GRC RISK ASSESSMENT TOOL – A WEB BASED PLATFORM FOR RISK IDENTIFICATION AND ANALYSIS

Ms. K. Sindhu
Assistant Professor/ Department of Information Technology
Sri Ramakrishna Engineering College
Coimbatore, India sindhu.k@srec.ac.in

L. Ramanahthan
UG student / Department of Information Technology
Sri Ramakrishna Engineering College **Coimbatore, India** ramanahthan.2205120@srec.ac.in

J. Salmon
UG student / Department of Information Technology
Sri Ramakrishna Engineering College **Coimbatore, India** salmon.2205164@srec.ac.in

T. Sri Krishna
UG student / Department of Information Technology
Sri Ramakrishna Engineering College **Coimbatore, India** srikrishna.2205165@srec.ac.in

Abstract— This tool checks cyber risks without heavy setup. Instead of complex systems, it runs in a browser. Because standards matter, it follows ISO/IEC 27001 and NIST SP 800-30 rules. Users log equipment, possible dangers, how likely they are, what damage could happen - then score shows up by math: Impact times Likelihood decides level. Frontend uses Bootstrap with HTML and CSS; backend relies on Flask plus Python code. Data lives inside SQLite files. A live summary screen tracks current threats. Reports come out as PDFs when needed. Small teams or schools get usable results at low cost. It acts like an early model but still guides real choices about digital safety. After testing, feedback shapes next steps.

I.Introduction

Nowadays, with more work happening online, companies need strong oversight just to stay safe - because cyber dangers grow sharper every day, rules tighten constantly, while reliance on tech deepens without pause. Critical resources demand clear tracking first; only then can possible attacks be weighed carefully against weak spots hiding within systems. Ongoing checks of danger levels keep operations steady, plus they help meet laws that never stop changing. When protections lack shape or direction, money often drains unexpectedly, public trust slips quietly, and fines arrive through official channels. Spreadsheets handled by hand tend to slip up when tracking risks across departments. One wrong entry here can throw everything off later down the line.
Updating those files feels like chasing shadows - always behind, never caught up. Seeing the full picture? Nearly impossible without connected systems feeding clear data. Score how bad a threat might get? Without agreed-upon rules, guesses replace judgment. Leaders end up spreading efforts too thin because priorities blur together. Choices made in isolation leave holes others don't even know exist. Governance falters when nothing ties actions back to real exposure levels.

One way to tackle these issues? A central GRC Risk Assessment Tool built around clear visuals and structure. This setup guides people through logging assets while linking possible threats step by step. Instead of guesswork, it uses a math-style score - Likelihood times Impact - to show how serious each danger might be. Visuals like dashboards pop up with color-coded patterns, giving quick insight into where risks pile up. From there, teams see the big picture without digging through reports. Seeing risk this way sharpens judgment when choosing next steps.

A small version of the app runs on a basic local database, built just enough to test core functions. One feature pulls together records automatically, shaping them into clear reports meant for audits. These outputs help teams check progress and meet oversight needs without extra steps. Though stripped down by design, it does not lock users into limited growth. Extra layers - like linking controls, handling proof files, setting user permissions by role, or streamlining routine checks - can plug in later. Built light now, ready to grow when demands shift.

II. Literature Review

Most past work on governance, risk, and compliance points to organized ways of checking dangers when handling digital safety issues. Standards from global groups - including ISO/IEC 27001 - along with advice found in documents like NIST SP 800-30, lay out step-by-step methods for spotting key resources, looking into possible attacks and weak spots, then judging danger levels through either descriptive ratings or number-based systems. Studies often mention score grids that multiply chance by effect size, helping teams sort which risks matter most while guiding clearer choices. Because rules keep changing, these models push regular checks, written records, plus updates shared across departments so companies stay within legal lines and better handle future shocks.

