## Security and Compliance Lead

**Ad Hoc Responsibilities**

* **Incident Response and Remediation:**
  + Lead investigations into security incidents or breaches affecting the GitHub environment.
  + Coordinate immediate remediation actions (e.g., patch deployment, configuration changes) when vulnerabilities are discovered.
* **Regulatory & Audit Inquiries:**
  + Respond to urgent inquiries or requests from external auditors, regulatory bodies, or internal compliance teams.
* **Policy Exception & Emergency Reviews:**
  + Address unexpected deviations from security policies and make ad hoc decisions to mitigate risk.
* **Threat Intelligence Integration:**
  + Quickly evaluate and act on new threat intelligence or emerging vulnerabilities relevant to GitHub usage.

**Daily Responsibilities**

* **Security Dashboard Monitoring:**
  + Continuously review security dashboards and alerts (e.g., GitHub Advanced Security notifications, audit logs) for signs of suspicious activity.
* **Alert Triage:**
  + Assess and prioritize security alerts, ensuring that critical issues are escalated and addressed promptly.
* **Log and Activity Review:**
  + Monitor real-time audit logs and user activities for anomalies or unauthorized access attempts.
* **Communication & Coordination:**
  + Stay updated on internal communications and external security advisories impacting the GitHub environment.

**Weekly Responsibilities**

* **Weekly Security Briefings:**
  + Convene with the security team and relevant stakeholders to review security incidents, trends, and ongoing risk mitigation efforts.
* **Permission and Access Reviews:**
  + Conduct spot-checks of user access and permission changes across repositories to ensure compliance with the principle of least privilege.
* **Compliance Report Review:**
  + Analyze weekly reports summarizing security events, vulnerability scan results, and compliance metrics from GitHub.
* **Update Security Runbooks:**
  + Document any incidents, lessons learned, or process improvements to update internal playbooks and procedures.

**Monthly Responsibilities**

* **Vulnerability Scanning & Assessment:**
  + Initiate and review vulnerability scans across GitHub repositories and integrations.
* **Configuration Audits:**
  + Verify that critical GitHub security settings (e.g., branch protection, required code reviews) and integrations remain aligned with policy.
* **Metrics & KPI Evaluation:**
  + Summarize and analyze key performance indicators (KPIs) related to security posture (e.g., incident response times, number of alerts) and report findings to leadership.
* **Team Training & Briefings:**
  + Conduct monthly security briefings or training sessions to reinforce security best practices and policy updates with the broader development and operations teams.

**Quarterly Responsibilities**

* **Comprehensive Security Reviews:**
  + Perform a thorough review of the overall security posture of the GitHub environment, including a gap analysis against internal policies and external regulatory requirements.
* **User Access and Permission Audits:**
  + Lead a detailed audit of user roles, team memberships, and repository access rights to ensure adherence to least privilege principles.
* **Incident Response Drills:**
  + Organize tabletop exercises or simulated incident response drills to evaluate and refine the team’s readiness and response procedures.
* **Policy and Procedure Updates:**
  + Review and update security and compliance policies based on recent audit findings, emerging threats, or changes in regulatory standards.
* **Stakeholder Reviews:**
  + Meet with internal audit teams, IT risk management, and executive leadership to review quarterly security performance and outline upcoming initiatives.

**Annual Responsibilities**

* **Full-Scale Security Audit and Risk Assessment:**
  + Lead an annual, comprehensive audit of the GitHub environment to evaluate security controls, identify risks, and assess overall compliance.
* **Strategic Planning & Roadmap Development:**
  + Develop and update the long-term security strategy and roadmap for the GitHub platform, including resource planning and future technology investments.
* **Policy Overhaul & Documentation:**
  + Review, revise, and formally document all security and compliance policies, procedures, and runbooks to reflect the current threat landscape and organizational requirements.
* **External Compliance and Regulatory Audits:**
  + Coordinate and participate in external audits and assessments, ensuring that all necessary documentation and evidence are provided to regulators and auditors.
* **Annual Training & Certification:**
  + Oversee organization-wide security training and certification updates, ensuring that all GitHub users and administrators are informed about the latest security practices and regulatory changes.
* **Budget and Resource Planning:**
  + Review the effectiveness of security investments and plan the annual budget to support ongoing and future security initiatives.

## Access Control and Permissions Manager

**Ad Hoc Responsibilities**

* **Urgent Access Issue Resolution:**
  + Respond immediately to escalated permission errors or unauthorized access incidents.
  + Approve or revoke temporary elevated access when emergency needs arise.
* **Incident Coordination:**
  + Collaborate with security teams during access-related breaches or misconfigurations.
  + Address ad hoc requests from business units requiring immediate access modifications due to changing project requirements.
* **Ad Hoc Policy Adjustments:**
  + Evaluate and implement quick adjustments to access policies when new threats or vulnerabilities are identified.

**Daily Responsibilities**

* **Access Log Monitoring:**
  + Review daily audit logs for permission changes and anomalies in access patterns.
  + Monitor automated alerts for unauthorized or unusual access activities.
* **User Support and Queries:**
  + Address user queries and immediate requests related to access permissions.
  + Provide first-level troubleshooting for access-related issues.
* **System Health Checks:**
  + Ensure that automated processes (such as LDAP/SSO synchronization) are operating correctly to update user statuses and permissions.

**Weekly Responsibilities**

* **Routine Access Audits:**
  + Perform spot-checks on permission changes across repositories and teams.
  + Reconcile user access levels with team roles and organizational hierarchies.
* **Team Collaboration:**
  + Meet with department leads and IT teams to discuss recent access changes, potential risks, and upcoming projects requiring access reviews.
* **Review of Temporary Permissions:**
  + Identify and revoke any temporary elevated access that is no longer needed.
* **Report Generation:**
  + Generate and distribute weekly reports highlighting significant permission modifications or potential issues.

