“RISK-BASED GREEN DEVSECOPS: A RISK-MATURITY ASSESSMENT FRAMEWORK FOR SECURE, CLIMATE-CONSCIOUS CLOUD OPERATIONS”

Research Paper

Ashwini Kumar Rath, Batoi Research, Bhubaneswar, India, ashwini.rath@batoi.com

”Abstract”

Software development and IT operations can have significant environmental footprints that are often overlooked. As organizations face new sustainability regulations and stakeholder pressures, there is a critical need to integrate “green” practices into DevSecOps workflows without sacrificing agility or security. This paper presents a Risk-Maturity Assessment Framework (RMAF) for Green DevSecOps that embeds ecological sustainability into DevSecOps risk management. RMAF enables organizations to assess their sustainability maturity across governance, process, technology, and culture dimensions, and provides a structured path for continuous improvement. The framework is aligned with emerging compliance requirements (e.g., EU CSRD) and corporate ESG goals, ensuring that DevSecOps teams can meet reporting obligations while improving efficiency. We outline the RMAF’s components, scoring methodology, and alignment with DevSecOps principles, and propose an evaluation approach via a small enterprise case study. The paper provides practical insights for integrating sustainability into software engineering practice, aligning with current policy mandates.

Keywords: DevSecOps, Sustainability Metrics, Risk Management, CSRD, ESG, Cloud Software Engineering.

1 Introduction

Modern software delivery pipelines (DevSecOps) emphasize speed and security but traditionally overlook environmental sustainability. The carbon footprint of the technology industry is growing, with data centers, continuous integration builds, and cloud deployments consuming a significant amount of energy. In response, businesses are increasingly motivated by climate goals and regulations aimed at reducing IT-related emissions. For instance, the EU’s Corporate Sustainability Reporting Directive (CSRD) now requires organizations to track and report emissions (European Commission, 2023). Likewise, investors and customers are pressuring firms to meet Environmental, Social, and Governance (ESG) criteria (Calero, Moraga, and García, 2022). However, the existing DevSecOps approaches lack structured methods for measuring and mitigating environmental effects across development and operations. This gap leaves organizations unsure of how to integrate green computing into their agile, security-focused workflows.

To address this challenge, our recent doctoral research introduced structured frameworks that embed sustainability metrics and risk evaluation in DevSecOps. In particular, we developed a Risk-Maturity Assessment Framework (RMAF) to evaluate an organization’s “green” maturity in DevSecOps and guide improvements. By leveraging familiar risk/maturity concepts, RMAF helps teams systematically identify sustainability gaps and progress toward optimized eco-efficient operations.

This study focuses on RMAF and its application in the context of Green DevSecOps. We begin by explaining the policy context and motivation for this framework (Section 2), including regulatory drivers such as CSRD and ESG. Section 3 outlines the methodology for the development of RMAF.

In Section 4, we detail the RMAF structure, including its maturity dimensions, scoring system, and examples of maturity levels in practice. We also discuss how RMAF aligns with DevSecOps principles and differs from previous models. Section 5 maps the elements of the framework to CSRD requirements and ESG objectives, demonstrating alignment with compliance. In Section 6, we propose an evaluation plan for RMAF through a case study in a small to medium-sized enterprise (SME) environment, illustrating its applicability. We then consider the implications for industry practitioners in Section 7. Finally, Section 8 discusses the limitations of this study and future work.

2 Policy Context and Motivation

Global policy trends and corporate sustainability commitments are key drivers for the integration of environmental concerns into DevSecOps. The European Green Deal and associated regulations such as the Corporate Sustainability Reporting Directive (CSRD) signal a new era of accountability for software-intensive organizations. The CSRD requires businesses to track and publicly report carbon emissions and environmental impacts. This prompts firms to integrate sustainability metrics into their IT and software development process. By adopting frameworks such as the Green Metrics Framework (GMF) and the Risk-Maturity Assessment Framework (RMAF), organizations can align with these sustainability policies while simultaneously improving software efficiency. In other words, regulatory compliance and software performance goals can go hand-in-hand; for example, reducing energy waste in CI/CD pipelines not only cuts emissions but can also lower cloud costs (an efficiency gain).

Beyond regulatory mandates, the ESG agenda motivates companies to demonstrate responsible technological practices. Investors and boards are increasingly evaluating how IT operations align with Environmental, Social, and Governance (ESG) goals. In the software domain, this translates to optimizing infrastructure and processes to minimize environmental impacts as part of good governance. Thus, an organization’s software delivery process should be able to produce data on energy usage and carbon footprint per release, among other metrics, to inform ESG disclosure.

These policies and stakeholder pressures motivated the RMAF. Organizations require a practical framework to assess their current sustainability maturity and a roadmap to enhance it in alignment with external expectations. RMAF achieves this by integrating sustainability into risk management, helping companies proactively manage climate-related and environmental risks within their DevSecOps workflow. The framework also addresses compliance officers and auditors: a high RMAF maturity can serve as evidence that a company has robust processes in place to support CSRD reporting and ESG performance tracking.

3 Methodology

The Risk-Maturity Assessment Framework (RMAF) was developed through a rigorous research process that combined insights from the literature and empirical data. We employed a mixed-methods research design to explore the integration of sustainability into DevSecOps. This approach involved two phases.

