# Table of contents

[Table of contents](#_utiy44o4o1m6)

[Summary](#_lpuumse8e0ul)

[Plan](#_n41tmsuabxfr)

[● Organizational Scoping](#_7eei92xm7e7s)

[● Asset Management](#_w4q5ow6g9ls2)

[● Reference Model Creation](#_2plopphkm8ep)

[● Assessment Planning](#_sm6f6jbsgora)

[● Assessment Execution](#_70ppc4w1fue7)

[● Gap Analysis & Reporting](#_h0l3hq90yelu)

[● Risk Assessment](#_l2tmz7ybqzsy)

[● Goal Setting](#_2rqd9r39d7v5)

[Do](#_6ntuldlcgv95)

[1. Action & Resource Planning](#_a0zmqgwnt22l)

[● Action planning](#_8h0y3l1upztt)

[● Resource Planning](#_jowqpm303s9b)

[2. Implementation Tracking](#_hsagpppeo24g)

[3. Evidence Collection](#_2rlv6iwyenba)

[4. Training and Awareness](#_s3iurequ9u4g)

[Check](#_2my29w7uuk90)

[1. Continuous Monitoring](#_5oejdegu8tw)

[2. Assessment Execution](#_fave4ljsxln)

[3. Assessment Planning](#_l7jyk6b6tzts)

[4. Gap Analysis & Reporting (identical to Plan)](#_2h1y7yl8e2rs)

[5. Risk Assessment (identical to Plan)](#_tdx12mco22v9)

[Act](#_7qz4vohaywip)

[1. Effectiveness Evaluation](#_2c75zqsq0c83)

[2. Action & Resource Planning](#_1t9qlxi0nvgc)

[3. Strategic Review](#_xq6bp399zw7e)

[4. Process Improvement](#_4k19grz7pl7o)

[5. Regulatory Update](#_ala7da5mmlsz)

[Additional Elements](#_uh55lfpr3jn2)

[Usability Recommendations](#_rzbrdu3aue29)

[Integration with Platform Design](#_5uxppy47g2mm)

[Potential Challenges and Solutions](#_ltro4xm3gq3x)

# 

# 

# Summary

*“Imagine an intuitive compliance platform built specifically for SMEs that need to meet cybersecurity and regulatory demands but don’t have dedicated compliance teams. Our platform simplifies compliance management by guiding users step-by-step, ensuring they understand not only what they need to do but also why it matters for their business.”*

1. Organizational Scoping

* Start with Organizational Scoping, where users define their compliance landscape through a plain-language questionnaire and industry based templates. The platform helps users identify relevant regulations and map them to their unique business functions.
* This step also generates a business capability map, linking compliance requirements directly to critical functions, which helps users see the connection between compliance and business value.

1. Unified Control Framework

* We then build a Unified Control Framework by mapping regulatory requirements and any internal policies to industry standards like ISO 27001 or NIST. This unified approach simplifies managing multiple regulations under one structure.
* With drag-and-drop tools and templates, users can easily create practical controls and remove redundant work by identifying overlapping requirements.

1. Asset Management

* With controls in place, we move to Asset Management, where users build an inventory of business objects (data, systems, process, teams, physical devices,..) categorized by type and importance.
* This inventory links assets to relevant business capabilities, helping users track ownership and responsibilities. Integrations with automated discovery tools keep this list updated without manual effort.

1. Assessment Planning

* Next, we plan assessments with Assessment Planning. Users schedule periodic checks and audits to ensure controls are working as intended. With calendar integration, reminders, and templates, assessments are easy to manage.
* This planning is tailored to asset criticality and risk levels, ensuring resources are directed where they’re needed most.

1. Assessment Execution

* In Assessment Execution, users conduct assessments with the help of checklists and templates, evaluating each control for compliance. Evidence collection can be manual or automated for a streamlined process.
* This step ensures thorough evaluation of each control and creates an organized record of compliance actions.