Some research plus practical examples point out flaws in old- school spreadsheet methods for handling risk, suggesting online automation instead to boost precision and clarity. Dashboards, visual risk maps, and live reports now come built into current GRC software, offering up-to-the-minute views on threats. Yet a number of high-end systems bring heavy complexity along with steep prices,

leaving smaller groups or schools behind.

III. System Architecture

Fig 1 Flow Chart

Built like stacked blocks, the GRC Risk Assessment Tool runs on a flexible three-part online structure allowing room to grow without breaking down easily. One level handles how users see things, another processes actions behind the scenes, then a third stores everything securely below. These layers do separate jobs yet fit together smoothly so risk checks happen in order. Free tools power every piece which keeps costs low while letting others copy or tweak the setup later. Small firms can run it just fine, colleges too, since nothing needs expensive licenses or special gear.

Starting off with clean layouts built through HTML and CSS, this front part uses Bootstrap to keep things flexible on any screen size. Instead of confusing menus, it guides users smoothly when logging assets, spotting threats, or evaluating dangers. Smooth checks happen as you go, making sure every field gets proper input without hassle. On the main view, quick numbers show how many items, risks, and reviews are logged so far. A shifting color map spreads out possible issues based on how likely they are and how severe their effect might be. Information comes together clearly in reports designed to line up facts neatly before saving them offline. Printed pages look sharp because formatting stays intact even outside the app. With clear labels and logical flow, people who aren't tech experts still find what they need fast. Auditors, compliance staff - anyone new - can move around without getting stuck. Even complex inputs feel manageable thanks to thoughtful design choices throughout.

Behind the scenes, Flask powers the app layer - it's a lean tool built with Python that supports clean API design along with core server tasks. Business decisions, checks on data accuracy, and movement of information live right here. When new assets appear or risks get logged, specific entry points take charge, keeping front and back ends in sync. The way risk levels are calculated follows a fixed math: multiply chance by consequence, nothing more. Scores for chance and effect stick to numbers one through five, keeping reviews steady and lined up. When totals come in, dangers get sorted - low, middle, high - so

teams know what needs attention first. Instead of freeform entries, links behind the scenes check if items connect right: assets point to real risks, each review ties back correctly. That way, nothing floats unattached; every hazard traces to something actual inside the company.

SQLite runs quietly under the surface, handling data without extra weight. Built around three main pieces - assets, risks, assessments - the structure stays lean. What belongs to whom shows up in the assets table: names, owners, how they're classified. Risk details live separately, each tied to type, status, title, plus connected items. When evaluating threats, numbers come into play through likelihood, effect size, and overall score logged over time. Change happens slowly here, tracked across visits instead of guesses. One thing keeps relations in check: foreign key rules. Data sticks around between uses, thanks to storage that lasts. Even though SQLite handles things now - simple setup, runs locally - the design doesn't lock you in. Bigger needs later? Shifting to a heavy-duty database stays possible.

Starting off, assets get identified first, after that risks tied to them are recorded. Once logged, each threat goes through evaluation using probability plus consequence ratings, which sets off automatic scoring in the background. Outcomes show up on dashboards along with color-coded maps, later bundled into reports fit for review. In design, it follows big-picture ideas from known frameworks - ISO/IEC 27001 shows influence, also NIST's approach to managing threats, alongside COBIT's structure - especially around spotting dangers, judging severity, keeping records, watching changes over time. Because of this match, the setup gains stronger backing from accepted theory.

IV. Novelty

What stands out about the new GRC Risk Assessment Tool is how it turns complex governance and risk ideas into something straightforward - lightweight, web-based, yet still solid in approach. Most big-name GRC products target large organizations and need heavy setup; this one shows essential features can run on open- source tools, built with academic care. Starting from assets, moving through risks, applying consistent scores, then showing results - it wraps everything into a single flow. Instead of sitting separate from real work, it connects classroom concepts to actual use. Even though it follows known models like ISO/IEC 27001 and NIST, it runs smoothly even where time, money, or tech access are limited.