- *Qualitative Exploration:* We conducted semi-structured interviews with DevSecOps professionals and sustainability experts to identify the challenges, risks, and best practices for “green” DevSecOps. These interviews provided nuanced insights into organizational barriers (e.g., cultural resistance and lack of tools) and helped identify essential sustainability metrics and governance issues. The qualitative phase was invaluable for uncovering themes such as the absence of standardized green metrics (Lago, Gu, and Bozzelli, 2014) and the perception that sustainability can conflict with performance deadlines.
- *Quantitative Analysis:* To validate and generalize the qualitative findings, we designed and distributed surveys to a broader sample of IT professionals. The surveys measured the prevalence of identified practices and challenges across organizations and industries. This confirmatory analysis quantified the prevalence of specific issues, such as the percentage of

firms that monitored energy usage in CI pipelines or the number of firms that had sustainability included in their risk registers. By statistically analyzing these data, we prioritized the most critical factors to be addressed in the framework.

The insights from both methods were then integrated to construct the RMAF. We combined the interview themes (e.g., the need for governance policies, automation of green metrics, and cultural training) with the survey trends, and these insights were then integrated with existing maturity model concepts. Notably, we drew on established risk and security maturity models, such as the RIMS Risk Maturity Model and the OWASP DevSecOps Maturity Model (RIMS, 2015; OWASP, 2023), as a foundation for our approach. Adapting elements from these models ensured that RMAF built upon proven structures for capability maturity, while extending them to include sustainability. The development process involved iterative refinement, in which we validated the draft framework against participant feedback and case observations to ensure that it was both practically viable and grounded in empirical data. This resulted in a framework that was both theoretically robust and actionable, addressing the identified gaps with evidence-driven components.

Finally, the RMAF and its companion, the Green Metrics Framework (GMF), were conceptually evaluated within the thesis work by mapping them to known problem areas and using a small-scale case implementation of green metrics to illustrate their potential impact. Although a full industrial trial of RMAF was outside the scope of this thesis, the framework's content was firmly grounded in real-world input and aligned with the current policy directives. The following sections detail the RMAF and its applications.

4 The Risk-Maturity Assessment Framework (RMAF)

The Risk-Maturity Assessment Framework (RMAF) provides a structured approach to evaluating and enhancing an organization's sustainability integration in DevSecOps. It extends traditional maturity models to security and risk management by explicitly adding ecological sustainability as a key risk dimension. RMAF posits that managing the environmental impact should be part of the DevSecOps risk posture, alongside managing security vulnerabilities and operational risks. The framework defines a maturity model with multiple dimensions and levels, enabling organizations to benchmark their current state and plan progression toward more sustainable DevSecOp practices.

4.1 Maturity dimensions

The RMAF evaluates organizational readiness across four key dimensions, each addressing an essential aspect of sustainable DevSecOps, as illustrated in Figure 1.

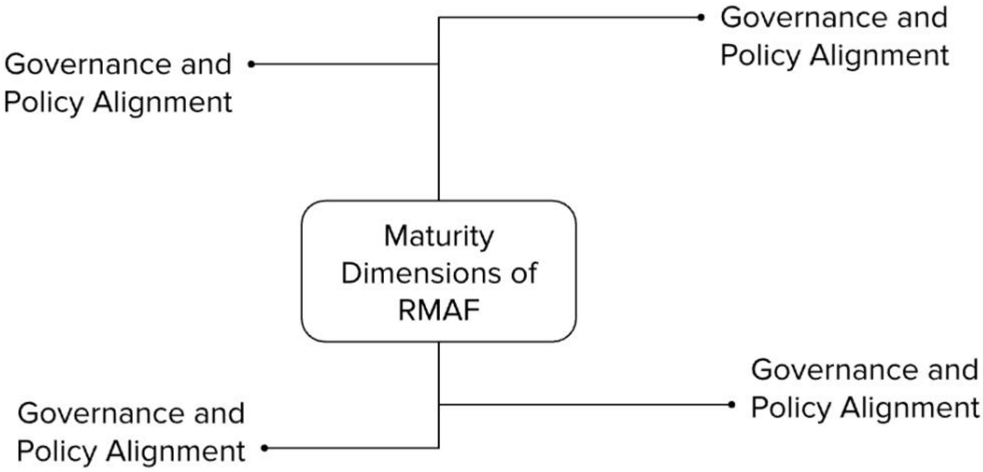
Governance and Policy Alignment
Governance and Policy Alignment
Maturity Dimensions of RMAF
Governance and Policy Alignment
Governance and Policy Alignment

Figure 1. Four Maturity Dimensions of the Risk-Maturity Assessment Framework (RMAF)

Let us now discuss each of these four dimensions:

1. *Governance and Policy Alignment:* Measures the extent to which sustainability is embedded in governance structures and policies for software development. At higher maturity, organizations have formal policies and corporate IT strategies that integrate sustainability objectives (e.g., carbon reduction targets) and treat them on par with security and quality policies. For example, a mature organization might require sustainability risk assessments as part of project governance and include sustainability criteria in compliance audits.
2. *DevSecOps Process Integration:* Assesses how well sustainability practices and metrics are incorporated into DevSecOps pipelines and workflows. It encompasses the automation of green computing metrics in CI/CD, building on prior reviews of sustainability metrics in software engineering (Lago, Gu, and Bozzelli, 2014), the optimization of deployments for energy efficiency, and the inclusion of sustainability checks in release processes. A low-maturity organization may only occasionally discuss sustainability. In contrast, a high-maturity one continuously monitors energy use in buildings and employs sustainability-aware security protocols (ensuring that security measures themselves do not waste resources).
3. *Technology and Automation Readiness:* Evaluate the use of tools and technology for automated sustainability monitoring and improvement. This dimension aligns with DevSecOps's emphasis on automation and continuous monitoring. It examines whether the organization has instrumented its infrastructure and applications by monitoring power, CPU, and carbon metrics, and whether it leverages advanced techniques (e.g., AI-driven analytics) to optimize resource usage in real-time. Mature teams have dashboards for sustainability KPIs and automated alerts for inefficiencies, whereas low-maturity teams lack such tooling.
4. *Cultural and Organizational Adoption:* Examines human and organizational factors – the extent of sustainability mindset and practices in the team's culture. This includes leadership support for green initiatives, team training in sustainable coding practices, and cross-functional collaboration to achieve environmental goals. Research indicates that cultural resistance is a significant barrier to the adoption of green DevSecOps (Lago, 2019; Bogdanović et al., 2013). Thus, the RMAF assesses whether teams prioritize eco-friendly practices or whether sustainability is still seen as beyond their scope. High maturity in this dimension means that sustainability is an integral part of the DevSecOps ethos, and employees at all levels are incentivized to enhance environmental performance.

4.2 Maturity levels and scoring

RMAF defines five maturity levels (Ad Hoc, Reactive, Defined, Managed, Optimized) that describe the progression of sustainability integration. These levels mirror typical capability maturity models but are tailored to green DevSecOps. Table 1 summarizes the maturity levels of the RMAF with their general characteristics and key indicators.

Level (Score)	Description	Key Indicators
Level 1 – Ad Hoc (Score: 1–2)	No structured sustainability practices in DevSecOps. Sustainability is often overlooked or addressed in an ad hoc, uncoordinated manner.	- No policies or objectives related to sustainability - No automation of environmental metrics - General lack of awareness among staff
Level 2 – Reactive (Score: 3–4)	Some awareness of sustainability, but efforts are reactive rather than proactive. Actions are taken in response to issues or external prompts, rather than through a planned strategy.	- Use of a few basic tools (e.g., simple energy monitoring) on occasion - Sustainability discussions happen only after incidents or when convenient

Level 3 – Defined (Score: 5–6)	Sustainability metrics and practices are being defined and are beginning to be standardized. The organization has set sustainability goals and initiated automation on a small scale.	- Key green metrics identified and regularly tracked (e.g., carbon footprint per build) - Sustainability considerations are integrated into DevSecOps policies and documentation
Level 4 – Managed (Score: 7–8)	Sustainability is managed with continuous monitoring and improvement. Practices are refined based on metrics, ensuring clear accountability for sustainability outcomes.	- Automated tracking of energy and resource use in CI/CD is in place - Sustainability is part of DevSecOps compliance and risk management processes (treated similarly to security).
Level 5 – Optimized (Score: 9–10)	Sustainability is fully embedded and continuously optimized through the use of innovative techniques. The organization is a leader, continually refining processes for maximum sustainability without external prompting.	- Predictive analytics and AI are used for proactive energy optimization (Haugsvær, 2023) - Near-real-time sustainability monitoring; organization shares best practices industry-wide

Table 1. RMAF Maturity Levels and Key Indicators. Each level corresponds to an increasing integration of sustainability into DevSecOps processes, from negligible (Level 1) to highly optimized (Level 5).

To apply RMAF in practice, an organization would assess its DevSecOps processes against the criteria of each level and dimension. The framework also introduces a quantitative scoring system to enhance objectivity and accuracy. In our design, maturity can be scored on a scale (1–10) and broken down by weighted factors, for example:

- *Carbon footprint tracking* – weighted 25% (e.g., whether and how well the team measures carbon emissions of their software/infrastructure).
- *Energy consumption impact* – weighted 30% (how actively energy efficiency is monitored and improved).
- *Operational resource optimization* – weighted 20% (efforts to optimize computing resources, reduce wasteful provisioning, etc.).
- *Security and compliance factors* – weighted 25% (ensuring sustainability efforts do not undermine security, and that processes meet compliance requirements).

These weights (which sum to 100%) reflect a balanced emphasis, with a slightly higher weight on direct energy/carbon metrics (55% combined), recognizing their importance, and a substantial weight on maintaining security/compliance (since green initiatives must integrate with existing DevSecOps obligations). Using this scoring, an organization might compute an overall "sustainability maturity score." For instance, a company scoring 6.5/10 may be considered mid-level (between Defined and Managed). The scoring approach enables benchmarking and precise gap analysis, allowing a team to identify which component (e.g., automation vs. culture) is dragging their score down and target improvements accordingly. It also enables progress tracking over time or by comparing business units.

