IT Security Analyst IT Security Analyst IT Security Analyst - Kennametal Inc Having 4.3 years of overall experience in maintenance of SAP security for various environments like R/3, ECC 6.0, BI, HR & Governance Risk and Compliance (GRC 10.1) Experienced in the areas of User administration, Role management, development, troubleshooting, testing and reports generation in Security environment. Developed and maintained authorization process design and related documentation for SAP. Experience in working independently. Experience in facing the client. Experience in managing team if required with full responsibility of maintaining high level of Response & Resolution SLA for the client. Excellent communication, interpersonal, leadership, Documentation, troubleshooting skills and flexible and ability to work in a team environment. Work Experience IT Security Analyst Kennametal Inc - Latrobe, PA February 2016 to Present area. Global Headquarters is located in Latrobe, PA. Kennametal delivers productivity to customers seeking peak performance in demanding environments by providing innovative custom and standard wear-resistant solutions. This proven productivity is enabled through our advanced materials sciences and application knowledge. Kennametal's portfolio of well-respected brand names and broad global presence enable us to help customers of all sizes in virtually every geography drive success at every stage of their value chain. Strategically aligned across our two core businesses - Industrial and Infrastructure - our products and services touch nearly every manufacturing process. People around the globe can see and touch these results throughout many aspects of their day, from the light switch they turn on to the car they drive. Responsibilities: Role modification as of business requirement. Trouble shooting access issue's for support and business users. Working on SAP Go-Live projects for new countries. Worked on SAP VB Scripting. Supporting on calls and flexible to work in rotational shifts. Administered Central User management (CUA) for non-production and Production system. Performed Client Open/Close activities on production environment based on business requirement. Working on Solution manager 7.1 Working on Fire Call (FF) access set ups Working on transport requests Working on user administration Working knowledge on ECC, BI, SRM, CRM Security Working knowledge on Active Directory Administration Provided support during monthly SAP maintenance activities. Working on OSS

Administration which includes OSS ID set up, OSS Connection open, and Access key management & Developer Key management. Working on MII Security. Working on Konnect application security. Working on Enterprise portal administration (User/Role) Working on Hitachi Password Management tool. Assigning PD profiles to the positions and user id's as per the org structure. Role Administration and ongoing maintenance. Analyzing the UAR log and taking necessary action on unwanted user accounts. Performing risk analysis for the roles to validate roles are risk free. Handling new business requirements and coordinating with functional teams for unit level and integration level testing. Documenting the procedural guidelines which are relevant to security. Tracking authorization issues using ticketing tool. Sending status reports to management on weekly basis. Performing cleanup activity on scheduled basis. Providing emergency access to the users. Generating emergency access log. Project Contribution: Configured and Implemented GRC Access Control Suite 5.3 GRC implementation; automation; upgrade experience with GRC RAR, CUP, ERM, SPM and SAP CUA (Central User Administration) integration with SAP GRC. Excellent knowledge of SOX, Audit issues and Segregation of Duties (SOD) issues. Under Risk Analysis and Remediation, performed User & Role analysis to identify existing SOD violations risks. Using RAR produced Analytical Reports on User, User Groups, Roles and Profiles. Analysis reports provide real-time data and Management reports retain an offline history of SOD status. Performed remediation and mitigation against various risks associated with roles and users. RAR has Simulation features to allow you to assess the impact of potential remediation activities on the reported conflicts prior to making the actual change. Experience in creating and assigning FF ID's and extracting Fire Fighter logs. A firefighter ID is a temporary user ID that grants the user exception-based, yet regulated, access. The firefighter ID is created by a system administrator and assigned to users who need to perform tasks in emergency or extraordinary situations. Configured distribution list in CUP, by creating an LDAP connector, created distribution group and add DL group to DL Approvers. Created distribution list users in LDAP and UME, assigned distribution list to Roles. Configuring and troubleshooting of HR triggers in CUP Created SAP HR Connector, HR Triggers, Field Mapping. Configured Workflow, actions

and rules. Configured HR trigger provisioning and scheduled background jobs. Configured User Data source and defined authentication system for requestors using CUP Strong capability in using CUP to use the work flow functionality to ensure a comprehensive and compliant change management process for risk control and maintenance. Experience in using CUP to configure workflow for User Access Review and User SoD Review. Setting up role creation methodology, condition group and role approvers using ERM. Skilled in using ERM to configure an approval workflow for role maintenance in Workflow Engine. Successfully measured the system for SAP License audit 2010. Tracing the functionality after development phase and then designing the Roles/Composites, following SOD analysis and approval process to meet the timely deadlines. HANA Security: Configured Standard, Technical and Restricted Users. Created Roles for Developers, End User and Database Users. Worked on Schema/Object level Privilege access. Worked on System, Object, Analytic and Package Privileges. Knowledge in SAP HANA Studio. CRM Security: Developed the Security design for CRM 7.0 Worked with the CRM functional team to outline security requirements around several CRM services Created OSS Ids, maintained OSS Connections and OSS accounts. Set up CRM 7.0 security for Marketing and Campaign Management, Business Partner Security, E-commerce (Internet Sales) and Product Security Worked with functional analysts in developing CRM security in accordance to CRM Business Role requirements and assigning PFCG roles to business roles. Extensively used CRMD_UI_ROLE_PREPARE report to generate the necessary UIU_COMP settings corresponding to the CRM business role. MII Security: Worked on creating MII Active directory LDAP groups. Working on creating MII Production users. Working on crating MII Production Operators on MII portal and assigning MII portal roles to the users. Project -2 Client Power Mech Projects. SAP Security Consultant Power Mech Projects Ltd. June 2013 to January 2016 Client Description: Power Mech Projects Limited is an engineering and construction company providing versatile and comprehensive services in power and infrastructure industries. Power Mech Projects Ltd was established in the year 1999 with a vision in outlook and passion in approach to create one of the leading power infra companies. Today Power Mech stands tall among contemporary players in the