**Monthly Responsibilities**

* **Comprehensive Permissions Audit:**
  + Conduct a detailed review of all user and team permissions across the organization.
  + Validate that access assignments adhere to the principle of least privilege.
* **Access Policy Review:**
  + Update internal documentation and guidelines on access controls based on recent audit findings.
  + Review and adjust group policies, roles, and access levels to reflect changes in the organizational structure.
* **User Lifecycle Management:**
  + Verify that onboarding and offboarding processes are correctly provisioning and de-provisioning access rights.
  + Reconcile active user lists with HR records to remove or adjust permissions for inactive or terminated employees.
* **Integration Checks:**
  + Confirm that external integrations (SSO, LDAP, or third-party identity providers) are correctly propagating permission updates.

**Quarterly Responsibilities**

* **In-Depth Access Reviews:**
  + Perform thorough audits of high-risk repositories and teams to detect and correct any permission creep.
  + Analyze trends from monthly audits and adjust controls or thresholds as needed.
* **Policy and Process Revisions:**
  + Update access control policies to incorporate new security best practices, compliance requirements, or organizational changes.
  + Engage in cross-functional reviews with security, compliance, and IT risk management teams.
* **User Training and Awareness:**
  + Host quarterly sessions or workshops on access control best practices and recent policy updates for team leads and administrators.
* **Integration & Automation Validation:**
  + Reassess automated permission management tools and integrations to ensure they continue to meet organizational needs and compliance standards.

**Annual Responsibilities**

* **Comprehensive Security Audit:**
  + Lead a full-scale audit of the organization’s access control framework, reviewing all user, team, and repository permissions.
  + Document audit findings and present risk assessments to executive leadership.
* **Strategic Planning and Roadmap Development:**
  + Develop or update the long-term strategy for managing access controls, including potential technology investments and process improvements.
  + Plan major reviews or overhauls of access policies in line with new compliance regulations or organizational restructuring.
* **Policy Overhaul and Documentation:**
  + Revise and formally document all access control policies and procedures, ensuring alignment with industry best practices and compliance mandates.
* **Training and Certification Programs:**
  + Roll out organization-wide training initiatives on access management practices.
  + Ensure key staff members are updated on the latest tools, technologies, and regulatory requirements.
* **Review and Update Metrics:**
  + Evaluate performance metrics from the past year (e.g., incident response times, number of unauthorized access events) to adjust KPIs and targets for the upcoming year.

## Repository Governance Manager

**Ad Hoc Responsibilities**

* **Emergency Repository Issue Resolution:**
  + Address unexpected misconfigurations (e.g., incorrect visibility, missing branch protection) that risk security or compliance.
  + Resolve urgent disputes or questions around repository ownership, naming, or structure.
* **Policy Exception Management:**
  + Evaluate and approve ad hoc exceptions for repository creation or modification when business needs require deviation from established guidelines.
* **Incident Collaboration:**
  + Work with security and compliance teams during repository-related incidents (e.g., accidental data exposure) to quickly implement corrective actions.
* **Legacy Migration & Onboarding Issues:**
  + Provide immediate support during the integration or migration of legacy repositories into the current governance framework.

**Daily Responsibilities**

* **Monitoring New Repository Creations:**
  + Review and validate that newly created repositories comply with naming conventions, documentation standards, and initial configuration requirements.
* **Dashboard and Alert Review:**
  + Monitor governance dashboards for anomalies or configuration drift (e.g., missing READMEs, branch protection lapses).
* **User Inquiries and Support:**
  + Respond to daily queries from teams regarding proper repository setup and compliance with governance policies.
* **Automated Process Verification:**
  + Ensure that automated scripts or tools enforcing repository standards (e.g., tagging, policy compliance) are running as expected.

**Weekly Responsibilities**

* **Routine Repository Audits:**
  + Perform spot checks on a sample of repositories to verify compliance with established governance guidelines (naming conventions, branch protections, documentation).
* **Metadata & Settings Review:**
  + Validate that repository metadata (e.g., descriptions, topics, licensing information) is complete and accurate.
* **Team Coordination Meetings:**
  + Meet with project leads and repository administrators to review recent changes, discuss challenges, and reinforce governance expectations.
* **New Repository Request Reviews:**
  + Evaluate and provide feedback on submitted repository requests to ensure they meet organizational policies before provisioning.
* **Trend Analysis:**
  + Monitor weekly metrics on repository creation, updates, and archiving to identify emerging issues or non-compliance trends.

**Monthly Responsibilities**

* **Comprehensive Governance Reporting:**
  + Generate and distribute detailed reports on repository compliance, highlighting deviations, trends, and areas needing improvement.
* **Legacy and Inactive Repository Assessment:**
  + Review repositories that have been inactive or flagged, determining if they should be archived, updated, or decommissioned.
* **Policy Documentation Review:**
  + Update internal documentation and checklists related to repository governance based on recent audit findings or process changes.
* **Training and Communication:**
  + Conduct or coordinate training sessions and informational updates for repository administrators and developers on governance best practices.
* **Integration and Tool Evaluation:**
  + Verify that integrated tools (e.g., for automated policy enforcement) are functioning correctly and adjust configurations as needed.

**Quarterly Responsibilities**

* **In-Depth Repository Reviews:**
  + Lead a thorough audit of a broader set of repositories to assess adherence to governance standards across the organization.
* **Policy Revisions:**
  + Review and update repository governance policies to reflect evolving business needs, technology changes, or security best practices.
* **Gap Analysis and Remediation Planning:**
  + Identify gaps between current repository practices and desired governance outcomes, then develop and prioritize remediation plans.
* **Cross-Functional Collaboration:**
  + Engage with security, compliance, and IT operations teams to align repository governance with broader enterprise policies and risk management strategies.
* **Feedback Sessions:**
  + Host structured sessions with stakeholders to review governance effectiveness, gather feedback, and adjust processes accordingly.