4.3 Alignment with DevSecOps principles

Importantly, RMAF is designed so that adopting it will reinforce DevSecOps' best practices, not detract from them. RMAF supports the key DevSecOps principles of DevSecOps, as follows.

- *Automation:* DevSecOps relies on automation to achieve consistency and speed. RMAF strongly encourages automated tracking of sustainability metrics (e.g., auto-logging energy use per test run) to ensure real-time visibility of the environmental impact. By embedding these checks into the CI/CD pipelines, teams extend their automation culture to cover sustainability.

- *Continuous Monitoring:* As security or performance metrics are continuously monitored, RMAF pushes for continuous sustainability monitoring. At higher maturity, organizations integrate sustainability data into their monitoring dashboards and security information and event management (SIEM) tools. This ensures that environmental indicators are monitored with the same vigilance as uptime or security events, enabling quick responses to inefficiencies.
- *Risk Management*: DevSecOps fosters a mindset for managing risk (particularly security risk) throughout development. RMAF augments this by adding quantitative sustainability risk scoring along with traditional risk metrics. For example, high-power usage is a risk that needs to be mitigated, similar to a high-severity security vulnerability. This integration ensures that sustainability considerations are formally incorporated into the risk assessment matrix, facilitating more holistic decision-making.
- *Collaboration and Culture:* A DevSecOps principle involves breaking silos and building a culture of shared responsibility. RMAF assesses and cultivates a sustainability-aware culture, ensuring that developers, operations, and security teams prioritize green computing. It encourages cross-functional collaboration (e.g., ops sharing energy data with devs to optimize code) and highlights the role of leadership and training in driving cultural change.

This alignment also ensures that improving environmental maturity will not compromise security or agility.

4.4 Adoption process and benefits

To implement RMAF, organizations can follow a structured process:

- *Self-Assessment:* First, an internal assessment was performed using the RMAF maturity model. Key stakeholders, including DevOps engineers, security leads, and sustainability officers (if applicable), evaluate current practices against the framework criteria. It identifies the organization's current maturity level in each dimension and pinpoints gaps. For example, the assessment might reveal that while automation (Dimension 3) is strong, cultural adoption (Dimension 4) lags with low awareness among developers.
- *Strategic Roadmap Development:* Based on the assessment findings, the organization formulates a roadmap for improvements. This plan should establish short- and long-term goals for advancing maturity levels aligned with business strategies. For instance, if the goal is to reach Level 4 (managed) within two years, the roadmap might include introducing energy-monitoring tools in the next quarter, integrating sustainability into QA criteria by the end of Q4, and conducting training workshops for staff. The roadmap ensures that sustainability objectives are tied into the DevSecOps strategy and product roadmaps, rather than being treated as ad hoc fixes.
- *Integration into Risk Management:* The RMAF outcomes are then embedded into the organization's broader risk management and governance frameworks. Sustainability risks (e.g., "excess carbon emissions per user transaction" or "inefficient resource usage leading to high costs and footprint") should be recorded in risk registers and treated on par with cybersecurity risks. It may involve updating risk assessment templates to include an environmental risk section and ensuring that oversight bodies (such as risk committees or CIO/CTO) review sustainability risk indicators regularly. By institutionalizing it, improvements are maintained and audited, reinforcing accountability.

By following these steps, organizations can gradually increase their maturity. The benefits of implementing RMAF, as observed in our research, include the following.

- *Improved Visibility and Tracking:* Teams gain significantly better insight into their green metrics, including energy use, carbon footprint, and other environmental metrics within

DevSecOps environments. This data-driven approach enables the identification of inefficiencies (e.g., a test suite consuming disproportionate CPU resources) and the tracking of improvements over time.

- *Alignment of Security, Risk, and Sustainability Goals:* RMAF helps break the notion that sustainability is separate from the core DevSecOps. Organizations achieve a better alignment between security, risk management, and sustainability objectives, leading to more cohesive policies. For instance, a change management process may simultaneously check for security impact and environmental impacts.
- *Higher DevSecOps Maturity Overall:* Participants reported that incorporating sustainability actually enhanced their DevOps maturity, driving more automation, more careful resource management, and improved cross-team communication. In effect, striving for level 5 optimization in sustainability often synergizes with optimizing performance and reliability, thus scaling and hardening the entire pipeline.
- *Compliance Readiness and Reputation:* Although not a direct "technical" benefit, being at a high RMAF maturity positions a company advantageously for regulatory compliance and demonstrating ESG leadership. It can simplify the process of collecting data for sustainability reports (CSR/CSRD reports) and reassure stakeholders that the company systematically manages environmental risks. This can improve brand reputation and stakeholder trust.

Next, we discuss how RMAF maps to specific compliance frameworks (CSRD) and ESG criteria, before outlining how one might evaluate the framework in a real-world SME setting.