installation of power projects as a comprehensive service provider with over 8500 direct and 40, 000 indirect employees. The core activities of the Company include three major business lines: Erection, Testing and Commissioning of BTG and BOP, Operation and Maintenance, renovation and modernization of power plants and civil works. The company has undertaken projects of all types, sizes and in all environments in India and abroad which include Ultra Mega Power Projects, Super Critical Thermal Power Projects, Sub Critical Power Projects, Heat Recovery Steam Generator, Waste Heat Recovery Steam Generator, Circulating Fluidized Bed Combustion Steam Generator, Gas Turbine Generator, Hydro Electric Plants, maintenance, renovation, modernization and annual maintenance of running plants and complete civil works. Roles and Responsibility: User Administration activities. Mass locking and unlocking of users while doing special activities. Created LSMW/CATT scripts for user creation and password resets. Assigning PD profiles to the positions and user id's as per the org structure. Role Administration and ongoing maintenance. Maintaining authorization objects to custom transactions as per the business requirement. Configuring SU24 for custom transactions as per the business requirement. Involved in annual User Access Review. Analyzing the UAR log and taking necessary action on unwanted user accounts. Performing risk analysis for the roles to validate roles are risk free. Taking necessary action on identified risk by coordinating with the Security SME from the client end. Downloading authorization objects & texts from the backend systems. Uploading Authorization objects into RAR. Updating functions & generating rules as per the requirement. Updating Rule set as per the requirement. Troubleshooting authorization issues. Handling new business requirements and coordinating with functional teams for unit level and integration level testing. Working on Audit reports. Mass user administration using SU10. Documenting the procedural guidelines which are relevant to security. Tracking authorization issues using ticketing tool. Sending status reports to management on weekly basis. Performing cleanup activity on scheduled basis. Providing emergency access to the users. Generating emergency access log. Responsible for providing support to IT Users and Business users in their day to day issues. Implemented Structural Authorizations for HR Created Batch User ids and Roles to give Batch Access to specific users

Created and maintained Training user ids Configuring SU24 to make sure objects have only maintained and standard state in PFCG Securing critical Spool request through (S_SPO_ACT) Made sure the Roles are under Compliance with Sarbanes- Oxley Security Act Scheduling PFCG_TIME_DEPENDENCY to Run as a night job Securing System by setting up Profile Parameters Setup password Rules Created Structural Authorization Profiles and assign the profiles to positions and User IDs as per the organizational structure. Updating HR master data through PA30 and Assigning roles based on positions for users in PO13. Participated in building security roles and structural authorization profiles and Helped in solving critical post production support issues. Effectively analyzed trace files and tracked missed authorizations for user's access problems and inserted missing authorizations manually. Transporting Security changes from development systems to quality and production servers. Extensively worked on HR authorizations like P_ORGIN, P_ORGINCON, PLOG, P_ABAP, P_ORGXX, P_ORGXXCON, P_PERNER, P_PCLX, etc. Proficient in use BI Analyses Authorizations tools as (RSECADMIN) Saving work books in roles. Authorization trace in BI authorization Create and maintain simple roles and derived roles. Maintain transaction selections and authorization data in roles. Create and Transport roles and Analysis Authorizations. Analyzed SU53 error checks during testing and to find missing authorizations and transaction codes. Ran authorization trace ST01. Implemented Security patches. Resolving authorization issues from the users analyzing the authorization issues using SU53 and ST01 and providing the solutions to the users. Expertise in identifying the missing authorizations using SU53 report from the user. Configuring su24 to follow standards of SAP Interacting with end-users to understand their issues and find out the solutions.