**Annual Responsibilities**

* **Full-Scale Repository Audit:**
  + Conduct an organization-wide audit of all repositories to ensure full compliance with governance policies, security standards, and documentation requirements.
* **Strategic Roadmap Development:**
  + Develop a long-term roadmap for repository management, including major upgrades, archival strategies, and technology investments.
* **Governance Policy Overhaul:**
  + Revise and formalize all repository governance policies and procedures, incorporating lessons learned and changes in regulatory or organizational requirements.
* **Executive Reporting and Review:**
  + Present an annual report to executive leadership detailing governance performance, audit findings, incident resolutions, and planned improvements.
* **Organization-Wide Training:**
  + Plan and implement comprehensive training programs on repository governance best practices for all relevant teams.
* **Budget and Resource Planning:**
  + Review resource allocations and budget requirements for repository governance initiatives, ensuring alignment with the strategic IT roadmap.

## DevOps Integration Manager

**Ad Hoc Responsibilities**

* **Urgent Issue Resolution:**
  + Troubleshoot and resolve unexpected failures in CI/CD pipelines or integration points with minimal downtime.
  + Coordinate with development, operations, and third-party vendors during critical integration incidents.
* **New Integration Onboarding:**
  + Rapidly deploy and test integrations requested by development teams or external partners.
* **Incident Escalation:**
  + Act as the escalation point for issues impacting build, deployment, or integration processes.
* **Emergency Configuration Changes:**
  + Implement ad hoc configuration changes or rollbacks in response to security alerts or system failures.

**Daily Responsibilities**

* **Pipeline Monitoring:**
  + Review and monitor CI/CD pipeline runs and integration logs for failures or performance degradation.
  + Track alerts from integration tools and systems, ensuring immediate remediation of any issues.
* **Operational Support:**
  + Provide day-to-day support to developers and DevOps engineers regarding integration tools and processes.
  + Validate that scheduled jobs, webhooks, and automated scripts are executing as expected.
* **Status Reporting:**
  + Keep a pulse on system health dashboards and update key stakeholders on operational status.

**Weekly Responsibilities**

* **Performance and Health Reviews:**
  + Analyze weekly performance metrics and logs from integration systems to identify trends and areas for improvement.
  + Conduct routine checks on deployment pipelines to ensure consistent performance and compliance with best practices.
* **Team Coordination Meetings:**
  + Hold weekly syncs with DevOps, development, and infrastructure teams to discuss ongoing issues, upcoming releases, and integration improvements.
* **Documentation Updates:**
  + Update internal documentation, runbooks, and integration playbooks to reflect recent changes or lessons learned.
* **Feedback Analysis:**
  + Review feedback from users and teams regarding integration issues and incorporate improvements into the workflow.

**Monthly Responsibilities**

* **Comprehensive Integration Audits:**
  + Perform detailed audits of CI/CD pipelines, integrations, and automated workflows to verify correct configurations and optimal performance.
* **Tooling and Version Reviews:**
  + Check for updates, patches, and upgrades to integration tools, ensuring compatibility and security.
* **User Training Sessions:**
  + Organize or facilitate training sessions or workshops on new integration features, best practices, and troubleshooting techniques.
* **Process Improvement Planning:**
  + Evaluate monthly performance metrics and user feedback to identify opportunities for process enhancements or automation improvements.
* **Inter-Team Coordination:**
  + Coordinate with repository governance and security teams to ensure integration workflows align with overall organizational policies.

**Quarterly Responsibilities**

* **Strategic Integration Reviews:**
  + Conduct an in-depth review of the integration ecosystem, evaluating the effectiveness, scalability, and security of CI/CD pipelines and tools.
* **Risk Assessments:**
  + Assess risks associated with integration endpoints, third-party services, and automation scripts; develop mitigation plans.
* **Cross-Functional Workshops:**
  + Lead cross-functional review sessions with development, security, and operations teams to discuss challenges and propose strategic enhancements.
* **Scalability and Resource Planning:**
  + Review capacity planning and resource usage to ensure that integration systems can scale with organizational growth.
* **Policy and Process Updates:**
  + Update integration policies and standard operating procedures (SOPs) based on the latest industry practices and internal audit findings.

**Annual Responsibilities**

* **Roadmap and Strategic Planning:**
  + Develop a long-term roadmap for CI/CD and integration tools, including future upgrades, new technology adoption, and strategic improvements.
* **Comprehensive System Audit:**
  + Perform a full-scale audit of all integration workflows, assessing their performance, security posture, and alignment with business objectives.
* **Budgeting and Resource Allocation:**
  + Plan and propose the annual budget for integration tools, infrastructure upgrades, and training programs.
* **Executive Reporting:**
  + Compile an annual report summarizing integration performance, incidents, improvements, and strategic goals for executive leadership.
* **Vendor and Contract Reviews:**
  + Evaluate existing contracts and relationships with integration tool vendors; negotiate renewals or explore new partnership opportunities.
* **Training and Certification:**
  + Implement organization-wide training programs and certifications to ensure teams are up-to-date with the latest integration technologies and best practices.

## Incident Response Coordinator / Security Operations Specialist

**Ad Hoc Responsibilities**

* **Immediate Incident Response:**
  + Activate the incident response plan when a new security event or breach is detected.
  + Coordinate with cross-functional teams (IT, legal, PR) to contain and mitigate incidents.
* **Critical Escalations:**
  + Engage with external experts or vendors for forensic analysis or specialized remediation when required.
* **Emergency Communications:**
  + Issue urgent notifications to internal stakeholders and external partners during high-severity incidents.
* **Ad Hoc Forensic Analysis:**
  + Initiate ad hoc investigations to determine root causes, scope, and impact of an incident.
* **Process Adaptation:**
  + Quickly adjust incident response procedures in reaction to emerging threats or vulnerabilities.

**Daily Responsibilities**

* **Monitoring and Alert Triage:**
  + Continuously monitor security dashboards, SIEM feeds, and log aggregators for signs of suspicious activity.
  + Triage alerts and initiate the incident response workflow for any critical findings.
* **Documentation and Logging:**
  + Record incident details, timelines, and actions taken in incident logs or ticketing systems.
* **System Health and Tool Checks:**
  + Verify that all incident response tools, monitoring systems, and alerting mechanisms are operational.
* **Stakeholder Communication:**
  + Provide timely updates to relevant teams regarding ongoing incidents or anomalies.