One standout feature is how the system models risk around assets, using connections inside a relational database. While many research tools list risks separately, with no clear link to what they affect, this one ties every risk directly to specific business resources. Instead of treating threats in isolation, it maps them through defined relationships so their importance becomes clearer based on context. Because each threat connects back to an actual asset, decisions gain better grounding in operational reality. These built-in links - using keys that bind data across categories - make it easier to track who owns what and why certain choices were made. Such structure mirrors established practices seen in enterprise compliance setups, where clarity and responsibility matter most.

A fresh twist comes through built-in updates inside a slim design. Rather than sticking to one fixed rating, it allows repeated checks on every risk item across time. These ongoing reviews track shifts in risk levels when company situations shift.

V. Results and Discussions

Testing the new system happened by running it through clear situations built around real office risk tasks. Built-in functions, checks for accuracy, plus steady performance runs shaped how tests unfolded. Assets like servers, databases, and workstations filled the setup - each tagged with owner names and sensitivity levels. Instead of mixing everything at once, risks came next - those tied to hacking attempts, breakdowns in daily operations, or missing legal rules. Only after setting those links did the test environment act more like actual business conditions.

One after another, test cases showed the scoring system kept its math sharp. Instead of errors, every likelihood paired with impact on the 1-to-5 range produced spot-on results when checked by hand. Where numbers landed matched exactly what the formula demanded. Without drift, each outcome slotted into low, middle, or high risk based on set lines. Through repetition, it proved the code underneath holds firm - built not guesswork but rules tied to accepted oversight frameworks.

Right away, the dashboard showed that live data matched up perfectly with what was stored behind it. When something got added, things like asset tallies or risk figures changed instantly on screen - no waiting around. Seeing updates happen without lag proved the front display truly connected to the engine underneath. Confidence grows when users know results aren’t stuck in the past due to slow processing steps found in old spreadsheet setups.

Testing the heatmap confirmed how well the system works. Where each risk landed on the grid matched its chance and effect exactly. Risks that are both likely and severe showed up clearly toward the top, making threats hard to miss. Seeing numbers turned into colors helps leaders grasp patterns fast, without sorting through spreadsheets. Clarity jumps when dense figures become shapes anyone can follow.

Every report check looked at how complete it was, whether layout stayed steady, then if auditors could trust what they saw. Pages in PDF form pulled together gear lists, danger logs, last rating numbers without missing pieces. Clean layouts showed only needed parts, nothing extra crowding the page. This kind of order means fewer papers to fix by hand when inspectors arrive. Well-built summaries also make staying within rules feel less heavy on teams later.
When the app restarted, stored information stayed exactly as it was meant to be. Every failed attempt with wrong entries or empty required sections got caught before causing issues.
Validation checks handled errors without letting bad data through. Through repeated cycles, the database showed it could hold steady under pressure. Even when users made mistakes, the structure held firm and kept everything in order.

Looking at everything, the findings show the new GRC Risk Assessment Tool puts key governance ideas into real practice using a simple design. Because of its layout, it makes processes clearer, sharpens how risks are ranked, cuts down on mistakes made by people, while also helping keep records organized. This approach proves useful when dealing with risk in companies. The tool fits well where structure and clarity matter.