5 Compliance Mapping (CSRD and ESG)

One of RMAF's strengths is that it bridges the gap between technical practices and compliance requirements in sustainability. Here we map the framework's elements to the Corporate Sustainability Reporting Directive (CSRD) and broader ESG goals to illustrate alignment:

- *Carbon and Energy Metrics → CSRD Environmental Disclosures:* CSRD mandates that companies disclose their greenhouse gas emissions, energy usage, and other environmental impacts in their annual reports (European Commission, 2023). RMAF directly supports this by ensuring that organizations have processes in place to capture these metrics. Firms implement automated carbon footprint tracking and energy monitoring in their pipelines through progress in the DevSecOps Process Integration and Technology Automation dimensions. At a higher maturity, carbon accounting is built into software operations, making it straightforward to gather accurate data for CSRD reports. In short, an organization at RMAF Level 4 or 5 will inherently collect the data that CSRD compliance requires (e.g., total cloud energy consumption and carbon per deployment) as part of its continuous monitoring.
- *Governance and Risk Alignment → CSRD Strategy and Risk Sections:* The CSRD not only requires raw metrics but also an explanation of how sustainability risks are managed and integrated into corporate strategy. RMAF's Governance and Policy Alignment dimension ensures that sustainability is woven into IT governance, risk management, and corporate policies. For example, companies at high maturity have sustainability objectives in their IT strategies and report environmental risks in their risk filings. It directly feeds into the CSRD's requirement to describe sustainability risk management approaches. An RMAF-mature organization can demonstrate that it has a formal framework (RMAF itself) to assess and improve sustainability, which would strengthen its CSRD disclosures on governance and strategy.
- *Sustainability Risk Scoring → EU Taxonomy and ESG Ratings:* The EU Taxonomy for sustainable activities and many ESG rating schemes require quantification of environmental performance and risk. RMAF's quantitative scoring (with weighted factors, such as carbon

and energy) provides a mechanism to numerically assess environmental risk maturity, which can be translated into internal KPIs or scores for ESG reporting. For instance, if a company tracks its RMAF score improving from 4/10 to 7/10 over three years, it can communicate this improvement in ESG reports as evidence of building the capacity to manage environmental issues. While RMAF is not an externally recognized score, such as an ESG rating, it can serve as an internal proxy that underpins external disclosures.

- *Cultural Adoption and Social Governance:* The ESG framework's "Social" and "Governance" aspects include how well a company engages employees in sustainability and how governance bodies oversee these efforts. RMAF addresses this by evaluating cultural and organizational options; a high score here implies strong employee engagement and training on sustainability, which aligns with social responsibility expectations. Additionally, having sustainability integrated in governance (part of dimension 1) means boards and executives are involved, aligning with the "Governance" aspect of ESG. In effect, by implementing RMAF, an organization operationalizes the "G" of ESG for environmental issues, creating governance structures and accountability for its sustainability performance.
- *Regulatory Compliance as Opportunity:* Rather than viewing CSRD compliance as a separate overhead, RMAF helps to reframe it as part of the DevSecOps improvement journey. By adopting RMAF, organizations preemptively build capabilities demanded by upcoming regulations. For example, if a new law requires software teams to consider energy efficiency (much like accessibility or security), those following RMAF would already have an advantage. This alignment can also yield competitive benefits – organizations that can comply and demonstrate concrete sustainability maturity swiftly may gain a preference in contracts (as clients and partners start to evaluate suppliers on ESG criteria) and avoid potential penalties or brand damage from non-compliance.

6 Suggested Evaluation Plan: SME-Based Case Study

To illustrate the applicability of RMAF and refine it further, we propose a case study evaluation in the context of a Small or Medium-sized Enterprise (SME). SMEs are fascinating test beds for RMAF because, as our research noted, they often face resource constraints when implementing sustainability initiatives. Many SMEs lack dedicated sustainability teams or substantial budgets for new tools, making it challenging for them to adopt frameworks such as RMAF despite their potential benefits. By conducting a focused case study, we can assess how RMAF can be tailored to an SME's scale and what impact it can have.

Objectives: The evaluation aims to (a) validate that the RMAF is understandable and usable in a real-world setting, (b) measure the improvements (if any) in sustainability metrics and practices after applying RMAF, and (c) identify any adjustments needed to accommodate SME limitations (e.g., simpler scoring methods and open-source tools to reduce cost).

Proposed Case Study Design: Find an SME (e.g., a cloud software startup or a mid-sized fintech company) willing to collaborate. Ideal candidates are those practicing DevSecOps to some degree and expressing interest in improving sustainability (perhaps because of client demands or corporate values).

1. *Baseline Assessment (Pre-RMAF):* Work with the SME to perform an initial RMAF self-assessment. It involves interviewing key team members (DevOps engineers, CTO, etc.) and examining their processes against RMAF criteria. We would determine their current maturity level in each dimension. It's likely an SME might start at Level 1 or 2 in some areas (e.g., they may have no formal policies, reflecting Level 1 Ad Hoc). We also capture baseline quantitative metrics, such as the current average energy consumption per build, the frequency of sustainability-related discussions, and any existing monitoring tools.
2. *Identify Gaps and Tailor Plan:* Using the baseline, identify high-priority gaps. For instance, the assessment may reveal a lack of automation for sustainability metrics and the absence of

governance policies. Together with the SME, set realistic targets (maybe aim to move from Level 1 to Level 3 in one year). Develop a tailored improvement plan. Because cost is a concern for SMEs, the plan would emphasize low-cost or free solutions (like utilizing open-source energy monitoring tools, leveraging existing cloud provider metrics) and incremental process changes rather than significant investments.