**Weekly Responsibilities**

* **Incident Review Meetings:**
  + Conduct weekly meetings with the security operations team to review recent incidents, trends, and response outcomes.
* **Follow-Up Analysis:**
  + Perform a preliminary review of unresolved or recurring incidents to identify patterns or process gaps.
* **Threat Intelligence Briefing:**
  + Update the team on emerging threats, new vulnerabilities, or changes in the threat landscape.
* **Runbook Updates:**
  + Review and refine incident response runbooks and procedures based on lessons learned during the week.

**Monthly Responsibilities**

* **Comprehensive Incident Reporting:**
  + Compile detailed monthly reports on incident frequency, response times, outcomes, and lessons learned for management review.
* **Post-Incident Reviews:**
  + Conduct in-depth post-mortem analyses for significant incidents to determine root causes and recommend process improvements.
* **Tool and Process Assessment:**
  + Evaluate the effectiveness of current monitoring and incident response tools; propose enhancements or adjustments.
* **Training and Drills:**
  + Organize refresher training sessions or tabletop exercises for the incident response team to keep skills sharp.
* **Policy and Procedure Review:**
  + Update incident response policies and documentation based on evolving threat intelligence and audit feedback.

**Quarterly Responsibilities**

* **Tabletop Exercises and Simulations:**
  + Plan and execute simulated incident response drills to test team readiness and identify areas for improvement.
* **Full Process Audits:**
  + Conduct a comprehensive review of incident response processes, communication flows, and escalation procedures.
* **Cross-Team Collaboration:**
  + Coordinate with other departments (e.g., IT, compliance, legal) to review incident response coordination and ensure alignment with broader organizational risk management.
* **Metrics and Performance Evaluation:**
  + Analyze quarterly incident data to track trends, measure KPIs (e.g., time to detection, resolution rates), and adjust strategies accordingly.

**Annual Responsibilities**

* **Strategic Incident Response Review:**
  + Lead an annual, full-scale evaluation of the incident response program, including a review of past incidents, response effectiveness, and overall security posture.
* **Plan and Policy Overhaul:**
  + Update and formalize the annual incident response plan, policies, and playbooks to reflect lessons learned and changes in the threat landscape.
* **Executive Reporting:**
  + Prepare and present a comprehensive annual incident response report to executive leadership, highlighting key trends, improvements, and future risk mitigation strategies.
* **Training and Certification:**
  + Organize organization-wide incident response and security operations training sessions; ensure team certifications are up to date.
* **Budget and Resource Planning:**
  + Evaluate and plan the annual budget for incident response initiatives, including investments in new tools, technologies, and staff training.
* **External Audit and Benchmarking:**
  + Engage with external auditors or consultants to perform an independent review of incident response capabilities and benchmark against industry standards.

## Auditing and Monitoring Specialist

**Ad Hoc Responsibilities**

* **Incident-Driven Audits:**
  + Launch targeted audits when a security incident, unusual activity, or compliance breach is detected.
  + Collaborate with the incident response team to analyze logs and pinpoint root causes.
* **Forensic Investigations:**
  + Conduct in-depth forensic reviews in response to escalated audit findings.
  + Provide detailed documentation and evidence for legal, regulatory, or internal investigations.
* **Ad Hoc Compliance Checks:**
  + Perform spot audits when new compliance requirements or regulatory changes are announced.
  + Address sudden internal requests for evidence or audits related to specific concerns.

**Daily Responsibilities**

* **Continuous Log Monitoring:**
  + Review system and application logs (e.g., GitHub audit logs, access logs) for anomalies or irregular activities.
  + Monitor security dashboards and automated alerts for potential breaches or misconfigurations.
* **Alert Triage and Verification:**
  + Evaluate daily alerts to filter false positives from genuine security or compliance issues.
  + Escalate findings to relevant teams if suspicious activity is confirmed.
* **Data Integrity Checks:**
  + Verify that monitoring tools and log collection systems are running correctly and capturing all critical events.
* **Documentation:**
  + Record daily observations, unusual events, and initial analyses to maintain a continuous audit trail.

**Weekly Responsibilities**

* **Audit Report Compilation:**
  + Generate summary reports covering key audit findings, anomalies, and system activities from the past week.
  + Identify trends or recurring issues that may require further investigation.
* **Team Briefings:**
  + Participate in weekly meetings with IT, security, and compliance teams to review audit results and discuss corrective actions.
* **Policy and Configuration Verification:**
  + Cross-check system configurations and user activity against established policies and compliance standards.
* **Follow-Up Reviews:**
  + Reassess any issues flagged in previous audits to confirm that remediation efforts have been successful.

**Monthly Responsibilities**

* **Detailed Compliance Audits:**
  + Conduct comprehensive audits of user permissions, system configurations, and access controls to ensure they adhere to internal and external standards.
* **Performance and Trend Analysis:**
  + Analyze monthly audit data to detect long-term trends, potential vulnerabilities, or shifts in user behavior.
* **Tool Calibration and Updates:**
  + Review and adjust monitoring and logging tools to ensure they remain tuned to the evolving threat landscape.
* **Stakeholder Reporting:**
  + Prepare and distribute detailed audit reports to management and relevant stakeholders, highlighting key metrics, anomalies, and compliance statuses.
* **Documentation Updates:**
  + Update audit runbooks, standard operating procedures (SOPs), and compliance checklists based on the monthly findings.

**Quarterly Responsibilities**

* **Comprehensive System Audits:**
  + Perform in-depth, organization-wide audits to assess the effectiveness of current monitoring tools and compliance controls.
  + Validate that all systems are configured according to the latest security and compliance policies.
* **Process and Policy Reviews:**
  + Review and refine auditing methodologies and monitoring processes to incorporate new best practices and regulatory requirements.
* **Trend and Risk Assessments:**
  + Analyze quarterly data to identify emerging risks or potential areas for policy improvement.
* **Cross-Department Collaboration:**
  + Coordinate with IT, security, and legal teams to review audit findings and update risk management strategies.
* **Training Sessions:**
  + Organize refresher training for team members on audit tools, compliance standards, and effective monitoring practices.