HR security Activities: Role modifications like adding t-codes and object level modifications based on Client requirement. Day to day technical support and resolution of HR Security issues. Created Structural Authorization Profiles and assign the profiles to positions and User IDs as per the organizational structure. Assigning roles based on positions for users in PO13. Worked on HR triggers in GRC. Working with HR authorization issues based on user requirement. Mapping of HR records to the user id's. Participated in building security roles and structural authorization

profiles and Helped in solving critical post production support issues. Effectively analyzed trace files and tracked missed authorizations for user's access problems and inserted missing authorizations manually. Transporting Security changes from development systems to quality and production servers. Extensively worked on HR authorizations like P_ORGIN, P_ORGINCON, PLOG, P_ABAP, P_ORGXX, P_ORGXXCON, P_PERNER, P_PCLX, etc. Generating PD profile using t-code Zrhprofl0. BI security Activities: Proficient in use BI Analyses Authorizations tools as (RSECADMIN) Saving work books in roles. Authorization trace in BI authorization. Create, maintain, lock and unlock users and change passwords. Create and maintain simple roles and derived roles. Maintain transaction selections and authorization data in roles. Create and Transport roles and Analysis Authorizations. Analyzed SU53 error checks during testing and to find missing authorizations and transaction codes. Ran authorization trace ST01. GRC Activity: Creating users and assigning roles using GRC 5.3 CUP. Checking the SOD (Segregations of Duties) using RAR before assigning to the users. Designed Firefighter Roles and IDs for Super user access. Risk analysis has been performed and created Mitigation Controls. Developed various SOD reports for users & Roles and cleaned up Roles with conflicting actions. Developed mitigation controls and assigned appropriately. Education M.Sc in stream of Computer Science Osmania University Skills ACCESS (4 years), BI (4 years), BUSINESS INTELLIGENCE (4 years), BUSINESS REQUIREMENTS (4 years), HR (4 years) Additional Information SAP SKILLS R/3 and ECC Security: Experience in, development, and maintenance of SAP Security in SAP R/3, ECC, BI, HR & GRC (Governance Risk and Compliance) Experience in User Administration - Includes user creation, deletion, changing user access for different systems and environments, Mass user administration. Experienced extensively in using PFCG in creating and modifying Single Roles, Composite roles and Derived roles. Working on role changes as per the business requirement. Maintenance of Derived roles based on the Organizational Values differentiation. Transport of roles across clients in the landscape Performed User Master Reconciliation for mass roles in bulk. Making user administration easier by using User Groups. Maintenance of authorization objects for transactions. Effectively analyzed trace files and tracked missing authorizations for user's

access problems using SU53 and ST01. Use of SU24 and SU25 during upgrade project Creating authorization objects using SU20 and SU21 Expertise in Troubleshoot users access problems. Proficient knowledge on USR* & AGR* tables. Experience in maintaining critical authorizations like S_TABU_DIS, S_TABU_NAM, S_PROGRAM, S_DEVELOP, S_USER_GRP, P_ORIGIN, P_ORIGINCON, S_RS_COMP & COMP1. Experience in maintaining restrictions on sensitive tables by assigning them to authorization groups through SE54. Generating security reports from SUIM Experienced extensively in User Information System. Worked on various ticketing tools. Preparing Role Matrix. Preparing Role Designing strategy. HR Security Exposure Position based role assignment and PD profile assignment. Knowledge on implementing structural authorizations. Mapping personnel numbers with SAP login id. Knowledge on HR authorization objects & basic info types. Troubleshooting HR issues. Knowledge of *HR * security tables Assigning roles to positions and Removing roles from positions (PP02) Reading the org structure to check for valid persons & users (PPOSE / PA20) Checking non-manager/manager position using PO13D Running reports like RHANALYSIS_TOOL, RHPROFLO, RHUSERRELATIONS, PFUD BI Security Exposure Creation and maintenance of analysis authorizations. Troubleshooting BI authorization issues. Good understanding on BI authorization objects. GRC AC 5.3 & 10.1 From GRC implementation prospective, actively working in implementing GRC AC -products like RAR-ARA, SPM-EAM, and CUP-ARM. Preparing configuration & customizing documentation for RAR, SPM, and CUP & ERM. Experience in SAP GRC applications and troubleshooting activities of Access Controls at the time of pre & post installations. Participated in ongoing GRC AC 5.3 implementation, GRC component deployments. Gathering requirements for customizing Rule set. Creating and Modifying Risks/Functions whenever it is required. Modifying/Enabling/disabling Function actions/Function permissions as per business requirements Working experience on SUIM reports, scheduling background jobs. Monitoring daily back ground jobs Scheduling RAR back ground jobs weekly/monthly. Assist/Reports weekly/Monthly/Quarterly SOD'S reports and support for both Internal and External Auditing. Created mitigation controls as per BPO or auditor suggestions. Assign mitigation

control to user. Design and implementing Workflows of CUP. Worked on CUP application configuration based on client requirement like connectors, Workflows, Email notification set up etc. Defined critical transactions to be used for Fire Fighter Access. Customizing Super User Privilege Management (SPM), creating Fire Fighter User, designing and assigning Fire Fighter roles, Fire Fighter logs activities, Critical operation Alerts and etc. Existing role creation process process Identifying functional areas, approvers, &business Process Identifying naming conventions Build the new roles as per business process requests. Experience in User Administration involves Creation/ Deletion/ Locking/ Modifying Users as per the Approval. Extracting reports from CC for SOX/SOD. TECHNICAL SKILLS ERP: SAP ECC 6.0, HR, BI &CRM.. Compliance tools: VIRSA tool, Governance Risk and Compliance 5.3/10.1.

Name: Miguel Reyes

Email: timwilliams@example.org

Phone: (857)459-7542