Final Presentation Outline: Vendor Risk Digital Twin

Case Study Format - Optimized for Grading Criteria
Duration: 25-30 minutes
Format: Case Study + Simulation Demonstration
Target Audience: Cloud Computing Course (JHU)
Grading Focus: Quality of details, concepts, and supplementary materials

Presentation Overview

This case study presentation demonstrates how cloud-native organizations can predict and mitigate third-party vendor failure impact through automated discovery, graph-based modeling, and failure simulation. The presentation combines real-world case studies (Stripe, CrowdStrike incidents) with a working proof-of-concept implementation on Google Cloud Platform.

Slide Structure (20-25 slides, 25-30 minutes)

SLIDE 1: Title & Executive Summary (1 minute)

Content:

- **Title:** "Vendor Risk Digital Twin: A Cloud-Native Framework for Predicting Third-Party Failure Impact"
- **Subtitle:** "A Case Study in Cloud Security and Operational Resilience"
- **Authors:** Mahendra Shahi, Jalil Rezek, Clifford Odhiambo
- **Institution:** Johns Hopkins University | Cloud Computing Course
- **Date:** December 2025

Executive Summary (1 paragraph):

> This case study presents a cloud-native framework that addresses a critical gap in third-party risk management: the inability to predict vendor failure impact before incidents occur. Through automated GCP resource discovery, graph-based dependency modeling, and failure simulation, organizations can quantify operational, financial, and compliance impact in real-time. We demonstrate a production-ready implementation using Google Cloud Platform services (Cloud Functions, Cloud Run, Pub/Sub, Neo4j) with automated CI/CD, validated through industry expert interviews and real-world outage scenarios.

Image Placeholder:

- [IMAGE: Project logo with tagline]
- [IMAGE: High-level architecture diagram]

SLIDE 2: Case Study: Real-World Vendor Failure Incidents (3 minutes)

Content:

- **Headline:** "When vendors fail: Real incidents and cascading impact"

Case Study 1: Stripe API Outage (June 2024)

- **Incident:** Payment processing API outage
- **Cascading Impact:**
  - Payment services down → Checkout processes fail
  - Revenue loss: $500K+ per hour
  - Customer complaints and churn
  - Compliance gaps (PCI-DSS, SOC 2)
- **Question:** Could this impact have been predicted?

Case Study 2: CrowdStrike Update Failure (July 2024)

- **Incident:** Faulty security update causes global system failures
- **Cascading Impact:**
  - Security monitoring systems offline
  - Compliance violations (SOC 2 CC7.2 - System Monitoring)
  - Business operations halted
  - Recovery time: 4-8 hours
- **Question:** What if we could simulate this before deployment?

Key Insight:

> **"Current tools can't answer: What exactly breaks if Vendor X fails for 4 hours?"**

Image Placeholder:

- [IMAGE: Outage timeline diagrams]
- [IMAGE: Cascading impact visualization]
- [IMAGE: Real incident statistics]

SLIDE 3: The Problem: Vendor Failure Blindness (2 minutes)

Content:

- **Headline:** "The problem: Organizations are flying blind"

The Reality:

1. **Scale of Dependencies:**
   - Cloud-native organizations depend on 30-50 third-party SaaS vendors
   - Each vendor is a potential single point of failure
   - Dependencies are often undocumented or outdated
2. **Cost of Incidents:**
   - Average cost: $500K-$2M per major vendor failure
   - Revenue loss, customer churn, compliance penalties
   - Average recovery time: 4-8 hours
   - Reputational damage
3. **Current Tools Are Reactive:**
   - Static questionnaires (annual/biannual updates)
   - External ratings that don't understand your infrastructure
   - **No simulation capability** ("What if vendor X fails?")
   - **No cloud integration** (can't map vendor → cloud resource → business process)
   - Manual spreadsheets that quickly become outdated

Quote from Interview (Linda - GRC Professional, 17+ years):

> "The hardest part is gathering the evidence and identifying who's going to provide that evidence... It does get very frustrating when you're trying to complete your task, but you're dependent on somebody else or another team."