1. Gap Analysis & Reporting

* After assessments, the platform performs a Gap Analysis to identify areas needing improvement, with gaps color-coded by criticality.
* Each gap comes with actionable recommendations tailored to the criticality of the affected assets. This guidance enables users to focus on high-impact improvements without requiring specialized knowledge.

1. Risk Assessment

* In the Risk Assessment phase, the platform evaluates each gap’s impact on critical assets, helping users prioritize resources for high-impact areas.
* By focusing on risk in business-critical areas, this step helps users allocate resources effectively, reducing risks with the most significant impact on the organization.

1. Action and Resource Planning

* For each identified gap, the platform translates regulatory requirements into actionable tasks with clear language and provides AI-powered recommendations for resource allocation.
* Users can view tasks based on priority and dependencies, helping them manage timelines and adapt plans as compliance needs change.

1. Implementation Tracking

* The platform provides Implementation Tracking to monitor each action item’s progress, focusing on quick wins and high-priority items first.
* Visual tools, like Gantt charts or progress bars, allow users to see at a glance which actions are complete, in progress, or pending, helping them stay organized and on track.

1. Evidence Collection

* With Evidence Collection, the platform organizes all documentation proving compliance. Users can store and retrieve evidence by gap, asset, or compliance requirement, ensuring quick access during audits.
* Automated logging and secure storage make it easy to maintain a detailed audit trail, showing regulators a clear history of compliance actions.

1. Training and Awareness

* Training and Awareness programs are essential for compliance, so our platform provides role-based training sessions and e-learning modules to raise awareness.
* Progress tracking and comprehension scores help users measure training effectiveness, ensuring that all employees are aware of compliance requirements and best practices.

1. Continuous Monitoring

* With Continuous Monitoring, users track key compliance and risk metrics in real-time. Dashboards display alerts for any deviations, helping users stay on top of compliance status.
* AI-powered anomaly detection notifies users of potential issues immediately, reducing response times and strengthening the organization’s security posture.

1. Effectiveness Evaluation

* The Effectiveness Evaluation tool measures the impact of implemented controls on risk posture. It reviews feedback from users and analyzes the effect of actions on overall security and compliance, identifying any gaps in control effectiveness.
* This continuous feedback loop enables users to make informed improvements to their compliance strategy.

1. Strategic Review and Improvement

* In the Strategic Review and Improvement phase, users align compliance activities with broader business goals. This step allows users to adjust priorities based on organizational needs, assessing how security and compliance support business functions and identifying areas needing more investment.
* This long-term perspective enables the organization to use compliance as a competitive advantage, protecting operations while supporting growth.

1. Regulatory Update

* Based on the outcome of the strategic review, it is possible that the regulatory needs are to be updated (e.g. entering new customer segments require additional regulatory compliance). Changes to the company’s unified control framework are pushed accordingly.
* The platform’s Regulatory Update feature monitors changes in relevant regulations, alerting users to any new requirements that impact their compliance framework.
* With automatic updates and summaries, users stay informed about regulatory changes without needing to monitor updates themselves, ensuring ongoing alignment with legal requirements.

# 

# 

# Plan

## Organizational Scoping

* + Complete a guided questionnaire to define your organization's regulatory landscape and business capabilities.
  + Conduct intake sessions using guided questionnaires with plain language.
    - Define the organization's regulatory landscape using pre-populated, industry-specific templates.
    - Identify applicable best practice models and standards.
  + Create business capabilities map based on best practice models and industry standards.
    - Map business capabilities to potential security and compliance impacts
    - Use visual tools (e.g., flowcharts or mind maps) for easier understanding.
    - Create a high-level view of where security and compliance efforts may need to focus.
  + Update Organizational Scoping based on output of [Strategic Review](https://docs.google.com/document/d/1HSm5yRCuBBOLp2nhm8uy9-pmFVNzFPnxB6DR2tALjBY/edit?pli=1&tab=t.0#heading=h.xq6bp399zw7e) (if needed)
  + AI assistant provides industry-specific suggestions and explanations in plain language.