**Annual Responsibilities**

* **Full-Scale Audit Program Review:**
  + Conduct a comprehensive, organization-wide audit to evaluate the overall effectiveness of the auditing and monitoring program.
  + Identify gaps, redundancies, and areas for improvement.
* **Strategic Roadmap Development:**
  + Develop a long-term strategy for evolving auditing and monitoring capabilities, including technology upgrades and process improvements.
* **Executive Reporting:**
  + Prepare and present an annual audit report summarizing findings, performance metrics, risk assessments, and improvement plans to executive leadership.
* **Regulatory and Compliance Alignment:**
  + Review changes in regulatory requirements and ensure that the audit program is updated accordingly.
* **Budget and Resource Planning:**
  + Assess and plan resource needs, including tool investments and training budgets, to support the auditing and monitoring function for the upcoming year.
* **External Audit Coordination:**
  + Facilitate external audits and reviews, providing necessary documentation and addressing any external recommendations.

## Developer Advocate / Security Educator

**Ad Hoc Responsibilities**

* **Emergency Training & Support:**
  + Provide impromptu coaching or one-on-one sessions when developers face urgent security issues.
  + Develop and release quick-response guides or bulletins in reaction to new vulnerabilities or critical advisories.
* **Ad Hoc Content Creation:**
  + Create targeted content (e.g., blog posts, FAQs, or how-to guides) on emerging security topics as needed.
* **Incident-Driven Communication:**
  + Participate in emergency meetings or security incident reviews to help interpret security findings and advise on best practices.
* **Community Engagement:**
  + Jump in on unexpected developer queries via internal forums, chat channels, or social media, ensuring accurate security information is shared.

**Daily Responsibilities**

* **Developer Community Engagement:**
  + Monitor and respond to questions on internal channels (Slack, Teams, discussion boards) related to security best practices.
* **Content Updates & Curation:**
  + Review and update existing educational materials, FAQs, or micro-blog posts to ensure they remain current.
* **Security News & Trend Monitoring:**
  + Stay abreast of the latest security news and vulnerabilities; share brief updates or insights with developer communities.
* **Feedback Collection:**
  + Collect and log feedback from developers regarding current educational materials or training sessions for continuous improvement.

**Weekly Responsibilities**

* **Interactive Sessions:**
  + Host webinars, Q&A sessions, or "office hours" focused on security topics and emerging best practices.
* **Content Development & Distribution:**
  + Publish blog posts, newsletters, or internal communications highlighting key security updates, tips, and lessons learned.
* **Team Coordination:**
  + Participate in team meetings with security and development leads to align on upcoming educational initiatives and address any immediate challenges.
* **Engagement Metrics Review:**
  + Analyze participation and engagement metrics from community platforms to identify areas where developers need additional support.

**Monthly Responsibilities**

* **In-Depth Workshops:**
  + Organize and deliver hands-on workshops or training sessions on specific security topics (e.g., secure coding, vulnerability management, tool usage).
* **Curriculum and Resource Review:**
  + Assess and update training materials, documentation, and best practice guides based on feedback and evolving security standards.
* **Cross-Functional Meetings:**
  + Coordinate with product, engineering, and security teams to discuss integration of security practices into the development lifecycle.
* **Impact Assessment:**
  + Distribute surveys or hold focus groups to gauge the effectiveness of educational efforts and identify gaps in knowledge.

**Quarterly Responsibilities**

* **Major Security Events:**
  + Plan and host large-scale events, such as hackathons, security challenges, or conferences, to promote security awareness and innovation.
* **Curriculum Overhaul:**
  + Conduct a comprehensive review and update of the security education curriculum to ensure alignment with industry trends and organizational needs.
* **Cross-Departmental Workshops:**
  + Facilitate multi-team sessions that bring together developers, security professionals, and operations staff to discuss challenges and share insights.
* **Program Performance Review:**
  + Analyze quarterly engagement and training metrics, review feedback, and adjust strategies to improve the overall effectiveness of the educational program.

**Annual Responsibilities**

* **Strategic Roadmap Development:**
  + Develop and publish a comprehensive annual security education and advocacy roadmap aligned with organizational priorities and industry best practices.
* **Major Conferences and Summits:**
  + Organize or participate in a flagship event (internal or external) to showcase security innovations, share best practices, and build community.
* **Program Impact Evaluation:**
  + Conduct a full review of the education program’s impact, including success metrics, feedback from developers, and ROI on training initiatives.
* **Long-Term Strategy & Partnerships:**
  + Update long-term educational strategies and toolkits, and establish or renew partnerships with external organizations, educational institutions, or industry groups.
* **Goal Setting & Budget Planning:**
  + Set strategic goals for the upcoming year and contribute to budget and resource planning to support continuous improvements in security education initiatives.

## Tooling and Automation Engineer

**Ad Hoc Responsibilities**

* **Emergency Automation Fixes:**
  + Troubleshoot and resolve sudden failures in automated scripts or integrations impacting critical workflows.
  + Implement quick patches or temporary workarounds for broken tools until a permanent solution is developed.
* **New Tool Evaluation and Onboarding:**
  + Research, prototype, and deploy new automation tools or scripts in response to emerging business needs or technology updates.
  + Rapidly develop proof-of-concept integrations for unplanned projects.
* **Incident Response Support:**
  + Assist incident response teams by creating or modifying automation scripts to gather forensic data or streamline remediation actions.
* **Custom Automation Requests:**
  + Build custom scripts or integrations on demand to support special projects, ad hoc reporting, or unique operational challenges.

**Daily Responsibilities**

* **Automation Process Monitoring:**
  + Check the status of scheduled automation jobs, CI/CD pipelines, and scripts to ensure they are running as expected.
  + Review alerts and logs for any failures or anomalies in automated processes.
* **Quick-Turnaround Fixes:**
  + Address minor issues or errors in automation scripts as they are reported by users or detected by monitoring tools.
* **Communication and Coordination:**
  + Respond to queries from development or operations teams regarding automation tools and processes.
  + Collaborate with team members to track the status of ongoing automation projects.

