AMERICAN NATIONAL BANK®

Adapting to and responsibly integrating generative AI

Rob Baldi
Corporate Security Officer
3/20/2024

A dialogue

What we’re currently dealing with….

grammarly

There are several AI capabilities similar to Grammarly that provide grammar and writing assistance. Some popular alternatives include:

1. **ProWritingAid**: ProWritingAid is a comprehensive writing tool that offers grammar and style checking, contextual suggestions, readability analysis, and plagiarism detection.

2. **Ginger**: Ginger is an AI-powered writing assistant that provides grammar and spelling correction, sentence rephrasing suggestions, and contextual definitions. It also offers a text-to-speech feature.

3. **Hemingway Editor**: Hemingway Editor helps improve writing clarity and readability by highlighting complex sentences, passive voice usage, adverb overuse, and other readability issues.

4. **LanguageTool**: LanguageTool is an open-source grammar and style checker that supports multiple languages. It provides suggestions for grammar, spelling, punctuation, and style errors.

5. **WhiteSmoke**: WhiteSmoke offers grammar and spelling checking, style suggestions, and a translator. It also provides a plagiarism checker and a writing tutorial feature.

Top Chrome AI Plug-ins

1. **Grammarly**: Grammarly is a widely used AI-powered writing assistant that helps with grammar and spelling correction, style suggestions, and readability improvements.

2. **Honey**: Honey is an AI-powered shopping assistant that automatically finds and applies coupon codes at checkout, helping users save money while shopping online.

3. **Momentum**: Momentum is a personal dashboard that uses AI to provide a customized experience with features like to-do lists, weather updates, inspirational quotes, and beautiful backgrounds.

4. **Evernote Web Clipper**: Evernote Web Clipper is an AI-powered tool that allows users to save and organize web content, including articles, images, and screenshots, for easy access and reference.

5. **LastPass**: LastPass is an AI-powered password manager that securely stores and autofills passwords for websites and apps, making it easier to manage and protect online accounts.

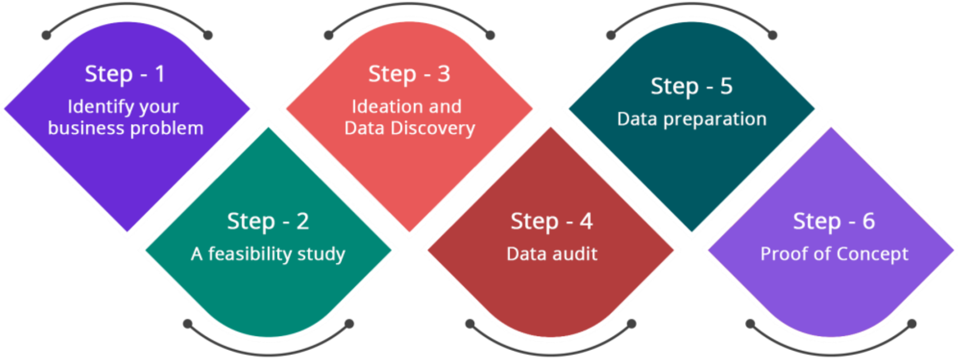
6. **Pocket**: Pocket is an AI-powered bookmarking tool that allows users to save articles, videos, and web pages for later reading or viewing, with personalized recommendations based on interests.

7. **AdBlock Plus**: AdBlock Plus is an AI-powered ad blocker that helps users block intrusive ads, pop-ups, and tracking scripts, providing a smoother and faster browsing experience.

8. **Google Translate**: Google Translate is an AI-powered language translation tool that allows users to translate web pages, text, and even spoken words in real-time across multiple languages.

Frameworks for implementation

A framework is a basic conceptional structure, a skeletal, openwork, or structural frame, or a frame of reference.