## Asset Management

* + Create and maintain an inventory of all organizational assets (hardware, software, data, and systems).
  + Categorize assets based on type, importance, and sensitivity.
  + Map assets to related business capabilities.
  + Assign ownership and responsibilities for each asset.
  + Use a very lightweight tool to register assets or integrate with (external) automated discovery tools to keep the asset inventory up-to-date.
  + Implement version control and change management for the asset inventory.

## Reference Model Creation

* + Build a unified control framework for your organization by translating all your regulatory requirements and cybersecurity expectations to control frameworks like ISO27K and NIST.
  + Use pre populated templates or drag-and-drop tools to map regulatory requirements and expectations to control frameworks like ISO27k and NIST.
  + Link actions to the control frameworks; the actions can be context specific (e.g. privacy check on Microsoft is much lighter than Alibaba, e.g. priorities for international vs local customer base requires different actions on the level of CRM related assets). Idea is to link the action variations to strategic drivers (e.g. international growth, M&A, etc…)
  + Develop a unified control framework tailored to your organization.
  + Map control frameworks and regulatory requirements to asset categories.
    - Since assets are linked to business capabilities, we establish an implicit link between regulatory requirements and business capabilities (useful for risk and impact evaluations)..
  + Employ AI to suggest potential control overlaps and gaps, providing brief explanations in layman's terms.

## Assessment Planning

* + Conduct periodic checks / audits / assessments to assess the effectiveness of (implemented) controls.
  + Use audit scheduling with calendar integration and automated reminders.
  + Leverage templates for common audit types to streamline the process.
  + Compare audit results against previous assessments to measure progress.
  + Plan assessments based on asset criticality and risk levels.
  + Plan assessments based on business capability criticality and risk levels.
  + Ensure assessment scope covers all relevant asset types and business capabilities.

## Assessment Execution

* + ​​Conduct assessments on a per-asset or per-asset-type basis.
  + Use the asset inventory to ensure comprehensive coverage in assessments.
  + Conduct baseline assessment either manual or via user-friendly automated tools.
  + Provide checklists and examples for proper evidence collection and documentation.
  + Gather evidence of existing controls and practices.

## Gap Analysis & Reporting

* + Compare assessment results against the unified control framework.
  + Compare [continuous monitoring](#_5oejdegu8tw) data (if available, see [Check](#_2my29w7uuk90)) against the unified control framework.
  + Identify (residual) gaps in compliance and security controls.
  + Link identified gaps to specific assets, asset types and business capabilities.
  + Use color-coded visuals or urgency labels to (re)prioritize gaps.
  + Prioritize gaps based on the criticality of affected assets or business capabilities.
  + Provide actionable recommendations for each identified gap.
  + Generate comprehensive, stakeholder-specific compliance reports.
  + Use data visualization techniques and infographics to present complex data in an understandable format.
  + Include trend analysis to show progress in compliance over time.
  + Use AI to predict potential future gaps, presenting predictions in an easy-to-understand format.

## Risk Assessment

* + Conduct a risk assessment to define gap prioritization.
  + Evaluate risks in the context of specific assets, asset types or business capabilities.
  + Consider asset value and criticality in risk calculations.
  + Prioritize gaps and actions based on their impact on critical business capabilities. This ensures that resources are focused on areas that most significantly affect business operations.
  + Re-evaluate risks considering newly implemented controls and changing landscapes.
  + Utilize simplified risk models with clear definitions of impact and likelihood levels.
  + Perform simplified risk assessment with industry-relevant examples.
  + Use Monte Carlo simulations or other risk modeling techniques to quantify potential impacts.
  + AI provides actionable recommendations for each gap and risk.

## Goal Setting

* + Create a high-level roadmap for addressing identified gaps.
  + Use a SMART Objectives Wizard to guide users through setting specific, measurable, achievable, relevant, and time-bound objectives.
  + Visualize dependencies and set priorities.
  + Clearly define and assign roles and responsibilities, with default roles for common organizational structures.