3. *Implement Interventions:* Over a period (say 6–12 months), assist or observe the SME as they implement the roadmap. Interventions could include:
   - Establishing sustainability champions in the team to drive cultural change.
   - Integrating a lightweight carbon-tracking script into their CI pipeline (for example, using an API to estimate emissions from resource usage).
   - Introducing a policy that every project must include at least one sustainability KPI.
   - Regular knowledge-sharing sessions on green coding practices.

   The interventions are documented, and any challenges in applying RMAF steps in the SME context are noted (e.g., difficulties in quantifying specific metrics or resistance due to tight release schedules).
4. *Midpoint Check-ins:* Conduct periodic check-ins (monthly or sprint-wise) to measure progress. It could involve conducting brief surveys or interviews to assess whether awareness is increasing (indicating a cultural shift) and utilizing infrastructure data to determine if any efficiency gains are being realized. For instance, by month 6, has the average build energy consumption dropped or stabilized? Are team members more engaged in discussing sustainability in retrospectives?
5. *Post-Implementation Assessment:* After the intervention period, perform a follow-up RMAF assessment using the same framework as in step 2. Determine the new maturity levels and scores. Ideally, we expect to see improvement – perhaps the organization has moved from an overall Level 1– 2 (ad-hoc/reactive) to Level 3 (defined) on most dimensions. We would specifically look for tangible changes such as:
   - Existence of at least one sustainability-related governance document or policy (addressing Governance dimension).
   - Implementation of a monitoring tool or script for energy (Process/Technology dimensions).
   - Evidence of increased team awareness (Culture dimension), via an internal survey of attitudes.

   We also collect final quantitative data: for example, if at baseline a complete CI/CD pipeline run consumed X kWh, has it reduced after optimizations? If they started measuring it, any reductions or more stable resource usage could be attributed to RMAF-inspired changes (such as turning off idle test environments and optimizing code).
6. *Analysis of Outcomes:* Compare pre- and post-data to assess the impact of RMAF. We would analyze improvements in metrics (e.g., any % reduction in energy or carbon per deployment) and enhancements in maturity levels. We'll also evaluate qualitative feedback: what did team members feel about the process? Did RMAF make DevSecOps more complex, or did it integrate well? Notably, we will check if any security or speed regressions occur – the hypothesis is that RMAF should not impede these; in fact, one would hope for neutral or positive side effects on efficiency (e.g., trimming waste can speed up pipelines).
7. *Report and Iterate:* Document the lessons. For example, specific RMAF criteria need clarification for SMEs, or the scoring weights might be adjusted (perhaps SMEs find a 25% weight on security/compliance too high if they have minimal compliance obligations). We also expect to document any creative solutions the SME used, which can be shared as best practices (for example, utilizing existing DevOps tools in innovative ways to gather sustainability data).

By following this case study approach, we can demonstrate the practicality of RMAF. A successful outcome would show that even a resource-constrained SME can make measurable progress in greening their DevSecOps using RMAF as a guide. It would underscore the framework's flexibility and value proposition. On the other hand, any difficulties will inform future refinements. For example, if the SME struggled with the framework's complexity, we might develop a simplified checklist version of RMAF for smaller organizations.

It is worth noting that our research already included a preliminary case where integrating green metrics in a DevOps pipeline led to tangible improvements (e.g., a 15% reduction in energy consumption in one case study). Although this case was not an explicit RMAF evaluation, it gives confidence that measuring and acting on sustainability metrics can yield real benefits. The SME evaluation of RMAF would extend this by examining changes in organizational and process maturity, not just in metrics. Given the identified challenge that SMEs often find sustainability investments costly or secondary, a documented success story could encourage more SMEs to embrace green DevSecOps practices, knowing that there is a clear framework to follow and that improvements can be made progressively without heavy expenditures.

7 Implications for Practice

The introduction of the RMAF has several important implications for software engineering practice and IT management.

- *Embedding Sustainability in DevSecOps as Standard Practice:* RMAF provides a blueprint for integrating sustainability into the "new normal" of DevSecOps. Practitioners can use this framework to systematically include environmental considerations at each stage of software delivery (planning, coding, testing, deployment, and monitoring). This means that teams will start treating metrics such as energy consumption with the same attention as they do security vulnerabilities or uptime. Over time, such integration could lead to the incorporation of sustainability non-functional requirements in projects, the adoption of green coding guidelines, and the inclusion of checklists in deployment pipelines, all of which would become commonplace. The practical implication is that DevSecOps teams need to broaden their skill sets slightly; operations engineers might need familiarity with energy measurement tools, and developers might learn patterns for efficient coding.
- *Risk Management and Compliance Alignment:* For IT risk managers and compliance officers, RMAF shows a way to align IT processes with emerging compliance needs. This translates high-level sustainability mandates into practical, on-the-ground actions. Companies implementing RMAF will find it easier to satisfy auditors and regulators regarding their management of environmental risk. For example, if an audit asks, 'How do you ensure your software operations align with the company's climate targets?', a company with an RMAF can demonstrate a documented maturity model and improvement logs as evidence. This elevates the role of DevSecOps teams in corporate sustainability compliance; they become key contributors to meeting CSRD and similar requirements. It also fosters closer collaboration between technical teams and sustainability governance teams (or CSR departments) because RMAF provides a common language (maturity levels, scores, and risk items) that both teams understand.
- *Efficiency and Cost Benefits:* Green practices advocated by RMAF often have direct operational benefits. By focusing on resource optimization, companies can reduce wasteful computing. In practice, this may entail tuning CI jobs to run off-peak times to use renewable energy, rightsizing cloud resources, or eliminating redundant processes. Many such optimizations save money (e.g., lower cloud bills) in addition to reducing emissions. As noted in our findings, sustainable DevSecOps can lead to energy cost reduction and efficiency savings (Gmach et al., 2010; Bogdanović et al., 2013). Thus, implementing RMAF can reveal opportunities for cost savings. IT managers might find that sustainability initiatives pay for themselves through improved efficiency. A cultural mindset of avoiding waste can also enhance discipline in other areas (e.g., cleaner code and streamlined processes), thereby indirectly improving quality and performance.