Step - 1
Identify your business problem

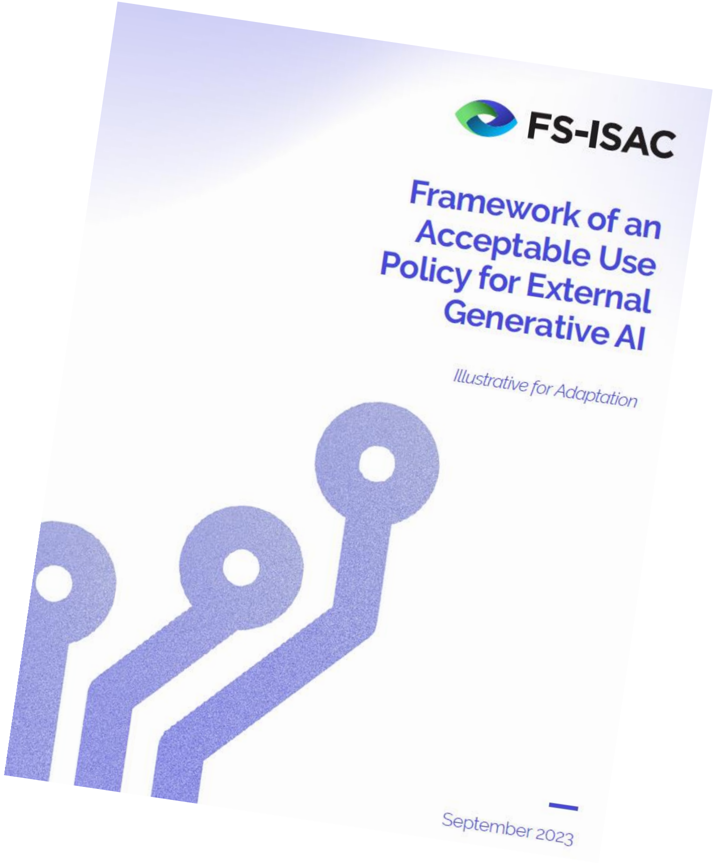
Step - 2
A feasibility study

Step - 3
Ideation and Data Discovery

Step - 4
Data audit

Step - 5
Data preparation

Step - 6
Proof of Concept



FS-ISAC

Framework of an Acceptable Use Policy for External Generative AI

Illustrative for Adaptation

September 2023

Legal Considerations

1. Data Protection and Privacy: Financial institutions must comply with data protection and privacy laws when collecting, storing, and processing customer data. AI systems often require access to large amounts of personal and sensitive data, so it's crucial to ensure compliance with regulations such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA).

2. Anti-Discrimination Laws: AI systems can inadvertently perpetuate biases or discriminate against certain individuals or groups. Financial institutions must ensure that their AI models and algorithms do not violate anti-discrimination laws, such as the Fair Credit Reporting Act (FCRA) or the Equal Credit Opportunity Act (ECOA).

3. Financial Regulations: Financial institutions are subject to various regulations, such as the Dodd-Frank Act, Basel III, or the Payment Services Directive (PSD2). When implementing AI, it's important to ensure compliance with these regulations, especially when it comes to risk management, fraud detection, and customer protection.

4. Intellectual Property: Financial institutions need to consider intellectual property rights when implementing AI. This includes ensuring that they have the necessary licenses or permissions to use third-party AI models or algorithms and protecting their own AI-related intellectual property through patents or trade secrets.

5. Contractual Obligations: Financial institutions must review and consider any contractual obligations they have with customers, partners, or vendors when implementing AI. This includes ensuring that AI systems comply with service level agreements, data sharing agreements, or confidentiality agreements.

6. Cybersecurity and Data Breach: AI systems can be vulnerable to cybersecurity threats and data breaches. Financial institutions must implement robust security measures to protect AI systems and the data they process, including encryption, access controls, and regular security audits.

Monitoring

Define Key Performance Indicators (KPIs): Identify the KPIs that align with your AI objectives, such as accuracy, latency, throughput, or error rates. These metrics will help you measure the performance of your AI models.

Implement Logging and Monitoring: Set up logging and monitoring systems to capture relevant data relating to AI (Proxy server logs, firewall logs, SIEM, web filtering). This includes logging predictions, inputs, outputs, and any errors or exceptions that occur during runtime. Use tools like Elasticsearch, Kibana, or Splunk to aggregate and visualize the logs.