Fig 2 Displaying of risk present

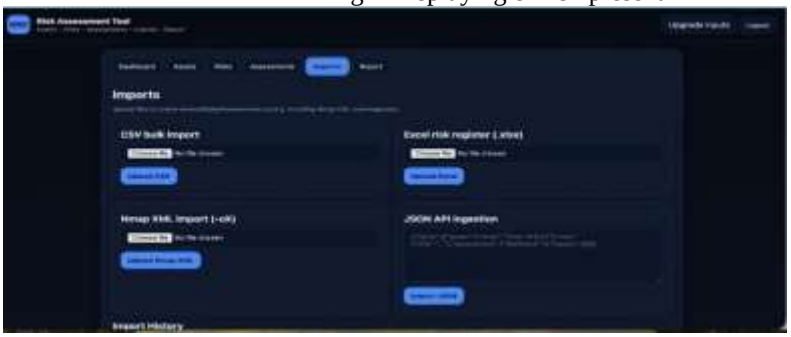

Fig 3 Importing the XML file

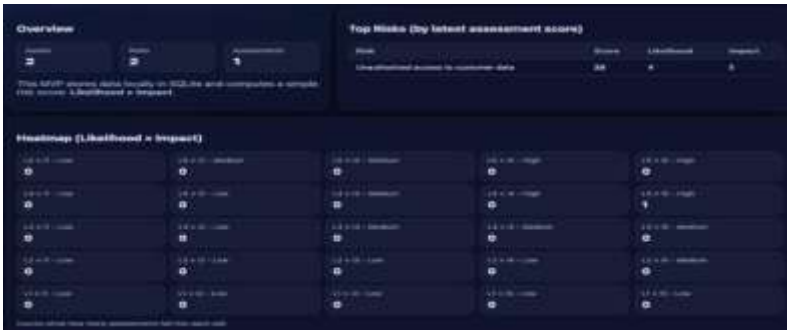

Fig 4 Heatmap

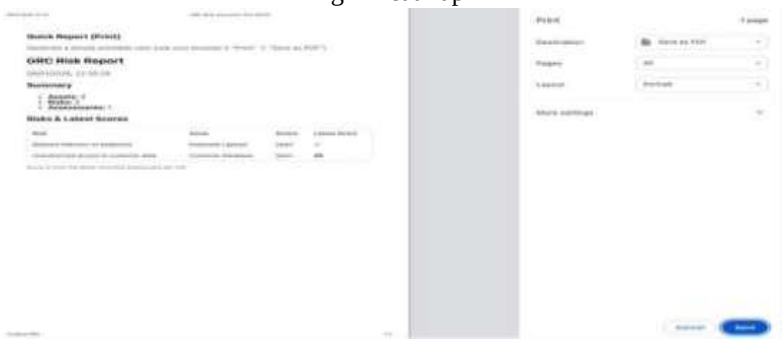

Fig 5 Output in PDF format

VI. Merits and Demerits

What stands out about the new GRC Risk Assessment Tool is how it pulls governance details into one organized database setup. Instead of scattered spreadsheets, messages, or paper trails, everything fits under one roof. When asset logs, threat entries, and past evaluations live together, seeing who did what becomes far clearer. A web- like structure ties each piece - equipment to vulnerabilities, those to checks - just like official methods.

One strong point is how clearly the tool shows data. Visual summaries of assets, risks, and assessments update live, giving a current picture of overall exposure. Instead of relying number-heavy reports, leaders see where problems cluster using a color-based grid. This map plots chance against consequence, highlighting zones that demand attention. Areas needing urgent response stand out immediately, reducing time spent scanning rows of figures.

What stands out most is how fast meaning emerges from visuals alone. Picture this idea makes it far easier for leaders to share insights while sharpening focus on key goals. Unlike old-school spreadsheets that demand hand-built charts, the auto-generated heatmaps speed up risk updates and smooth out daily workflows.

What helps this system stand out is how little it costs to run while still being easy to reach. Open tools like Python, Flask, Bootstrap,

and SQLite mean no license fees pop up along the way. Instead of needing powerful machines, it runs just fine on everyday computers. Small businesses find it useful, so do schools and government offices with tight budgets. Because setup stays simple, more groups can adopt clear rules for handling risks. Access opens up when expensive setups are no longer a must.
Built-in reassessment strengthens how oversight grows through ongoing checks. Instead of locking risks into one fixed judgment, updates can happen again and again. Watching shifting threats becomes possible along with how well controls work and shifts in daily operations. Refreshing risk ratings regularly fits with steady progress goals common in management rules. With movement built in, records stay useful now instead of stuck in the past.

