Artificial Intelligence: AI Driven Talent Optimization

Business Context

Enterprises need agile talent strategies to stay competitive in a rapidly changing market. Traditional HR systems often fail to map evolving skills to open roles or provide actionable upskilling paths. This gap creates inefficiencies in workforce planning and limits career growth opportunities. AI agents can automate these processes at scale, but they introduce risks around bias, explainability, and data privacy. A successful solution must combine intelligent automation with strong governance and transparency.

Problem Description

Design an AI-driven talent strategy agent that:

1. Maps skills from employee profiles to open roles.
2. Generates personalized upskilling plans to close skill gaps.
3. Provides clear, human-readable explanations for recommendations.
4. Incorporates risk mitigation features, including:
    - Bias detection and fairness checks in role recommendations.
    - Explainable AI for why a role or learning path was suggested.
    - Data privacy safeguards for sensitive HR information.

The solution should balance accuracy, fairness, and transparency, while considering scalability for large organizations.

Desired Deliverables:

1. *Working Prototype*
    - Demonstrates skill-role matching and upskilling plan generation for at least 5 synthetic profiles.
    - Note: The solution must be used in an LLM-based approach.

2. *Explainability & Governance*
    - Explanation framework showing why roles and learning paths were recommended.
    - Governance packet including decision log, bias checks, and privacy safeguards.

3. Presentation & Demo
    - ≤10-slide deck summarizing problem, solution, architecture, and guardrails.
    - Short demo (video or live) highlighting functionality.

Success Criteria:

1. The solution must solve a real enterprise need and show clear value.
2. It must give accurate, meaningful role recommendations beyond keyword matching.
3. The upskilling plans must be practical, sequenced, and consider time and cost.
4. It must include transparent, human-readable reasons for all decisions.
5. The design must show bias checks and follow privacy-conscious principles.
6. It must address IT security risks and AI-related risks such as bias and misuse.
7. The solution must have robust, well-documented architecture.
8. It must deliver clear user experience with strong presentation and storytelling.

Business Analytics: Data-Driven Decision Making

Data is everywhere, but raw numbers do not tell a story on their own. The United States Federal Government established Data.gov in 2009 with the goal of improving public access to high value, machine-readable datasets. Since then, the site has grown to more than 370,000 datasets, capturing everything from lotto numbers to food prices to storm events. The data is the starting point, what you do with it tells the story.
Your challenge is to design and prototype a business analytics solution that combines descriptive analytics (summarizing and visualizing trends) with predictive modeling (forecasting what might happen next) using one or more of the data sets available on Data.gov to provide recommendations to decision-makers.

Your solution should:

1. Visualize insights: Build dashboards or reports that summarize trends, KPIs, and patterns.
2. Tell a story: Use visuals that highlight key takeaways and support decision-making.
3. Predict the future: Incorporate predictive modelling to help identify what will happen in the future.
4. Support decisions: Show how the platform helps identify risks, opportunities, and "what-if" scenarios.
5. Make recommendations: Use prescriptive models to give recommendations on how to move forward.
6. Describe your data sources, methods, and design choices.
    - The datasets you used (with links to Data.gov).
    - Your methods and tools.
    - Key design choices and rationale for your approach.

Deliverables:

1. A working demo highlighting dashboards, visualizations, and at least one predictive feature (descriptive, predictive, and prescriptive).
    - Dashboards or visualizations built from Data.gov data.
    - At least one predictive component (such as a simple forecast, trend model, machine learning prediction or etc.)
    - Clear connections between the data insights and recommendations for decision-makers.

By the end of this challenge, your solution will turn raw Government data from Data.gov into actionable insights and you will show your ability to communicate findings that drive smarter business decisions.

Cybersecurity: Strengthening Cyber Defense in Financial Services

In the heart of the Midwest, the city of Chicago is a major hub for financial services, hosting numerous banks and financial institutions that rely heavily on robust IT infrastructures. These institutions handle vast amounts of sensitive data, including customer financial information, transaction records, and investment portfolios. To manage and secure this data, the financial sector employs a complex array of IT systems, including core banking software, customer relationship management (CRM) systems, and data analytics platforms.

However, many of these IT systems were implemented over a decade ago and have not been updated to meet modern cybersecurity standards. This has made them susceptible to cyber threats, such as ransomware attacks, data breaches, and insider threats. Recent incidents, like the Fin7 cybercrime group's attacks on financial institutions and the REvil ransomware targeting global businesses, highlight the growing risks faced by the financial sector.

Your client, Midwest Central Bank, is a leading financial institution based in Chicago, responsible for managing billions of dollars in assets for its clients. With the increasing threat landscape and regulatory requirements such as the Gramm-Leach-Bliley Act (GLBA) and the Payment Card Industry Data Security Standard (PCI DSS), Midwest Central Bank's leadership has tasked your team with conducting a comprehensive IT Audit. The goal is to assess the current state of their IT systems, identify vulnerabilities, and recommend strategies to enhance cybersecurity and ensure compliance with relevant regulations.

Challenge

Using authoritative sources from government, academia, and industry, conduct an IT Audit for Midwest Central Bank that focuses on identifying major cybersecurity risks associated with their IT infrastructure. Develop a detailed report that includes:

- An evaluation of the current IT systems and their vulnerabilities.
- A risk assessment that prioritizes threats based on their potential impact on business operations.
- Practical, business-oriented strategies to mitigate identified risks, including recommendations for system upgrades, enhanced cybersecurity measures, and employee training programs.
- A compliance review to ensure alignment with regulatory standards such as GLBA and PCI DSS.