Real-time Monitoring: Implement real-time monitoring to track the performance of your AI models continuously. This can involve setting up alerts or notifications for specific events, such as a sudden drop in accuracy or an increase in error rates.

Compliance Monitoring: Ensure that your AI models comply with legal, ethical, and regulatory requirements. Monitor for any biases, discrimination, or privacy violations in the predictions made by your models.

Documentation and Auditing: Maintain comprehensive documentation of your AI models, including their architecture, training data, hyperparameters, and performance metrics. Regularly audit and review this documentation to ensure transparency and accountability.

Identity and Access Management

1. Data Privacy and Security: IAM systems deal with sensitive user data, such as personal information and access credentials. Implementing AI in IAM requires careful consideration of data privacy and security measures to protect this information from unauthorized access or breaches.

2. Bias and Discrimination: AI algorithms can inadvertently introduce biases or discrimination into IAM systems. This can occur if the training data used to develop the AI models contains biases or if the algorithms themselves are not designed to be fair and unbiased. It is crucial to ensure that AI models used in IAM are trained on diverse and representative data and regularly audited for fairness.

3. Scalability and Performance: IAM systems need to handle a large number of users and access requests in real-time. Implementing AI in IAM requires ensuring that the AI models can scale to handle the increasing volume of users and access requests without compromising performance or introducing latency.

4. Explainability and Transparency: AI algorithms used in IAM can be complex and difficult to interpret. It is important to ensure that AI models used in IAM are explainable and transparent, meaning that the decisions made by the AI can be understood and justified. This is particularly important in scenarios where access decisions impact individuals' rights or privileges.

5. Integration and Compatibility: Implementing AI in IAM may require integrating AI models with existing IAM systems and infrastructure. Ensuring compatibility and seamless integration between AI and IAM components can be a challenge, especially in complex and heterogeneous IT environments.

6. Regulatory Compliance: IAM systems often need to comply with various regulations and standards, such as GDPR, HIPAA, or PCI DSS. Implementing AI in IAM requires ensuring that the AI models and algorithms used are compliant with these regulations and do not violate any privacy or security requirements.

Top AI use cases for the Fortune 500

1. Customer Service and Support: AI-powered chatbots and virtual assistants are used to provide automated customer support, answer frequently asked questions, and assist with basic inquiries. These AI systems can handle a large volume of customer interactions, provide personalized recommendations, and escalate complex issues to human agents when necessary.

2. Supply Chain Optimization: AI is used to optimize supply chain operations, including demand forecasting, inventory management, and logistics optimization. Machine learning algorithms can analyze historical data, market trends, and external factors to predict demand, optimize inventory levels, and streamline logistics processes.

3. Fraud Detection and Risk Management: AI is used to detect and prevent fraud in financial transactions and identify potential risks. Machine learning algorithms can analyze patterns, anomalies, and historical data to identify fraudulent activities, flag suspicious transactions, and mitigate risks.

4. Process Automation: AI is used to automate repetitive and manual tasks, improving efficiency and reducing human error. Robotic Process Automation (RPA) and AI-powered automation tools can handle tasks such as data entry, document processing, and workflow management.

5. Predictive Maintenance: AI is used to predict equipment failures and optimize maintenance schedules. Machine learning algorithms can analyze sensor data, historical maintenance records, and environmental factors to predict when equipment is likely to fail, enabling proactive maintenance and reducing downtime.

6. Talent Acquisition and HR: AI is used in talent acquisition processes, including resume screening, candidate matching, and interview scheduling. AI-powered tools can analyze resumes, assess candidate skills, and automate parts of the recruitment process, improving efficiency and reducing bias.

In summary…

- Review your current policies
- Coordinate with legal counsel
- Understand your current AI use “today” and map our your desired AI uses cases for tomorrow
- Implement an AI policy/guidance and/or modify your currently policy/policies
- Monitoring access to AI systems
- Ensure access is restricted as appropriate