobank Malaysia, Leboh Pasar,

AGRO BANK

Project:

1. Acting as CISO
2. Compromise Assessment
3. Cyber Drill Exercise
4. Phishing Drill Exercise
5. SWIFT Attestation
6. Awareness on cyber security
7. Core Banking Ar-Rahnu
8. Threat Intelligence Operations
9. Finance Management Operation applications
10. Disaster Recovery Drills
11. Investigation taskforce

IT Risk Section Head, currently acting as CISO

1. As part of Risk Division with overview of CRO, become one of the taskforce members to investigate the high-risk profiles incident and cases.
2. Identify, assess, and evaluate IT Risk to enable the execution of the enterprise risk management strategy.
3. Identify potential threats and vulnerabilities for business processes, associated data and supporting capabilities to assist in the evaluation of enterprise risk.
4. Identify and evaluate risk response options and provide management with information to enable risk response decisions on IT Risk.
5. Review IT risk responses with the relevant stakeholders for validation of efficiency, effectiveness, and monitoring.
6. Monitor risk and communicate information to the relevant stakeholders

AWARD

Best Employee of the month May 2014 –T-Systems

TRAININGS

CompTIA security plus
EDS, Cyberjaya, Selangor

ITIL V3 Bridging
HP Campus, Cyberjaya, Selangor

Kepner Trego Resolve Workshop
EDS, Cyberjaya, Selangor

ITIL V2 Foundation
EDS Cyberjaya, Selangor

VMware Management Overview
Hewlett Packard GCM Malaysia

Active Directory Administration
Emerio Malaysia: 3rd Flr PNB Building ,
PBD, Malaysia

Ctirix Server Administration
Hewlett Packard GCM Malaysia
Platinum Book Guideline Training

PCA Hong Kong – Korea and Bali

Symantec Cloud Email.
PCA Singapore
Leadership Development Program
Egronomics
PDPA
Jabatan PDP
ASEAN Risk Management
Asia Risk
Neuro Linguistic Program
Awareness Before Change
Innovation thinking

to ensure the continued effectiveness of the enterprise's risk management strategy.

7. To ensure information systems controls is designed and implemented to be in line with the organization's risk appetite and tolerance levels to support business objectives.
8. Identify legal, regulatory, and contractual requirements and organizational policies and standards related to information systems to determine their potential impact on the business objectives.
9. Ensure that all IT policies and procedures are compliant with internal and regulatory requirements.
10. Facilitate the identification of resources (e.g., people, infrastructure, information, architecture) required to implement and operate information systems controls at an optimal level.
11. Serve as liaison to auditors, consultants, and the bank Compliance Committee regarding documentation and review of information compliance.

8 Feb 2019 until 24 August 2021, Alliance Bank, Cap Square

ALLIANCE BANK

Project

1. Cyber Drill
2. Security Critical vendor Assessment
3. Tender Evaluation
4. Awareness on cyber security
5. SWIFT Attestation
6. RMiT gap analysis and assessment
7. Server hardening automation
8. IT asset centralization
9. Identity Access Management
10. Vendors exit evaluation
11. Phishing drill
12. Vendor evaluation
13. PCI-DSS Assessment
14. Cyber Resilience Maturity Assessment

IT Security Policy, Governance and Compliance

a) Manage IS Security processes and functions within the bank/group

- Responsible for the implementation of all aspects of IS security processes and operations, group wide.

PruBSN

AICB training -Charted Bank

Mitre attack framework

Industy Brief - RMIT

Industry Brief – RENTAS and SWIFT

MBSB Bank

TRAININGS

Qualification: COBIT FOUNDATION

Date of Achieved : 2019

Issue Organization: Iverson Sdn Bhd

Qualification: Comptia A+ Certification

Date of Achieved: 2010

Issue Organization : HP Campus, Cyberjaya ,Selangor

Qualification: ITIL V3 Bridging

Date of Achieved: 2010

Issue Organization: HP Campus, Cyberjaya ,Selangor

Qualification: Kepner Trego Resolve Workshop

Date of Achieved: 2010

Issue Organization: EDS, Cyberjaya, Selangor

Qualification: ITIL V2 Foundation

Date of Achieved: 2010

Issue Organization: EDS, Cyberjaya, Selangor

Qualification: Microsoft Certified System Engineer

- Overall management of IS Security policies, standards, and procedures; to carry out maintenance, continuous improvement and ensure compliance requirements are met.
- Managing IS Security vendors on the vendor compliance certification program to assess new and existing vendors through initial contracting, performance of security due diligence and ongoing recertification efforts
- Ensure compliance with regulatory (e.g., BNM, PCI DSS) guidelines on IS Security Management.
- Lead/ assist in the review, analysis, and investigation on IS security incidents.

b) Assist Information Systems Security Management Head in his role.

c) Oversee Security unit by supervising team of security personnel on compliance and governance matters.

- Supervise team members on work in progress and work done (e.g., Incidents and Service request).
- Produce security team management reports e.g., progress report, duty roster, security checks, operational checklist, audit reports.
- Review and update Security documentation/manuals.

d) Preparing PAR, security policies, procedure, framework, and guideline.

e) Manage Security escalations related (e.g., evidence submissions, appliance issue, IS Security Project document submissions, audit evidence submissions etc.).

f) Manage and perform security control review at System level

- Align the project with Group IS Polices, standard & guidelines
- Review Security Requirements Checklist for new projects

g) Engage, with internal audit and control, external audits (e.g., regulators, third party auditor) as required to satisfy any audit related policy and compliance deliverables or work items related to IS Security.

h) Ensure security compliance to ISSP and regulatory requirements e.g., BNM, Bursa, AMLA, etc.

i) Develop, review and update hardening checklist for systems/databases e.g., Windows, AIX,

Unix and Linux, and (Databases) e.g., DB2, Informix, MS SQL, and MySQL.

Date of Achieved: January 2006

Issue Organization: Microsoft

Qualification : Diploma in Computing & Information System (CGPA 3.77)

Date of Achieved : 2005

Issue Organization : College Legenda

Qualification : Certified Cisco Network Associate

Date of Achieved : 2005

Issue Organization : Cisco

Qualification : SPM (Gred 2)

Date of Achieved : 2001

Issue Organization : Malaysia Education Department

j) Prepare and review items for CSA, BNM Operational Risk Integrated Online Network (ORION) and GIS ORM KRI Reporting (Technology) assessment.

k) Provide Security Awareness as proactive initiative promoting enhanced security controls and training across IT and business units.

2 May 2018 until 27 Jan 2019 MBSB Bank, Jalan Dungun

Project

1. RMIT Compliance
2. SWIFT compliance
3. ATM implementation
4. Cash deposit Implementation
5. Cheque Deposit Implementation
6. Converting old conventional account to Islamic account

Information Technology Risk Management (Manager)

- Identify, assess, and evaluate IT Risk to enable the execution of the enterprise risk management strategy.
- Identify potential threats and vulnerabilities for business processes, associated data and supporting capabilities to assist in the evaluation of enterprise risk.
- Identify and evaluate risk response options and provide management with information to enable risk response decisions on IT Risk.
- Review IT risk responses with the relevant stakeholders for validation of efficiency, effectiveness, and monitoring.
- Monitor risk and communicate information to the relevant stakeholders to ensure the continued effectiveness of the enterprise's risk management strategy.
- To ensure information systems controls is designed and implemented to be in line with the organization's risk appetite and tolerance levels to support business objectives.
- Ensure the IT Disaster Recovery Plan including annual reviews are conducted by IT department.
- Identify legal, regulatory, and contractual requirements and organizational policies and standards related to information systems to determine their potential impact on the business objectives.

- Ensure that all IT policies and procedures are compliant with internal and regulatory requirements.
- Facilitate the identification of resources (e.g., people, infrastructure, information, architecture) required to implement and operate information systems controls at an optimal level.
- Serve as liaison to auditors, consultants, and the bank Compliance Committee regarding documentation and review of information compliance.

10 November 2014 until 27 April 2018 PruBSN Berhad, Jalan Sultan Ismail

PRUDENTIAL BSN
TAKAFUL

<u>Project</u>

1. Task Force in developing Code of Practise PDPA for Insurance Industry
2. Developing Information Risk Framework with Group Prudential
3. Data Loss Prevention Implementation and enforcement
4. Data Management Enforcement on insurance wide.
5. Data Analytic and Management Innovations
6. Risk and Security Awareness

Deputy Manager Information Risk Management.

- To act as “second line of defense” on information risks.
- Review the followings in operational effectiveness to mitigate risks to information:
- Access matrices,
- Privileged user ids,
- Technology settings & logs protecting the business,
- Third party contracts,
- Information classification register and processes
- Liaise with CLR team to ensure local regulatory and legal requirements that affect our information are met.
- Coordinate and submit regular reporting to PCA Information Risk:
- UDA Register,
- Sensitive Information transfer register, and
- Incident reporting.
- Providing security authorization for requests from staff for exemptions to standard access.

- Coordinate and report half year Turnbull and end year Governance exemptions related to information risk.
- Coordinate and support completion of PCA led Information Risk reviews and on-site visit programmed as set out in the annual timetable
- Support operational functions as required to manage risks to information appropriately:
- Support to ensure projects take account of risks to information,
- Advice and guidance on information risk issues
- Attend PCA Information Risk annual training conference.
- To keep up to date the Privacy policies and procedures including the breach management policy and to disseminate new rules/regulations on privacy to staff.
- Analyze the types of breaches of Privacy law or regulation within the organization.
- Provide advice on projects, programs, privacy law, relevant legislation and data sharing.
- Conduct audits of data for compliance.
- Consult to Procurement /Vendor management department on Vendor risk assessment.
- Works with legal counsel to ensure the practice/organization has and maintains appropriate privacy and confidentiality consent & authorization forms, information notices and materials reflecting current organization and legal practices and requirements.

16 January 2013 - 1st November 2014 T-Systems Malaysia, CyberJaya

··T··Systems·

<u>Project</u>

1.Developing Risk Management Framework for Dutch Telekom (as one of the task forces from Malaysia Division)

2. Advising on Project Risk for Project team on security controls and risk

    1. Server implementation Upstream and Downstream
    2. SharePoint implementations on Oil and Gas Landscape
    3. Hardware refresh for Data center

Risk Analyst-For Shell Group Account (SGA)

- Perform Security Risk Assessments on Applications / System Enhancements or New Systems/ Applications / Devices introduced into the environment.

- Assist Project manager in review their potential risk and perform risk assessment on the new architectural design.
- Assist SDM/GCDM/SCDM on their highlight on potential Risk in their services. Providing advice and suggestion for their queries.
- Review and provide approval for Risk assessment submission for intended changes to DEV/UAT/Production environment to determine security impact for both businesses.
- Approve Controls, policies, and release of document to clients to the specific accounts.
- Develop any locally required SOPs or IT Security Guidelines and Procedures in line with Policies and Standards.
- Monitoring of Security Logs of High-risk Business Applications.
- Perform Security Configuration Review of servers in IT environment such as Wintel, dbase, AS/400, and network devices.
- Review IT implementation of Patches as advised by Global CIRT and assessment of latest security events impacting company (ad hoc).
- Submit Monthly report & Key Risk Indicators for the month to management.
- Review of IT technology environment to company Policies and Standards and advise management of potential issues /risks.
- Join Project management team in creating ISRM Framework for the Specific Account.
- Assisting Compliance and security in providing risk perspective on Findings and security incidents.

19 December 2011 Until 01 January 2013 ING Insurance Berhad, Jalan Raja Chulan

ING

Information Risk Management Officer

- Perform Security Risk Assessments on Applications / System Enhancements or New Systems/ Applications / Devices introduced into the environment.
- Approve Change Controls Forms for intended changes to DEV/UAT/Production environment to determine security impact.
- Develop any locally required SOPs or IT Security Guidelines and Procedures in line with Policies and Standards.
- Monitoring of Security Logs of High-risk Business Applications.

- Perform Security Configuration Review of servers in IT environment such as Wintel, dbase, AS/400, and network devices.
- Review IT implementation of Patches as advised by Global CIRT and assessment of latest security events impacting company (ad hoc).
- Submit Monthly report & Key Risk Indicators for the month to management.
- Review of IT technology environment to company Policies and Standards and advise management of potential issues /risks.
- Spread security and risk awareness to all ING's staff.

29 November 2010 until 02 December 2012 HP Enterprise, CyberJaya,Selangor

Hewlett Packard
Enterprise

Network Security Analyst (current positioned: Shift lead)

- First line (1st Level) Support of Monitoring and Investigations in GSOC (Global Security Operation Centre)
- Manage reported security Incident via GSOC Hotline for APJ Region
- Logging Security Event Cases into GSOC Dashboard
- Working together with America & EMEA GSOC agents handling security alert of multiple clients
- Perform hands on Security Investigation for Security Event alerts in GSOC dashboard
- Assign DW cases for Respective team for Security Investigations
- Liaising with System, Network & Firewall Administrator for investigations
- Handle, Validate and Investigate Security Events (Intrusions/Malicious Activity/Security Events)
- Review and analyze logs files, system messages, event details, network packets for Investigations
- Manage and follow up cases with Admin/Helpdesk, provide remediation for open cases (Security Event)
- Security Incident Escalations to GSIRT
- Work together with Account Security Officers (ASO) on critical Security Events communications
- Assist GSIRT in incident handling as directed

- Assist in Alert handling process and documentations update
- Assist in Alert Fine Tuning for specific IDS technology and accounts.
- Identify Security Risk base on the current security alert patterns.
- Analyze and provide recommendation for all IDS/IPS Alerts for specific accounts
- Involve in IDS/IPS Management (Specific Accounts)
- Minor Involvement in New Account on boarding task/process
- Managing teammates attendance, standby, Call backs and MC
- Assisting teams in Handling clients and Dealing with New clients
- Send report on the Team Daily BAU to the Manager.

29 September 2008 until 28 November 2010 EDS, CyberJaya,Selangor

Hewlett Packard
Enterprise

Information Security Analyst

- Responsible for the administration and enforcement of IT Security Policies, Procedures, Standards and Codes for Logical Access
- Ensure all documentation up to date in conjunction of the latest IT Security Policies, Procedures, Standards and Codes for Logical Access
- Manages plans and administers the operational and administrative activities associated with the running of the IT security section.
- Develops, implements security standards, procedures and guidelines for Application platforms and diverse systems environments.
- Maintain and control Security Officer and critical ID’s passwords.
- Work with other technical infrastructure team members for daily operations and support of IT systems and security.
- Responsible to analyze security issues, determine the root cause and impact and identify the corrective action needed to eliminate and prevent the event for the future.
- Ensure that the confidentiality, integrity, and availability of company’s information assets are protected.
- Generate User Listing, Access Matrix, and Audit trails.

- Monitor every activity and retrieval of critical IDs password in the system to ensure action had been authorized by Data Owner/Line Manager.
- Liaising with Data Owner and Line Manager as regards of issues, security policies, procedures, best practices, and escalation if there is any detected in the system.

2006 to 28 September 2008 Hewlett-Packard, Bkt.Damansara

Hewlett Packard
Enterprise

First Level Technical Support

- Supporting Platform from Windows NT4, 2000 and 2003
- Supporting and maintaining Windows servers operations around the world
- Responsible for troubleshooting the network and all supporting server
- Monitor and maintained Windows server backup, Hardware, important application system that running on the server
- Responded to Remedy, OVSD, and Clarify tickets.
- Trouble shooting by remote distance using VNC, PC anywhere, Remote desktop, VM ware and via Citrix meta-frame
- Responsible to monitor, maintain backup using Arc Server and Data Protector
- Responsible to create, maintain and modify user in Active Directory
- Responsible for troubleshooting and maintain all the shared drive and network printer.
- Responsible to monitor the SQL, MS access Database.
- Monitoring patching on server windows