Ready-made reports make it easier to show what the system tracks. Because everything comes together automatically, teams get clean summaries without reworking numbers each time. Files pull in device lists, risks found, and recent checks - neatly packed for meetings or regulators. Formatting happens behind the scenes, so there is less busywork for staff. Mistakes from copying by hand drop off since details go straight into place. When auditors look around, proof of control shows up fast and clear. Teams stay ahead because records update themselves between visits.

Even with those strengths, some downsides still stand out. Without login features or permissions based on roles, things get tricky. Right now, it works only for one person at a time - more like a personal tool than a shared workspace. Big teams that need clear divisions in who can do what will find this setup too limiting. When handling high-stakes data, not having fine-tuned access rules becomes a real problem.

One big gap sits in how it doesn't automatically link with outside security or operations tools. Tools like vulnerability checkers, event trackers, or system inventory logs often feed live risk details into corporate setups. Right now, adding assets or risks needs hands-on entry, opening space for lag or missed items. With API hooks or live data streams, updates could stay sharp while easing user effort. Without those links, keeping pace gets harder when systems shift fast.

SQLite's limits on scaling can cause problems down the line. Though it works well for small setups or learning settings, heavy workloads overwhelm it quickly. Big companies spread across locations might find it too weak under pressure. Shifting to stronger databases becomes unavoidable at that stage.

Features like tracking controls, automating risk steps, linking proof files, or forecasting trends? Missing entirely. Basic tools exist, yet gaps remain obvious even for early versions. Room to grow is clear when aiming beyond trial stages into real-world use.

VII. Applications

Imagine smaller buisnesses stepping into better control - this tool fits right in, especially when budgets block high-end options. Off-the-shelf methods like scattered sheets or messy email threads? They open doors to errors, repeats, repeated effort, blind spots. Instead, picture one place where every machine, threat, and check gets logged cleanly, scored fairly, reviewed clearly. No big fees, no complex setup; still, companies gain official-style records built on trusted rules. Clarity grows quietly, simply, as structure replaces chaos beneath the surface. Light on its feet, the setup runs lean without skipping steps when it comes to audits or deciding what matters most. What stands out is how well it fits startups aiming to tighten cyber oversight without stretching budgets too thin.

Schools form a key area where this tool could be used. Labs run by universities and technical colleges handle experiments, operate computer networks, while also holding private records of staff and learners - each activity bringing its own set of security and workflow challenges. Yet structured approaches to governance, risk, and compliance rarely exist on campuses, mainly because funds are tight and proper software is missing. This solution fits into that gap, working not just to monitor daily risks but also helping train future professionals in oversight practices.

From time to time, learners in infosec, risk analysis, or cyber governance apply this tool to carry out real-world asset-focused risk checks. It lets them walk through probability and consequence judgments using interactive models instead of just theory. Heatmap displays turn abstract numbers into clear visual patterns. Experience gained matches up closely with standards like ISO/IEC 27001, building stronger understanding without copying textbook examples. Classroom results grow sharper when practice shapes knowledge. Schools benefit too - risk records become more accurate, step by step.

Spot checks become easier when leaders see hot zones at a glance, thanks to color-coded maps that highlight trouble spots early. When inspectors show up unannounced, pre-built reports stand ready - no scrambling needed - to prove risks were logged and reviewed properly.

Banks and finance spots show up often as key users. Tight rules shape how they work, pushing constant checks on operations, digital threats, security gaps, plus legal alignment. Big lenders might run heavy-duty GRC tools, yet small credit groups, local outfits, or back-office teams could miss organized ways to log hazards. This solution fits right into those places, holding risk logs together near online banking tech, payment channels, or company money records. Every so often, checks line up with legal requirements thanks to built-in reevaluation features, whereas clear scoring keeps priorities fair. With steady recordkeeping and reports ready for audits, oversight becomes visible, readiness improves when facing both company and outside evaluations.