- *Holistic DevSecOps Improvement:* RMAF could serve as a lever to drive broader improvements in DevSecOps maturity. Often, when teams examine their processes through the lens of sustainability, they identify general bottlenecks or inefficiencies that they might otherwise have overlooked. For instance, an exercise to track energy usage might reveal a poorly designed test that unnecessarily runs too often; this helps reduce energy consumption and improves pipeline speed. By implementing RMAF, organizations can inadvertently strengthen their overall DevOps practices. We observed that organizations that align security, risk, and sustainability achieve higher maturity in the automation and scaling of DevSecOps.
- *Leadership and Cultural Signal:* Adopting RMAF and publicly committing to sustainable software practices can send a strong positive signal both internally and externally. Internally, it demonstrates to developers and engineers that leadership values sustainable innovation, a move that can boost morale, especially among employees who care about environmental issues. It can spark a culture of innovation in which teams experiment with innovations, such as more efficient algorithms or renewable energy-aware scheduling. Externally, companies can differentiate themselves by marketing their "Green DevSecOps" approach, potentially attracting customers or partners who prioritize sustainability. Given the rising importance of ESG scores, early adopters of frameworks, such as RMAF, could become industry role models.

However, in practice, to realize these implications, organizations must address specific challenges. They must invest in training teams on sustainability concepts, update KPIs to include sustainability targets (so that what gets measured gets done), and perhaps adjust incentives (e.g., recognizing teams or individuals who find ways to improve energy efficiency). Furthermore, tool vendors may begin incorporating sustainability features (for example, CI/CD platforms could natively report carbon footprints per run), spurred by demand from organizations following the RMAF. We may also see more cross-functional collaboration – for example, facilities or data center management working with DevOps teams – to achieve sustainability goals.

8 Limitations and Future Work

Although RMAF represents a novel step toward sustainable software engineering, it is not without limitations. A frank examination revealed areas where further work is required.

- *Limited Empirical Validation:* To date, RMAF has been developed based on the literature and initial field input (including interviews and surveys), but lacks extensive real-world validation. The effectiveness and ease of use of the framework must be tested across different organizations. The proposed SME case study (Section 6) is a single step, but future research should involve multiple case studies or pilot implementations. For example, applying RMAF in a large enterprise versus a startup can reveal scalability issues or the need for customization. Additionally, longitudinal studies could track over a year or more to see if improvements are sustained and if higher maturity truly correlates with better outcomes (e.g., reduced carbon footprint and improved DevOps KPIs). Without such empirical evidence, the framework's presumed benefits are indicative.
- *Scalability and Standardization Challenges:* As highlighted in our conclusions, advancing frameworks such as RMAF requires addressing scalability and standardization issues. Scalability refers to the model's ability to be applied effectively across organizations of various sizes and domains. A very detailed framework may overwhelm small teams, whereas a generic framework may not satisfy the needs of large enterprises. Standardization is another challenge; currently, there is a lack of industry-wide agreed sustainability KPIs for software. RMAF metrics (carbon, energy, etc.) are a starting point, but future work should focus on establishing universal DevSecOps sustainability benchmarks and standards. For instance, the community could agree on a standard way to measure "energy per transaction"

or adopt something akin to an "Energy Star" rating for software. Our framework benefits from alignment with emerging standards, ensuring it remains relevant and credible.