# Do

## Action & Resource Planning

### Action planning

* + - Translate identified gaps and compliance requirements into specific, actionable tasks using plain language.
    - Link action items to specific assets, asset types and business capabilities they aim to improve or protect.
    - Use AI-powered suggestions for best practices and implementation suggestions.
    - Use natural language processing to convert complex regulatory language into clear, understandable actions.
    - Assign due dates (priorities) to tasks based on the priority assigned to the related gaps.
    - Consider asset criticality when prioritizing actions.
    - Visualize task dependencies to show the sequence and relationship of actions.
    - Adjust existing action plans to address newly identified or residual gaps or changes in Resource allocation
      1. Allow action plans to adapt dynamically based on new data or changes in the compliance environment.
      2. Reprioritize actions based on their effectiveness and changing risk landscape.
      3. Use machine learning algorithms to suggest optimizations in the action plans.
      4. Maintain change logs for transparency and accountability.

### Resource Planning

* + - Assign personnel, budget, and tools to each action item.
    - Create worklists for personnel based on the assigned action items.
    - Provide AI-driven suggestions for resource allocation with user adjustment options.
    - Implement simple budgeting tools for tracking compliance-related expenses.

## Implementation Tracking

* + Execute planned actions, starting with quick wins and high-priority items.
  + Track implementation progress on a per-gap or compliance requirement basis.
  + Track implementation progress on a per-asset basis where applicable.
  + Track progress not just by individual actions, but by improvements to business capabilities.
  + Use Gantt charts or progress bars to track task completion visually.
  + Implement technical controls, policy changes, and process improvements.
  + Integrate messaging or commenting systems within tasks to facilitate team communication.

## Evidence Collection

* + Gather and organize evidence of implemented controls and actions.
  + Organize evidence by gap, compliance requirement, asset or asset type for easy retrieval and audit.
  + Use automated data collection where possible (e.g., system logs, policy documents).
  + Use automated evidence logging for actions taken within the platform.
  + Maintain an audit trail of all compliance-related activities.
  + Provide secure document upload and storage capabilities (EU based).

## Training and Awareness

* + Conduct role-based training sessions using interactive training modules with quizzes.
  + Use e-learning modules and simulations for effective knowledge transfer.
  + Track completion rates, comprehension scores, and overall training progress.
  + Offer certificates upon completion of training modules.

# Check

## Continuous Monitoring

* + Implement real-time monitoring of key security and compliance metrics.
  + Monitor asset-specific metrics and compliance status.
  + Set up alerts for changes in asset inventory or configuration.
  + Set up monitoring dashboards that show compliance and risk status per business capability.
  + Offer customizable dashboards focusing on metrics most relevant to users.
  + Use AI-powered anomaly detection to identify potential issues quickly.
  + Generate real-time alerts for significant deviations from expected states.
  + Automatically distribute alerts to SIEM or personnel/SOC.

## Assessment Execution

* + [Assessment Execution](#_70ppc4w1fue7) (reuse as defined in [Plan](https://docs.google.com/document/d/1HSm5yRCuBBOLp2nhm8uy9-pmFVNzFPnxB6DR2tALjBY/edit?pli=1&tab=t.0#heading=h.n41tmsuabxfr))

## Assessment Planning

* + [Assessment Planning](#_sm6f6jbsgora) (reuse as defined in [Plan](#_n41tmsuabxfr))

## Gap Analysis & Reporting (identical to Plan)

* [Gap Analysis & Reporting](#_h0l3hq90yelu) (reuse as defined in [Plan](https://docs.google.com/document/d/1HSm5yRCuBBOLp2nhm8uy9-pmFVNzFPnxB6DR2tALjBY/edit?pli=1&tab=t.0#heading=h.n41tmsuabxfr))

## Risk Assessment (identical to Plan)

* [Risk Assessment](#_l2tmz7ybqzsy) (reuse as defined in [Plan](https://docs.google.com/document/d/1HSm5yRCuBBOLp2nhm8uy9-pmFVNzFPnxB6DR2tALjBY/edit?pli=1&tab=t.0#heading=h.n41tmsuabxfr))

# Act

## Effectiveness Evaluation

* + Assess the impact of implemented controls on overall risk posture, as well as the risk posture per business capability.
  + Evaluate the effectiveness of controls on a per-asset or per-asset-type basis.
  + Gather feedback from users and stakeholders on the practicality and efficiency of new processes.
  + Use AI to analyze the correlation between implemented actions and risk reduction.