**Weekly Responsibilities**

* **Performance Reviews and Log Analysis:**
  + Analyze logs and performance metrics from automation tools to identify trends, recurring issues, or opportunities for optimization.
  + Summarize weekly automation performance and share insights with the team.
* **Team Meetings and Sync-Ups:**
  + Participate in weekly meetings with DevOps, security, and development teams to review tool performance, discuss new automation needs, and align on upcoming projects.
* **Maintenance and Script Updates:**
  + Update and refine automation scripts to improve efficiency, handle edge cases, or incorporate new requirements.
* **Documentation Updates:**
  + Document changes, new features, and troubleshooting steps for automation tools to keep internal documentation up to date.

**Monthly Responsibilities**

* **Comprehensive System Audits:**
  + Perform a detailed audit of all automation tools, scripts, and integrations to ensure proper functioning and security.
  + Verify that all automated processes align with current business workflows and compliance standards.
* **Tooling and Integration Reviews:**
  + Evaluate the performance of existing tools and integrations; recommend upgrades, enhancements, or decommissioning where needed.
* **User Feedback Sessions:**
  + Gather and review feedback from developers and operations teams regarding the effectiveness and usability of automation solutions.
* **Scheduled Maintenance:**
  + Plan and execute routine maintenance, updates, and backups of automation infrastructure to prevent downtime or data loss.
* **Training and Knowledge Sharing:**
  + Host a monthly knowledge-sharing session or workshop on new automation techniques, scripting best practices, or tool usage.

**Quarterly Responsibilities**

* **Strategic Tooling Assessments:**
  + Conduct a comprehensive review of the automation landscape within the organization, evaluating the ROI and effectiveness of current tools.
  + Research and propose new automation solutions that align with evolving business needs and technological advancements.
* **Process Optimization and Innovation:**
  + Lead initiatives to streamline workflows and reduce manual interventions by enhancing or expanding automation capabilities.
* **Cross-Functional Collaboration:**
  + Work with multiple departments (e.g., security, development, operations) to align automation strategies with overall organizational goals.
* **Security and Compliance Reviews:**
  + Audit automation scripts for compliance with security best practices; update tools to address any identified vulnerabilities.
* **Metrics and Reporting:**
  + Develop and present quarterly reports on automation performance, impact metrics (e.g., time saved, error reduction), and future improvement plans.

**Annual Responsibilities**

* **Long-Term Roadmap Development:**
  + Create and update the strategic automation roadmap, aligning with the organization’s long-term IT and operational goals.
  + Set priorities for major automation projects and technology investments for the coming year.
* **Comprehensive Infrastructure Review:**
  + Conduct a full-scale review of the automation infrastructure, including tools, scripts, integrations, and supporting systems.
  + Identify opportunities for consolidation, modernization, or migration to new platforms.
* **Budgeting and Resource Planning:**
  + Develop budget proposals and resource plans for new automation initiatives, training, and tool upgrades.
* **Vendor and Technology Partner Evaluation:**
  + Review and assess relationships with vendors or external partners providing automation tools or services.
  + Participate in contract renewals or negotiate new terms based on performance and future needs.
* **Annual Training and Certification:**
  + Organize or attend training sessions and certification programs to stay current with emerging automation technologies and best practices.
* **Executive Reporting and Strategy Alignment:**
  + Prepare an annual report summarizing automation achievements, challenges, and strategic plans for executive leadership.
  + Align automation initiatives with broader organizational transformation or digitalization strategies.

## Compliance and Risk Manager

**Ad Hoc Responsibilities**

* **Incident-Driven Risk Assessment:**
  + Initiate rapid risk evaluations and investigations in response to unexpected compliance breaches or security incidents.
  + Collaborate with relevant teams to determine the scope and impact of incidents and recommend immediate risk mitigation measures.
* **Regulatory Inquiries and Reporting:**
  + Respond to ad hoc requests from regulatory bodies, internal auditors, or legal teams seeking information on compliance matters.
* **Crisis Management Support:**
  + Provide immediate risk analysis and recommendations during business disruptions, ensuring compliance risks are minimized.
* **Policy Exception Evaluations:**
  + Assess and approve temporary deviations from established policies when urgent business needs require exceptions.
* **Emerging Threat Response:**
  + Quickly evaluate and incorporate new regulatory changes or emerging risks into existing frameworks as needed.

**Daily Responsibilities**

* **Regulatory and News Monitoring:**
  + Review industry news, regulatory updates, and legal bulletins to stay current on any changes that might affect compliance or risk posture.
* **Dashboard and Alert Review:**
  + Monitor compliance dashboards, risk registers, and automated alerts to detect anomalies or potential issues.
* **Operational Oversight:**
  + Check that automated compliance tools and reporting systems are functioning correctly and capturing relevant data.
* **Incident Log Updates:**
  + Record any compliance-related incidents or observations in internal tracking systems, ensuring that issues are documented for later review.
* **Communication with Stakeholders:**
  + Maintain daily communication with IT, security, and business teams to flag immediate compliance risks or updates.

**Weekly Responsibilities**

* **Risk and Compliance Meetings:**
  + Convene or participate in weekly risk committee meetings with cross-functional teams to review emerging risks, incidents, and compliance challenges.
* **Preliminary Reporting:**
  + Compile weekly summaries of compliance incidents, audit findings, and risk trends to inform management and support decision-making.
* **Control Verification:**
  + Perform spot checks to verify that critical controls and compliance measures are in place and functioning as designed.
* **Action Item Follow-Up:**
  + Review and update the status of action items and remediation plans from previous incidents or audits.
* **Training and Awareness:**
  + Conduct brief training sessions or send out updates to teams regarding any new compliance requirements or risk management practices.

**Monthly Responsibilities**

* **Detailed Compliance Audits:**
  + Lead monthly internal audits focusing on key compliance areas (e.g., access controls, data handling, code review processes) to ensure adherence to policies.
* **Risk Register Maintenance:**
  + Update and review the risk register, documenting new risks, status changes, and remediation efforts.
* **Metrics and KPI Analysis:**
  + Analyze monthly compliance and risk metrics (e.g., incident frequency, remediation timelines) to identify trends and areas for improvement.
* **Policy Review and Updates:**
  + Evaluate existing policies for relevancy and compliance with current regulations; update internal documentation as necessary.
* **Stakeholder Reporting:**
  + Prepare detailed monthly reports summarizing compliance findings, risk assessments, and recommended improvements for senior management.

**Quarterly Responsibilities**

* **Comprehensive Risk Reviews:**
  + Conduct an in-depth, organization-wide risk assessment, reviewing the effectiveness of current controls and identifying any gaps.
* **Cross-Departmental Workshops:**
  + Organize workshops or strategy sessions with key stakeholders from IT, legal, and business units to collaboratively address high-priority risks and compliance challenges.
* **Audit Program Evaluation:**
  + Reassess the auditing processes and tools used to monitor compliance, ensuring they remain aligned with industry best practices.
* **Policy and Procedure Revisions:**
  + Collaborate with legal and compliance teams to review and update risk management policies and procedures based on audit findings and regulatory changes.
* **Vendor and Third-Party Risk Assessment:**
  + Evaluate the compliance and risk posture of key vendors and third-party partners, ensuring they meet internal and regulatory standards.

**Annual Responsibilities**

* **Strategic Risk and Compliance Planning:**
  + Develop and update the annual risk management strategy and compliance roadmap, setting long-term goals and identifying resource requirements.
* **Organization-Wide Audits:**
  + Oversee or coordinate a full-scale, annual audit covering all aspects of compliance and risk management to identify systemic weaknesses.
* **Regulatory Compliance Review:**
  + Ensure that the organization’s policies, controls, and procedures are fully aligned with all applicable laws and regulations, preparing for external audits.
* **Executive Reporting and Board Briefings:**
  + Prepare a comprehensive annual report detailing risk assessments, audit results, compliance incidents, and the overall risk posture; present these findings to executive leadership and the board.
* **Budgeting and Resource Allocation:**
  + Develop the annual budget for compliance and risk management initiatives, including investments in tools, training, and process improvements.
* **Training and Certification Programs:**
  + Launch organization-wide training programs and certification updates to ensure all relevant personnel are up-to-date with the latest risk and compliance best practices.
* **Long-Term Partnership and Vendor Reviews:**
  + Review existing relationships with external auditors, regulatory consultants, and risk management vendors; plan for renewals or adjustments for the upcoming year.

## User Support and Engagement Specialist

**Ad Hoc Responsibilities**

* **Urgent Issue Resolution:**
  + Respond immediately to high-priority support tickets or escalated user issues that could impact productivity.
  + Coordinate with technical teams (IT, DevOps, or Security) to resolve critical incidents.
* **Ad Hoc Training & Communications:**
  + Develop and distribute impromptu guides or announcements when new GitHub features are released or when unexpected changes occur.
  + Address one-off requests for custom support or user training sessions.
* **Knowledge Base Updates:**
  + Quickly update FAQs, internal documentation, or troubleshooting guides when new issues or common questions are identified.

**Daily Responsibilities**

* **Monitoring and Response:**
  + Actively monitor support channels (e.g., helpdesk systems, email, chat platforms) and promptly respond to user queries.
  + Log and track issues in the ticketing system, ensuring timely follow-up and resolution.
* **User Engagement:**
  + Engage with users to collect real-time feedback on system performance, usability, and emerging issues.
* **Documentation:**
  + Record recurring issues and document solutions to build a repository of best practices.
* **Communication:**
  + Update internal communication channels with quick tips, reminders, or status updates to keep users informed.

**Weekly Responsibilities**

* **Support Ticket Review:**
  + Analyze open and closed support tickets to identify trends, recurring issues, and potential areas for improvement.
* **Team Sync-Ups:**
  + Participate in or lead weekly meetings with the support team and key stakeholders to review support metrics and address systemic challenges.
* **Reporting:**
  + Compile a weekly summary report of common issues, resolution times, and user satisfaction metrics.
* **Knowledge Sharing:**
  + Host brief Q&A sessions or “office hours” to address frequently asked questions and encourage user interaction.
* **Feedback Loop:**
  + Follow up with users who experienced recent issues to ensure their concerns were fully addressed and gather feedback on the support process.

**Monthly Responsibilities**

* **Documentation and Resource Updates:**
  + Conduct a monthly review of the support documentation, FAQs, and training materials, updating them based on the latest feedback and system changes.
* **User Training Sessions:**
  + Organize and deliver targeted webinars or interactive workshops on common challenges, best practices, or new features.
* **Performance Metrics Analysis:**
  + Analyze monthly support metrics (e.g., average response time, ticket resolution rates, user satisfaction scores) and identify areas for process improvement.
* **Cross-Functional Collaboration:**
  + Collaborate with teams like IT, Development, and Security to discuss feedback and coordinate on initiatives to improve the overall user experience.
* **Proactive Outreach:**
  + Initiate outreach to new users or teams to provide onboarding assistance and ensure they are effectively using GitHub tools.

**Quarterly Responsibilities**

* **Comprehensive User Feedback Surveys:**
  + Design and distribute detailed surveys or conduct focus groups to assess user satisfaction, identify pain points, and collect suggestions for improvement.
* **Process Review and Improvement:**
  + Evaluate support processes and escalation procedures, then update policies and workflows based on trends and feedback.
* **Training Program Evaluation:**
  + Review the effectiveness of training sessions and educational initiatives; plan and schedule updates to address identified gaps.
* **Interdepartmental Workshops:**
  + Organize joint sessions with key departments to align on support strategies, share success stories, and discuss challenges that impact user engagement.
* **Metric Deep-Dive:**
  + Perform a quarterly analysis of support metrics and engagement trends, using the insights to refine support strategies and service-level objectives.