- *Automation and Tooling Gaps:* Implementing RMAF effectively depends on having appropriate tools for monitoring and analysis. One key challenge is the lack of automated sustainability tracking tools for the CI/CD pipelines (Dahab et al., 2016). Many teams still rely on manual analyses or external estimations of carbon footprints. Future research and development efforts should focus on creating or improving tools that automatically gather sustainability data (e.g., plugins for Jenkins/Azure DevOps that output the energy usage of a pipeline run or IDE extensions that flag inefficient code). The integration of AI for predictive sustainability (predicting which deployment strategy would use the least energy, for example) is a promising area. RMAF needs to evolve in tandem with these technological advancements. If, in the future, AI-driven optimization becomes commonplace (Haugsvær, 2023), RMAF's criteria for top maturity may raise the bar to include those capabilities.
- *Breadth of Sustainability Dimensions:* Currently, RMAF, like green IT research, focuses primarily on environmental sustainability (the "E" in ESG). It emphasizes carbon, energy, and resource efficiency. However, software sustainability also has social and economic dimensions that have not yet been explicitly covered. For instance, "social sustainability" could involve considering the broader societal impacts of software or the well-being of employees (such as avoiding burnout, which is indirectly related to sustainable workload). Economic sustainability may consider long-term financial viability and cost savings associated with green practices. While these are tangential to our environmental focus, future work could expand RMAF to incorporate social and economic sustainability factors.
- *Cultural and Organizational Hurdles:* As noted, one of the significant challenges is the organization's culture. Cultural resistance and lack of awareness can significantly impede the adoption of RMAF. Employees may resist changes that they perceive as slowing down their development or adding extra work. Top management may be unconvinced of the ROI of sustainability initiatives. They require change management strategies, executive buy-ins, and industry pressure (or regulatory mandates) to overcome these challenges. Future work could explore techniques such as the gamification of green practices, reward systems, or integrative training that pairs security and sustainability to change mindsets. Additionally, studying how to create urgency around this issue (similar to how security has been elevated because of high-profile breaches) could be valuable.
- *Generalization and Prioritization:* Another limitation of RMAF is that it may need to be tailored to specific contexts. Different industries have distinct sustainability profiles (e.g., a SaaS company versus an embedded systems developer). The framework, in its current form, is generic. Companies might prioritize different metrics: a firm running heavy computations might focus on energy efficiency, whereas one with distributed users might focus on device-side impacts. Future research could develop domain-specific maturity models or versions of RMAF. Alternatively, the framework could be kept flexible with guidance on how to adjust weightings or criteria based on the context. Another possible future direction is to integrate RMAF with existing process improvement models (such as CMMI or ISO standards), which could help formalize it and adapt it to various contexts.
- *Need for Community and Ecosystem Support:* For RMAF (or any sustainability framework) to take hold truly, it needs support from the broader tech ecosystem. This includes integration into popular DevOps frameworks, references in practitioner guides, and endorsements by industry groups. One limitation is the lack of widespread awareness; many practitioners are unaware that such frameworks exist, as sustainability in software remains an emerging field of study.

Although RMAF is a promising step, it should be viewed as a starting point for further development. We demonstrated its conceptual feasibility and alignment with key needs; however, continuous refinement was necessary. The research community and industry practitioners are encouraged to experiment with the RMAF, provide feedback, and contribute to its evolution. Our study suggests many avenues, from technical tool development to cultural change techniques, that require attention. The ultimate goal is to have a robust, widely adopted framework for sustainable DevSecOps, and RMAF could be a precursor to this. Achieving this will be an ongoing journey that parallels the continuous improvement ethos of DevOps.

References

Bogdanović, Z. et al. (2013) 'The Role of DevOps in Sustainable Enterprise Development', *in Sustainability: Cases and Studies in Using Operations Research and Management Science Methods.* Cham: Springer International Publishing, pp. 217–237.

Calero, C., Moraga, M.Á. and García, F. (2022) 'Software, Sustainability, and UN Sustainable Development Goals', *IT Professional*, 24(1), pp. 41–48. DOI: 10.1109/MITP.2021.3117344.

Dahab, S. et al. (2016) 'A learning-based approach for green software measurements', *In: MEGSUS 2016: 3rd International Workshop on Measurement and Metrics for Green and Sustainable Software Systems*, September 2016, Ciudad Real, Spain. pp. 13–22. HAL. Available at: https://hal.science/hal-01387475v1 (Accessed: 9 September 2025).

European Commission (2023) *European Green Deal and Corporate Sustainability Reporting Directive (CSRD)*. Brussels: European Commission. Available at: https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en (Accessed: 9 September 2025).

Gmach, D. et al. (2010) 'Profiling Sustainability of Data Centers', *in Proceedings of the 2010 IEEE International Symposium on Sustainable Systems and Technology, –6.* DOI: 10.1109/ISSST.2010.5507750 (Accessed: 9 September 2025).

Haugsvær, S.B. (2023) *Sustainable BizDevOps: A novel methodology for reducing the carbon footprint of web products*. NTNU. Available at: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3079159 (Accessed: 9 September 2025).

Lago, P. (2019) 'Architecture Design Decision Maps for Software Sustainability', *in 2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS), pp. 61–64.*

Lago, P., Gu, Q. and Bozzelli, P. (2014) 'A systematic literature review on green software metrics'. *VU University Amsterdam.* Available at: https://research.vu.nl/ws/portalfiles/portal/910331/SLR%20GreenMetrics.pdf (Accessed: 9 September 2025).

OWASP (2023) 'OWASP DevSecOps Maturity Model (DSOMM)'. *Open Web Application Security Project.* Available at: https://owasp.org/www-project-devsecops-maturity-model/ (Accessed: 9 September 2025).

RIMS (2015) 'RIMS Risk Maturity Model (RMM)'. *Risk and Insurance Management Society (RIMS).* Available at: https://www.rims.org/Tools/risk-maturity-model (Accessed: 9 February 2025).