Deliverables

1. **10-minute Presentation**
    - Focus on key findings, top risks, and actionable recommendations.
    - Make it visually clear: charts, tables, and a simple “risk vs. impact” summary.
    - Short Audit Report included with only essential details: methodology, sources, key findings, recommendations, and compliance considerations.

Cybersecurity & Risk Analysis: Securing Critical Infrastructure Supporting Data Centers

Scenario

Northern Virginia hosts the world's largest concentration of data centers, which power today is rapidly growing artificial intelligence (AI) and cloud-based services. These facilities require immense amounts of electricity and water for continuous operations and cooling. Local utilities responsible for providing these services rely on **Operational Technology (OT)** such as supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), and industrial sensors to manage the infrastructure, pumps, valves, and substations delivering critical resources to both commercial and residential customers.

Many OT systems used throughout the country are decades old and not designed with cybersecurity in mind. As a result, they have become increasingly attractive targets for threat actors. Recent campaigns such as Volt Typhoon (China), Sandworm (Russia), and CyberAv3ngers (Iran) have focused on U.S. critical infrastructure—including water, energy, transportation, and manufacturing. Such threats have the potential to disrupt the data centers industry and government rely on for AI and cloud services, leading to widespread economic losses. Additionally, the unique integration of OT systems in industrial environments could result in physical damage to equipment and create dangerous safety conditions for employees.

Your client, Royal Duke Infrastructure Group, provides electricity and industrial water to several data centers in Loudoun County, Prince William County, and Fairfax County, Virginia. Following recent federal guidance on OT asset security, Royal Duke Infrastructure Group's leadership has asked your team to develop a Cyber Risk Assessment and Mitigation Plan that identifies vulnerabilities, prioritizes risks, and recommends cost-effective, realistic safeguards to protect critical infrastructure and ensure seamless data center operations.

Challenge

Using credible government, academic, and industry resources, evaluate the major cybersecurity risks facing Royal Duke Infrastructure Group's operational systems and propose practical, business-oriented strategies to reduce those risks.

Deliverables

Teams will submit:

1. A 5–10-minute video presentation summarizing findings and recommendations.

Presentation (Slide Deck)

1. Teams will present their findings to a panel of judges representing Royal Duke Infrastructure Group's executive board.
2. Presentation requirements
    1. **Format**
        1. Professional, consulting-style report
        2. PowerPoint, Google Slides, Canva, Prezi, or similar presentation platform.
        3. Slides should be clear, visually consistent, and properly sourced.
    2. **Content**
        1. **Overview:** Introduce Royal Duke Infrastructure Group's context and the problem statement.
            1. Describe Royal Duke Infrastructure Group's operational role and dependencies.
            2. Explain why OT systems are vulnerable and which cyber threats are most relevant.
            3. Include regional context - such as rising electricity demand to support existing and future data centers and the consequences of service disruptions.
        2. **Risk Identification**
            1. Key Risks: Identify your top three realistic cyber risks (use icons or simplified risk matrix)
            2. For each risk, explain.
                1. How it could occur (a short, realistic scenario)
                    1. Threat Scenarios: Explain realistic attack paths and potential consequences.
                2. Potential impact (financial, operational, safety, reputational, etc.)
                3. Likelihood (low, medium, or high)
        3. **Impact and Cost-Benefit Analysis**
            1. Estimate the potential business or operational impact of a cyber incident.
            2. Recommendations for at least three safeguards with rationale (i.e., cost vs. benefit) or mitigations, including description, relative cost level, and estimated benefit.
            3. Summarize how Royal Duke Infrastructure Group can balance investment, operational reliability, and resilience.
        4. **Implementation Roadmap:** Show timeline of short-, mid-, and long-term actions.
        5. **Business Impact Summary:** Explain expected improvements in risk posture and operational resilience.
    3. **References**
        1. Include a list of credible, properly formatted sources.

Recommended Frameworks & Methodologies

NIST: Cybersecurity Framework (CSF 2.0)
https://www.nist.gov/cyberframework
NIST: Risk Management Framework (RMF)
https://csrc.nist.gov/projects/risk-management
Lockheed Martin: Cyber Kill Chain®
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
CISA: Foundations for OT Cybersecurity – Asset Inventory Guidance for Owners and Operators
https://www.cisa.gov/resources-tools/resources/foundations-ot-cybersecurity-asset-inventory-guidance-owners-and-operators
ASD: Principles of Operational Technology Cyber Security
https://www.cisa.gov/resources-tools/resources/principles-operational-technology-cyber-security

Background Resources

CISA: Industrial Control Systems (ICS) Resources
https://www.cisa.gov/topics/industrial-control-systems
MITRE: ATT&CK for ICS
https://attack.mitre.org/matrices/ics/
MITRE: Common Attack Pattern Enumerations and Classifications (CAPEC)
https://capec.mitre.org/
WEF: The Dangerous Blind Spot in Infrastructure Cybersecurity
https://www.weforum.org/stories/2025/10/dangerous-blindspot-in-infrastructure-cybersecurity/
Dragos: OT Cybersecurity Fundamentals
https://www.dragos.com/insights/ot-cybersecurity-fundamentals
PwC: Global Digital Trust Insights
https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html
Deloitte: Can US infrastructure keep up with the AI economy?
https://www.deloitte.com/us/en/insights/industry/power-and-utilities/data-center-infrastructure-artificial-intelligence.html
IEEE: A Review of Colonial Pipeline Ransomware Attack
https://ieeexplore.ieee.org/document/10181159
Virginia JLARC: Data Centers in Virginia
https://jlarc.virginia.gov/landing-2024-data-centers-in-virginia.asp
NERC: Electricity Information Sharing and Analysis Center (E-ISAC)
https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx