Resume

SUNANDITA GANGULY

Bangalore - 560068
Mobile - 08884129666
e-mail : Sunandita.ganguly@gmail.com
Linkedin: https://www.linkedin.com/in/sunandita-ganguly-628604a/

A passionate Security professional, I have overall **21 yea**rs of experience in IT and more than **15 years** of work experience (**7+ years** of Security leadership) in Information / Cyber Security's multiple domains such as Governance, Risk Compliance (GRC), Vulnerability Assessment (VA), Application Security, SOC Operations, Security Incident Management (SIRT), Data Privacy (GDPR, HIPPA-Hi-Tech, CCPA, FASMA) catering to multiple customers' security & Business Continuity Management (BCM) requirements across BFSI or Banking Financial Insurance, Manufacturing, Consumers, Energy etc. I have substantial experience in building various security teams (above mentioned) from scratch and transforming businesses and have managed both internal and external stake holders. I have been part of and actively participated in defining and shaping the security postures, strategy and policies for some of the organizations. I have been part of acquisitions and have single handedly worked towards merger and transformation of 2 organizations' security practices post acquisition / merger. As security consultant have provided viable security solutions to various customers, working with various industries, security domains. I have always kept myself relevant in the domain through self education as well as choosing opportunities and accepting new challenges to help in enhancing my domain knowledge, expertise and experience. Looking back at my career in Information / Cyber Security and BCP-DR, I consider myself as a flexible, self starting individual whose quest for domain knowledge is insatiable.

Information / Cyber Security / BCP Work Experience:

Organization Names	From	To	Designation
Freelance Consultant	April, 2023	Till Date	Freelance Cyber Security Consultant
EagleView - APMSE Software Services Private Limited	July, 2020	February, 2023	Associate Director
Wipro Limited (Technologies)	Oct, 2016	July, 2020	Manager
CGI Information Systems and Management Consultants	Nov, 2011	Oct, 2015	Associate Consultant
Accenture India Services Pvt. Limited	Oct, 2003	Feb, 2011	BCP & Information Security Lead

Skills

- Information & Cyber security
- Security Leadership
- Business Continuity
- Security Assessments
- Governance, Risk and Compliance
- Threat Modelling
- Application Security
- Risk Management
- Disaster Mitigation & Response
- Vulnerability Assessments
- Cloud Security
- Vendor Risk Management
- Customer Assessments, RFPs, RFIs
- DLP deployment

- Security Incident Management
- Security Audits (Internal & External)
- Knowledge of GDPR, CCPA, HIPAA-HiTech

Tools

SIEM / SOAR – Azure Sentinel, QRadar
EDR / XDR – Microsoft Defender, Sentinel One
VA – Nessus, Rapid 7, Qualys Guard Nmap
DLP – McAfee DLP Suit
SAST – Checkmarx, SonarQube
DAST – Burp Suite Pro / Enterprise
SCA – Fortify, CheckMarx
PAM / IAM – CyberArc, Thycotic
Mail Filters / DMARC – Mimecast, MS O365
SSO – Okta 2.0
GRC - ZenGRC

Significant relevant experience & achievements:

As an Information Security & Cyber Security professional:

Cyber Security Leadership:

- As part of CIO leadership team, created organization level / location level Cyber Security Quarterly / Annual roadmaps and budgets (on existing allocated budgets as well as proposed additional budgets.) Have worked on team budgets as well as business cases for proposed annual budgets, interim budgets for additional resource requirements, domain related external trainings, expenses relating to security communications etc.

- Worked as CIO's advisor for Cyber Security and accordingly created the Cyber Security Roadmaps, initiatives, value adds, deliverables for presentations for Board.

- As part and head of Risk Steering Committee was instrumental in identifying the initial participants of the Committee as well as the Risk Board. Have driven the committee and presented to the board the comprehensive identified risks along with the analysis and impact. Helped and advised the management in determining the acceptable risk appetite and subsequently with the remediation / risk acceptance plan both at organizational level as well as at the regional levels.

- As part of Global Security Steering Committee, have been part of the organizational decisions / postures / definitions to be implemented at the organizational levels.

- Lead large Cyber Security teams across the sub-domains such as GRC, Application Security, Vulnerability Assessment, Pen Tests, Security Engineering and establishing the functionalities at BU and Org levels.

- Built Security organization / teams from scratch. Worked on budget approvals with business justification for hire, backed by road map projections of the security programs essential for organization and customer requirements.

- As a result oriented leader, have been managing both internal and external stakeholders for championing and defining security postures, policies and clauses (contractual) at the organizational and customer levels.

- Kept a tab on the new security developments and aligned them with organizational security and customer security requirements. In this regard helped / guided the team in developing the Secured SDLC program referencing latest OWASP guidelines, introducing ASVS, the Vulnerability Assessment remediation program.

- Have led, managed and implemented end-to-end ISO 27001:2013 and ISO27001:2005 standards and external and internal audits. Played a pivotal role in transition from ISO27001:2005 to ISO27001:20013.

- Worked as COE or Center of Excellence for Cyber Security and been part of defining the security postures for organizations. Represented organization's security framework and offerings to the existing and prospective customers for new and extension of businesses.

- Collaborated with internal teams such as Engineering, IT, Cloud Operations, Network for new security initiatives and implementation of security controls, processes, measures namely for DevSecOps, Risk Management, GDPR, DMARC, ASVS

- Helped organization in establishing the **Risk Management Committee.**

- Have single handedly designed and developed Security communication plan, calendars. Have worked closely with the communication teams in developing Security related contents.

- Have groomed, mentored, assessed and managed teams of security managers, Engineers and associates.

- Part of **Change Advisory Board (CAB)** responsible for assessing and overseeing risks associated with new change requests and security approval for the same.

- Worked with 3rd Party vendors (MSSP, external VAPT, ISO 27001, App Sec Pen Tests, Security tools) on the contractual and pricing clauses. Also, for renewal of the contracts by assessing the performance and value-adds provided by the existing vendors and comparing them with their competitors.

Governance Risk and Compliance (GRC)

- Have designed, created and updated ISMS policies, standards and procedural documents as per organizational changes and standard's requirements. Updated the existing ISMS documents after reviewing the same with the respective stakeholders.

- Have helped organizations in establishing the Risk Charter as well as establishing the Risk Management Committee. Have done risk assessments at the organization as well as at the account level with 360-degree approach, which takes care of infrastructure architecture review, Vulnerability assessment, Incidents, Backup and Information security controls for ensuring secure data input, processing and output

- Have worked on several Request for Proposals (RFPs) and participated in successful new bids. Worked closely with other stakeholders, namely, IT, HR and Admin-Facilities to ensure all security requirements are responded appropriately.

- Have participated in the review of the information security and business continuity sections of the draft MSAs.
    - Have reviewed and validated security controls of new Master Service Agreements (MSA) documents before they are enforced.

- Have worked on understanding of client security requirements and implementation of the required controls in conjunction with respective stakeholders. Have participated in due diligence client audits.

- Have single handedly managed end to end customer security audits. Have driven (preparation of the audits with the internal teams) all customer security audits of all business units and ensured successful completion of client audits.

- Have supported and participated in SSAE 16 / SSAE 18 (SOC1 & SOC 2) Type 1 and Type 2 audits at the organizational level.

- Have implemented and participated in successful implementation of PCI-DSS assessment for 2 of the accounts with PCI-DSS requirements.

- Have driven risk governance with the respective stakeholders for addressing of the identified high risks and building business justifications and cases for implementation and budget approval of new controls. Have worked on the preparation of mitigation plan and implementation of the same.

- Developed and designed the security exception request process and was responsible for overall security exception request processing and implementation.

- Have managed internal security audits. Have designed the internal audit checklist and control test procedural document. Was escalation level for all internal security audits for the team.
    - Groomed, mentored and trained team members on the security audits aspects.

Application Security

- Responsible for establishing the Application Security team from the scratch, including evaluation of tools.

- Participated in the POCs of SAST / DAST / SCA tools and evaluated them before on-boarding.

- Worked with Engineering and Ops teams to ensure 100% integration of the repos with the SAST tools.

- Worked in close conjunction with both the Engineering Ops as well as Cloud Ops teams to understand the CI/CD pipeline, PI Planning and upcoming releases for building a strategic plan / calendar for testing before each release.

- Defined the application release clauses. Provided security sign-offs / approvals for every applications ready for release based on the internal security pen tests performed and assessment of other defined security metrics.

- Defined the remediation process in-line with CVSS framework. Worked with the Engineering teams for agreement on stipulated timelines for remediation of identified vulnerabilities.

- Mentored the teams in developing Secured SDLC practices and the SDLC program.

- Mentored the team on the internal security trainings to be conducted for the internal teams.

- Mentored the team in defining the team threat modelling program.

- As part of DevSecOps Core Committee team, significantly contributed in formulating DevSecOps strategy plans.

- Worked with 3rd Party vendors in defining the VAPT scope for external tests, remediation plans with the internal respective teams for reported vulnerabilities.

Infrastructure / Security Engineering / Vulnerability Assessments

- Evaluated new SIEM / SOAR solutions and implementation of the same. Worked closely with SOC or Security Operations Center for analyzing and remediation of incidents.

- Defined the Patch Management program at organization level.

- Participating in evaluation of RED and PURPLE team exercises conducted by MSSP vendors.

- Responsible for establishing Vulnerability Assessment Program at the organization level, including the establishment of the team, framework and remediation program.

- Onboarded Thycotic PAM tool for Privilege Access Management. Headed a team of Security Engineers managing the PAM tools, Thycotic and CyberArk, secret vaults, privilege accesses at the organization level.

- Onboarded Mimecast tool in collaboration with the IT team. In conjunction with the IT Systems team defined Sender Policy Framework (SPF), whitelisting of the domains to be included. Defined the DMARC rules for unauthorized / unauthenticated mails.

Disaster Recovery & Business Continuity (DR-BCP)

- Have worked on developing the BCP – Disaster Recovery related documents at the organization level and other BCP related activities in helping developing Business Impact Analysis (BIA), BCP tests and project level BCP documents. Helped the IT team in drafting the ITDR document.

- Have actively participated in managing crisis situation and planning for invocation and managing of a BCP event with other relevant stake holders.

- Worked on Internal and External (Customer) communication during invocation of BCP.

- Drafted the Crisis Management Plan and helped in building the Crisis Management Committee.

- In conjunction with IT head helped in development of ITDR (IT Disaster Recovery) documents both at the organizational level as well as at site (India) levels.

- Laid out the Risk Management program for Assessment and Management of BCP related risks and remediation plan for the same.

I had taken a brief career break till April, 2023 and from May, 2023 onwards have been working as a freelance security consultant & trainer, pursuing Cloud Security / Cloud Security Architecture related certifications and self-learning to keep myself upraised on the current Security landscape.

Freelance Cyber Security & BCP Consultant
Period: April, 2023 – Till Date
Role: On a freelance capacity in collaboration with certain organization providing the following
Security trainings
Consultancy on GRC solutions / Tools POC & Implementation
Information Security / Cyber Security Risk Advisor, Assessor
ISO27001:2013 Implementation consultant
Security Auditor
Security Architectural consultations for some of the Startups & BFSI customers.
BCP Implementation Consultancy

EagleView - APMSE Software Services Private Limited
Period: July, 2020 – February, 2023
Designation: Associate Director for Global Cyber Security & Risk Management
Role: Head of Cyber Security & Risk Governance and Management (Globally, reporting into **CIO**)

Previously: Started as Global Cyber Security Manager, however, with sudden departure of designated CISO had picked up all the responsibilities and have delivered successfully since August, 2021 and hence was promoted to Associate Director for Global Cyber Security & Risk Management in April, 2022.

- Managing a team of Cyber Security Engineers and GRC Analysts responsible for Network Security, Application Security, Vulnerability Management, Penetration Testing and overall Risk and Regulatory Compliances.

- Have worked on Agile based PI (Program Increment) planning to lay down and track security projects. Worked on the sprints for all the security towers along with team PMO to ensure the quarterly / annual projections are created to be presented to the Board and Executive Leadership Team.

- Responsible for security sign-offs / approvals for every applications ready for release based on the internal security pen tests performed and assessment of other defined security metrics.

- Responsible for revamping as well as drafting of security related policies, procedures, standards, guidelines and overall management of ISMS or Information Security Management System at the Enterprise Level and in line with NIST Security Framework, NIST 800, CIS Framework and ISO27001:2013.

- As the GRC head of the organization, responsible for heading the Risk Management Committee and overall Risk Assessments, management, remediation / treatment and management assertion and presentation of the overall Risk Management program at the Enterprise level.

- Responsible for Vendor Risk Management, 3rd Party vendors audits and assessment of the questionnaires submitted by Vendors.

- Work in conjunction with the legal and pre-sales team on the drafting of Master Service Agreements for the new customers as well as for renewal of the existing contracts.

- As part of DevSecOps Core Committee team, significantly contributed in formulating DevSecOps strategy plans.

- Responsible for the assessment of the GRC tools and complete end to end implementation of it from the scratch in conjunction with the US tool vendors.

- Responsible for evaluation of new SIEM /SOAR solution and implementation of the same.

- Responsible for establishing Vulnerability Assessment Program at the organization level, including the establishment of the team, framework and remediation program.

- Responsible for establishing the Application Security team from the scratch, including evaluation of tools.

- Responsible for evaluation of Vulnerability Assessment (Scanning tools) and Application Security (DAST / SAST / SCA) tools before they are onboarded.

- Responsible for the SOC 2 Type II & ISO27001:2013 assessments at the organizational level.

- Part of Change Advisory Board (CAB) responsible for assessing and overseeing risks associating with new change requests and security approval for the same.

- Responsible for establishing and running the DR-BCP program at the enterprise level.

- Responsible for creation of overall Security roadmap and accordingly projections of security budget, drafting calculations and management for the organization.

Wipro Technologies

Period: October 2016 – July, 2020
Designation: Manager
Role: Cyber Security & Risk Consultant for Wipro Technologies

- Have been working in different business verticals as a Security Consultant, catering to the customer requirements.

- Have single handedly assisted the accounts in driving SOC 1 & 2 Type II audits, with GDPR implementations at the organization and accounts level.

- As part of Enterprise Risk Management team, had worked as a core member of the GDPR implementation team at the enterprise level in defining and designing the Wipro's GDPR approach in close conjunction with the legal and other relevant stakeholders.

- For 2 of the US accounts worked as Security Transition leads in transitioning the security requirements.

- Implemented Digital Certification Management for one of the Canadian accounts at the client locations.

- Managed BCP DR for one of the largest infrastructure accounts.

- Worked with the Central team on ISO 27001:2013 implementations.

CGI Information Systems and Management Consultants

Period: November, 2011 – October, 2016
Designation: Associate Consultant
Role: Information Security and BCP Manager & Global Data Protection Officer for some of the Financial Engagements

- Responsible and in charge of overall Information Security and BCP related activities across Bangalore, Mumbai, Chennai and Hyderabad and Data Protection related activities in the financial accounts.
- As designated Deputy Business Unit Security Officer, responsible for managing the client audits, ISO 27001 audit and coordinating between the various stake holders and departments to ensure successful completion of all client, internal and external audits across the India locations.
- Responsible for updating and reviewing security / BCP related organization's existing policies and procedures and creation of the policies and procedures as and when required.
- Coordinate with the corporate team and implement the Information Security and BCP related directives at the India Global Delivery Center level.
- Have single handedly revamped the existing BCP framework.
- From the Information Security and Business Continuity aspects, responsible for leading CGI-Logica integration related activities.
- Responsible for overall incident management process.
- Responsible for reviewing the Risk Assessments, GAP Analysis performed by the team.
- Work in conjunction with the CGI Corporate Security team in reviewing the global policies and procedures, e-Learning tutorials, Global Risk and GAP assessments, maintenance of the India Business Unit's score cards.
- Participated in implementation and preparedness of the ISO27001:2005 audit for one of the external business unit as consultant from India Business Unit.
- Played a pivotal role in documents transition and control mapping from the old standard, ISO27001:2005 to ISO27001:2013 and lead the team in this activity.
- Manage a team comprising of Sr. Associates and Lead Analysts across India. Responsible for their career progression, appraisals, mentoring and grooming.
- Responsible for overall Enterprise Security related communication across the organization.
- Responsible for responding to new bids or Request for Proposals (RFP) from Security perspective. Also, responsible for validation of Security related schedules and controls of Master Service Agreements (MSA) as per the respective RFPs before or during the signing of the contracts.

Accenture India Services Pvt. Limited

Period: October, 2003 – February, 2011
Designation: BCP & Information Security Center Lead for Accenture's NCR Centers / Region

I joined Accenture as an associate and was promoted as Sr. Software Engineer in May, 2004 and was again promoted as Quality Team Lead in April, 2006. In November, 2006 I got promoted to my last role as information Security and BCP sites lead for Noida and Gurgaon centers of Accenture.

Profile: Risk & Compliance Management (Information Security & BCP)

Responsibilities in BCP

- Managing and accountable for the BCP for accounts across Accenture Bangalore, Mumbai and Noida.

- Sole in charge of BCP and Information Security for Accenture Noida Centers.
- Conducting annual BCP mock drills / tests for the deals to check BCP readiness.
- Preparing annual BCP test plans after discussing and coordinating with the deal BCP SPOCs and IT Account Managers. Sharing the same plan with the Service Delivery Leads of the deals.
- Publishing the test reports after the tests are conducted to the Ops team and to Client in case requested. Work in conjunction with the IT Account Managers in setting the target dates for closure of test open items and ensuring closure of the same.
- Procuring seats across locations and cities for conducting tests. Responsible for maintenance of the Annual BCP test Calendar for India Location.
- Reviewing and updating the BCP documents like Business Impact Analysis, Strategy and Business Recovery Plan with deal SPOC and IT account Manager annually and as required.
- Reviewing the CPP or Capacity Plan document and updating the BCP documents accordingly. Participating in CPP sign offs for the existing as well as new deals / accounts. Understanding the Impact Analysis and other requirements from the transition teams or operations, depending on whether new or existing deals and updating the BCP documents (BIA, Strategy and BRP) and working in tandem with operations, transition and IT Account Management Team.
- Updating the risk logs for the deals / accounts after identifying, discussing and receiving acceptance from the deals' management.
- During BCP situation / occurrence of any severe crisis, closely monitoring the situation, take an hourly stock of incident and publishing the same to different stake holders. Working in tandem with F&S, Global Asset Protection Team, Operations and other LMT teams during the crisis. Preparing the incident report after the incident.
- Attending the center's BCP / Crisis Management calls with the other stake holders like operations, IT, F&S and help in formulating plans.
- Preparing the seat mapping, disaster incidents and global dashboard reports.
- Conducting the bi-annual BRT or Business Recovery Trainings for the critical users of different account.
- Schedule and publish the BCP calendar.
- Conducting the overview training sessions on BCP and Information Security for new joiners in inductions.
- Updating BCP training decks as per quarterly Global BCP call's updates received.
- Preparing and maintenance of the BCP test calendar centrally.
- Actively participated in BS25999 audit.

Responsibilities in Information Security

- Responsible for the Noida Centers' Information Security. Spreading information security awareness among the teams in the Center.
- Implementation of ISO 27001 controls and trainings to the project nominated SPOCs of the new processes and deals. Monitoring adherence to the ISO 27001 defined controls and procedures and client defined contractual controls as agreed in the contracts. Weekly / monthly meetings with SPOCs to check on the overall deal / process status.
- Attending the client's security audits.

- Conducting internal audits as per ISO 27001 standards. Preparing CAPA or Corrective Actions and Preventive Actions and sharing the finding & results of the audit with the Service Delivery Leads of the accounts.

- Conducting governance calls with the Service Delivery Leads and SPOCs for closure of the risks from various Vulnerability Assessments, Risk Assessments or internal audits.

- Reviewing client contracts and preparing the audit check lists and mitigating controls accordingly.

- Processing the exception requests to imposed controls from different deals and identifying and implementing mitigating controls for the risks associated with the exception requests.

- Processing business cases. Preparing the risk plan associated with the business case.

- Conducting Vulnerability Assessments on the deals. Presenting the assessment results to the Service Delivery Lead.

- Preparing the risk logs after CPP or Capacity Planning document review. Working in conjunction with the transition teams to identify the probable risks associated with the process during the transition phase and closure of the same.

- Completing the Asset Identification sheets and ISO Project Questionnaire with the help of nominated deal SPOCs. Preparing risk related documents of the deals & centers like Risk Assessment and Threat Vulnerability Controls with different stake holders.

- Preparing of Dash board and Random Floor Walk Reports and presenting the same to the Service Delivery Operations Center Lead.

- Actively participate in ISO27001 audits.

- Risk Assessment on Client Data Protection

Achievements

Was part of successful audit of ISO27001 recertification for Accenture BPO.

Was part of successful audit of BS25999 recertification for Accenture BPO.

Joint Patent holder for Call center application data and interoperation architecture for a telecommunication service center.

Read more: http://www.faqs.org/patents/app/20090175436#ixzz0yRe19W5o

MSource (India) Services Pvt. Limited
Period : August 2002 – August 2003
Designation : Sr. Customer Service Executive

Oceanus Creative Technology
Period: May, 2001 – March, 2002
Designation: Senior Programmer

Educational Qualifications :

Honors Graduate from University of Calcutta in 1998

Certifications

I. ISO27001: 2005 Lead Auditor and Implementer

II. Certified Information Systems Auditor (CISA)
III. Certified Information Systems Security Professional (CISSP)
IV. *Certified Payment Card Industry Security Implementer (CPISI)* for PCI DSS Version 3.0
V. *ISO27001: 2013 Lead Implementer*
VI. *Microsoft Certified Systems Engineer (MCSE)*
VII. *Pursuing CRISC, CCSK, CCSP*

Microsoft Certified Professional :

- C++ and Object Oriented Programming in Microsoft Foundation Class
- Microsoft SQL Server 6.5
- Network Essentials