Tech groups might use this system to manage risks from one central spot. Not every team keeps its findings together, even though they watch for weak spots and respond to issues regularly. This tool links up equipment lists with known dangers so staff can judge how serious each threat really is. Scan results showing gaps could go into the tool by hand, then get weighed on chance and effect to decide what needs fixing first. Seeing risks on a map helps leaders understand threats without needing tech details. Because all risk data lives in one organized place, security teams and top decision makers stay on the same page.

Instead of scattered reports, there is now a single view that connects daily cyber efforts to big-picture goals. This way, choices about safety are clearer, faster, stronger.Off to a start, government bodies might use this tool where resources are tight. When handling vital services and personal information, many offices still face strict spending rules that block high-end tools. Instead of heavy tech demands, the design here works on basic machines. Because setups stay simple, teams find it easier to list key systems and spot daily hazards. Step by step, checks get recorded without complex steps piling up. With everything recorded in one clear place, it becomes easier to track who did what - especially when printed records are available.

Because audits rely on consistent data, having documents ready helps teams review work without delays. What stands out is how each asset shapes the way risks are ranked. Instead of treating every system the same, importance grows alongside how vital a service is to daily function. When disruptions happen, the most crucial services stay protected first. This kind of structure keeps public operations running, even under pressure.

Factories and similar operations might use this system to keep their work running smoothly while guarding key setups. What happens inside today's production sites often ties together automated controls, delivery tracking programs, and linked machines - all of it building tricky exposure zones.

Using scores that weigh how probable and how damaging an event could be reveals which issues threaten ongoing output most strongly. Where risks pile up, a color-coded map shows plant supervisors where trouble might strike, helping guide time and budget decisions more wisely. Because records are laid out clearly, staying on track during setbacks becomes easier when systems face strain.
One last thing - this setup could be useful when offering advice about oversight and evaluating threats. Not just that, people who check systems independently, experts in digital safety, plus those guiding rule adherence usually need clear methods to record how risky a client's situation is. What helps here? A compact method like the one suggested might serve as a mobile way to judge early warnings, especially in smaller groups. Think of it: professionals noting down what clients own, listing dangers spotted, applying consistent ratings, then forming organized summaries meant for leaders to examine.
Even better, since rechecks are built in, later visits become possible - showing progress made across months or years. One step at a time, it grows - role controls added, hosted online, turning solitary checks into shared oversight work.

References

[1] N. G. Eapen, A. R. Rao, D. Samanta, N. R. Robert, R. Krishnamoorthy, and G. H. Lokesh, ‘‘Security aspects for mutation testing in mobile applications,’’ in Cyber Intelligence and Information Retrieval (Lecture Notes in Networks and Systems), J. Manuel, R. S. Tavares, P. Dutta,
S. Dutta, and D. Samanta, Eds. Singapore: ” IEEE Access,
Springer, 2022

[2] Zhenpeng Chen, Jie M Zhang, Federica Sarro, and Mark Harman. 2023. ‘‘A Comprehensive Empirical Study of Bias Mitigation Methods for Machine Learning Classifiers. ACM Transactions on Software Engineering and Methodology” IEEE Access, 32, 4 (2023), 1–30.

[3] Y. Cao, Q. Z. Sheng, J. McAuley, and L. Yao, ‘‘Reinforcement learning for generative AI: A survey,’’ IEEE Access, 2023, arXiv:2308.14328

[4] A. Pinto, L.-C. Herrera, Y. Donoso, and J. A. Gutierrez, ‘‘Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure’’ Sensors, IEEE Access, vol. 23, no. 5, p. 2415, Feb. 2023.

[5] Alessandro Fabris, Nina Baranowska, Matthew J Dennis, Philipp Hacker, Saldivar, Frederik Zuiderveen Borgesius, and Asia J Biega. 2023. Fairness and Bias in Algorithmic Hiring. arXiv preprint arXiv:2309.13933 (2023).