**Annual Responsibilities**

* **Strategic Planning and Roadmap Development:**
  + Develop an annual strategy and roadmap for user support and engagement initiatives that align with organizational goals.
* **Comprehensive Performance Review:**
  + Conduct an in-depth review of support performance over the past year, including ticket resolution trends, user satisfaction, and overall impact on productivity.
* **Major Training and Engagement Events:**
  + Plan and execute large-scale events such as user conferences, training summits, or hackathons to promote best practices and enhance community engagement.
* **Budget and Resource Planning:**
  + Evaluate the annual budget, determine resource needs for the support team, and plan for future investments in tools and training programs.
* **Executive Reporting:**
  + Prepare and present an annual report for executive leadership that outlines support achievements, challenges, key metrics, and strategic recommendations for the coming year.
* **Knowledge Base Overhaul:**
  + Conduct a full audit of the support documentation and resources, then update or reorganize the knowledge base to ensure it remains current and user-friendly.

## Collaboration and Integration Specialist

**Ad Hoc Responsibilities**

* **Emergency Troubleshooting:**
  + Rapidly address integration outages or failures between GitHub and collaboration tools (e.g., Slack, Jira, Teams) when critical workflows are disrupted.
  + Work with vendor support or internal IT teams to diagnose and fix unexpected integration issues.
* **Onboarding New Tools or Integrations:**
  + Evaluate, test, and deploy new collaboration platforms or integrations as business needs arise.
  + Create quick proof-of-concept implementations to validate the feasibility of emerging tools.
* **Ad Hoc Process Enhancements:**
  + Implement immediate process improvements or custom automations to streamline communication across platforms in response to user feedback.
* **Crisis Communication Support:**
  + Assist in coordinating communication flows during incidents by quickly integrating or configuring temporary solutions.

**Daily Responsibilities**

* **Integration Health Monitoring:**
  + Check the status of all active integrations between GitHub and collaboration platforms using dashboards and automated alerts.
  + Monitor logs and error reports to ensure smooth data flow and timely synchronization.
* **User Support and Issue Resolution:**
  + Respond to immediate queries and troubleshoot issues from users related to integrated tools.
  + Validate that notifications, webhooks, and automated workflows are functioning as intended.
* **Status Updates and Communication:**
  + Provide daily updates to relevant teams on the status of integrations and any minor issues or maintenance being performed.
* **Quick Documentation Fixes:**
  + Make rapid updates to internal documentation or FAQs to reflect any changes in integrations or to clarify new workflows.

**Weekly Responsibilities**

* **Performance and Usage Reporting:**
  + Generate and review weekly reports detailing integration performance metrics, usage statistics, and error rates.
  + Identify trends or recurring issues that may require deeper analysis or process improvements.
* **Routine System Checks:**
  + Perform manual checks on key integration points to confirm that automated processes are running smoothly.
* **Team Collaboration Meetings:**
  + Participate in weekly cross-functional meetings with development, IT, and business teams to review integration status, discuss upcoming changes, and plan enhancements.
* **Documentation Reviews:**
  + Update user guides, runbooks, and integration documentation based on recent changes, feedback, or incidents.
* **Feedback Sessions:**
  + Collect feedback from end users and stakeholders regarding the effectiveness of current integrations and potential areas for improvement.

**Monthly Responsibilities**

* **Comprehensive Integration Audits:**
  + Conduct detailed audits of all integrations to verify configuration accuracy, data integrity, and adherence to organizational policies.
  + Evaluate whether existing integrations continue to meet business needs or if adjustments are required.
* **Tool and Process Evaluations:**
  + Review the performance and functionality of current collaboration tools and integrations; research and propose upgrades or alternatives if necessary.
* **Cross-Departmental Reviews:**
  + Organize monthly check-ins with key stakeholders from different departments to assess integration satisfaction and alignment with business workflows.
* **Training and Best Practices:**
  + Lead or coordinate training sessions for users on how to effectively utilize integrated tools and adopt best practices for interdepartmental collaboration.
* **Documentation and Process Improvement:**
  + Update standard operating procedures (SOPs) and technical documentation to reflect lessons learned and new integrations or updates.

**Quarterly Responsibilities**

* **Strategic Integration Reviews:**
  + Conduct a deep-dive analysis into the overall integration landscape, including performance, scalability, and security aspects.
  + Assess how well current integrations support business objectives and plan for any necessary enhancements.
* **Process Optimization Workshops:**
  + Organize cross-functional workshops to discuss integration challenges and collaboratively design more efficient workflows.
* **Security and Compliance Checks:**
  + Evaluate integrated systems for compliance with security policies and regulatory requirements; adjust configurations or processes to address any gaps.
* **Vendor and Technology Assessments:**
  + Review vendor performance and evaluate new technologies or features that could improve integration capabilities.
* **Innovation Initiatives:**
  + Pilot new tools or automation techniques that could further streamline collaboration across platforms, gathering feedback for future implementation.

**Annual Responsibilities**

* **Long-Term Roadmap Development:**
  + Develop and update a strategic roadmap for collaboration and integration initiatives, aligning with overall digital transformation and IT strategies.
  + Set annual goals, priorities, and investment plans for upgrading or expanding integration capabilities.
* **Comprehensive System Review:**
  + Perform a full-scale review of all integrations and collaboration tools, assessing their performance, security, and ROI over the past year.
  + Identify redundant or obsolete integrations and plan for decommissioning or replacement.
* **Budgeting and Resource Planning:**
  + Prepare the annual budget for collaboration and integration initiatives, including costs for tools, training, and vendor contracts.
* **Executive Reporting:**
  + Compile an annual report summarizing integration performance, key achievements, challenges, and strategic recommendations for senior leadership.
* **Organization-Wide Training and Awareness:**
  + Plan and execute a major training or awareness campaign on collaborative best practices and the effective use of integrated tools across the organization.
* **Policy and Compliance Reviews:**
  + Collaborate with compliance and risk teams to update policies related to data flow, integration security, and cross-platform communication to ensure alignment with regulatory changes.