## Action & Resource Planning

* + [Action & Resource Planning](#_a0zmqgwnt22l) (reuse as defined in [Do](#_6ntuldlcgv95))

## Strategic Review

* + Align security insights & compliance to business capabilities (value chains) to show impact in terms of business risks / value -> inside-out
  + Review how current security and compliance efforts align with overall business goals -> inside-out
  + Assess the impact of compliance activities on customer relationships? -> outside-in
  + Identify which capabilities need more focus or investment based on compliance gaps and business priorities.
  + Identify opportunities where improved security or compliance can create business advantages.
  + Identify assets that may need to be acquired, retired, or upgraded based on compliance and security needs.
  + Evaluate resource allocation for compliance activities in relation to other business priorities.
  + Enable sharing of executive insights and plans with key stakeholders within the platform.

## Process Improvement

* + Identify bottlenecks or inefficiencies in the compliance management process.
  + Regularly solicit user feedback on the platform's usability and incorporate improvements.
  + Implement changes to streamline workflows and improve user experience.
  + Continuously update the knowledge base with new best practices and highlight them to users.

## Regulatory Update

* + Integrate with regulatory databases to provide real-time updates on changes.
  + Monitor for changes in relevant regulations and standards.
  + Communicate brief impact summaries of how regulatory changes affect the user's organization.
  + Assess the impact of regulatory changes on the current compliance posture.
  + Initiate new planning cycles for significant regulatory updates.

# Additional Elements

* Settings and Configuration
  + Design user-friendly interfaces with clear labels and explanations for non-technical users.Implement role-based access control with predefined roles and customizable permissions.
  + Allow users to set preferences for receiving alerts and updates.
  + Provide integration configuration for connecting with existing enterprise systems.
  + Offer customizable dashboards and report templates.
* Knowledge Center (Learn)
  + Create a searchable repository of regulatory texts, interpretations, and guidance.Categorize knowledge base articles by topic, industry, and relevance.
  + Enhance search functionality with filters to help users find information quickly.Provide best practice libraries categorized by industry and compliance domain.
  + Offer interactive decision trees for complex compliance scenarios.
  + Include forums or discussion boards for community engagement and sharing experiences.
* AI Assistant
  + Implement a natural language interface for querying compliance status and requirements.
  + Design the AI assistant to answer questions in natural language and guide users through tasks.
  + Provide on-demand help when users are unsure how to proceed with a task.
  + Offer predictive analytics for forecasting potential compliance issues.
  + Enable automated report generation and summarization.
  + Provide contextual help and suggestions throughout the platform.
  + Clearly communicate how user data is used by the AI assistant to build trust.
* Role based
  + To be described
  + Suggestion: dedicated profile for external auditors

# Usability Recommendations

* Maintain an intuitive navigation with a clean, straightforward user interface and clear calls to action.
* Ensure consistency in design elements across all pages to reduce cognitive load.
* Meet accessibility standards, including keyboard navigation and screen reader support.
* Design the platform to be fully functional and responsive on mobile devices for on-the-go access.

# Integration with Platform Design

* Use simplified single-word menu titles (Identify, Execute, Review, Improve, Learn) for clarity.
* Allow users to customize dashboards by adding or removing widgets based on preferences and roles.
* Employ visual cues, icons, and color coding to help users quickly identify sections and understand statuses.

# Potential Challenges and Solutions

1. Complexity of Compliance Content
   * Solution: Break down complex regulations into simple, actionable items and provide explanations in plain language.
2. User Engagement
   * Solution: Incorporate interactive elements and gamification, such as progress tracking and achievement badges, to motivate users.
3. Data Security Concerns
   * Solution: Implement robust security measures, including encryption and regular security audits, and communicate these measures to users.