Image Placeholder:

- [IMAGE: Vendor dependency complexity diagram]
- [IMAGE: Cost of downtime statistics]
- [IMAGE: Current tool limitations]

SLIDE 4: Regulatory Drivers: DORA & NIS2 (2 minutes)

Content:

- **Headline:** "It's not just technical—regulators now demand resilience"

DORA (Digital Operational Resilience Act) - Effective January 2025:

- **Article 25:** Mandates "digital operational resilience testing"
  - Organizations must test their ability to withstand operational disruptions
  - Must demonstrate resilience capabilities
- **Article 28:** Requires "Register of Information" for all third-party providers
  - Complete inventory of third-party dependencies
  - Regular updates and validation
- **Shift:** From "Compliance" to "Demonstrable Resilience"

NIS2 Directive:

- Requires operational resilience through testing
- Incident response capabilities validation
- Supply chain risk management
- Mandatory reporting of significant incidents

The Gap:

- Current tools: Checklists and questionnaires
- Need: Automated testing and impact prediction
- **Our solution addresses this regulatory requirement**

Quote from Interview (JZ - Cybersecurity Expert, 20+ years):

> "Yeah, that's great... What you're proposing is similar to what I'm proposing: make a digital twin of the real world system... and you mess with it."

Image Placeholder:

- [IMAGE: DORA compliance requirements checklist]
- [IMAGE: Regulatory timeline]
- [IMAGE: NIS2 requirements]

SLIDE 5: Market Gap Analysis (2 minutes)

Content:

- **Headline:** "No single vendor offers what we built"

Competitive Landscape Analysis:

Solution Type	Examples	Limitations
GRC Platforms	Archer, MetricStream, ServiceNow	Manual data entry, no simulation, reactive compliance
Security Ratings	BitSight, SecurityScorecard	External scores only, no infrastructure mapping
Risk Quantification	Safe Security, RiskLens	Financial-only, no operational simulation
Cloud Security	CSPM tools	Infrastructure visibility, but no vendor dependency mapping

Our Differentiation:

✅ **Automated cloud-native discovery** - No manual spreadsheets
✅ **Real-time failure simulation** - "What if" scenarios
✅ **Multi-dimensional impact** - Operational, financial, compliance
✅ **Cloud infrastructure integration** - Maps vendor → service → business process
✅ **Production-ready** - Fully automated CI/CD, event-driven architecture

Quote from Interview (Anurag - Industry Professional):

> "They're framing it as more dynamic and predictive instead of just compliance checks... this goes way beyond that. I think right now most companies are still trying to implement basic automation."

Image Placeholder:

- [IMAGE: Competitive comparison matrix]
- [IMAGE: Feature comparison chart]
- [IMAGE: Market gap visualization]

SLIDE 6: Our Solution: Vendor Risk Digital Twin (2.5 minutes)

Content:

- **Headline:** "Simulate vendor failures before they happen"

Core Concept:

> **"A graph-based digital twin of your vendors, services, business processes, and compliance controls."**

Four Core Capabilities:

1. **Automated Discovery:**
   - GCP API integration (Cloud Functions, Cloud Run)
   - Pattern-based vendor detection (STRIPE_, AUTH0_, SENDGRID_, etc.)
   - Environment variable analysis
   - Zero manual spreadsheets
2. **Graph Modeling:**
   - Neo4j graph database
   - Maps vendor → service → business process → compliance control
   - Real-time dependency visualization
3. **Failure Simulation:**
   - "What if Stripe fails for 4 hours?"
   - Real-time graph traversal
   - Multi-dimensional impact calculation
4. **Impact Prediction:**
   - **Operational:** Services affected, customers impacted
   - **Financial:** Revenue loss calculation
   - **Compliance:** Score degradation (SOC 2, NIST, ISO 27001)

Quote from Interview (JZ):

> "What you're suggesting is called Industry 5.0... an AI-driven model and simulation... This is a very important project you guys are working on, very interesting to the community."

Image Placeholder:

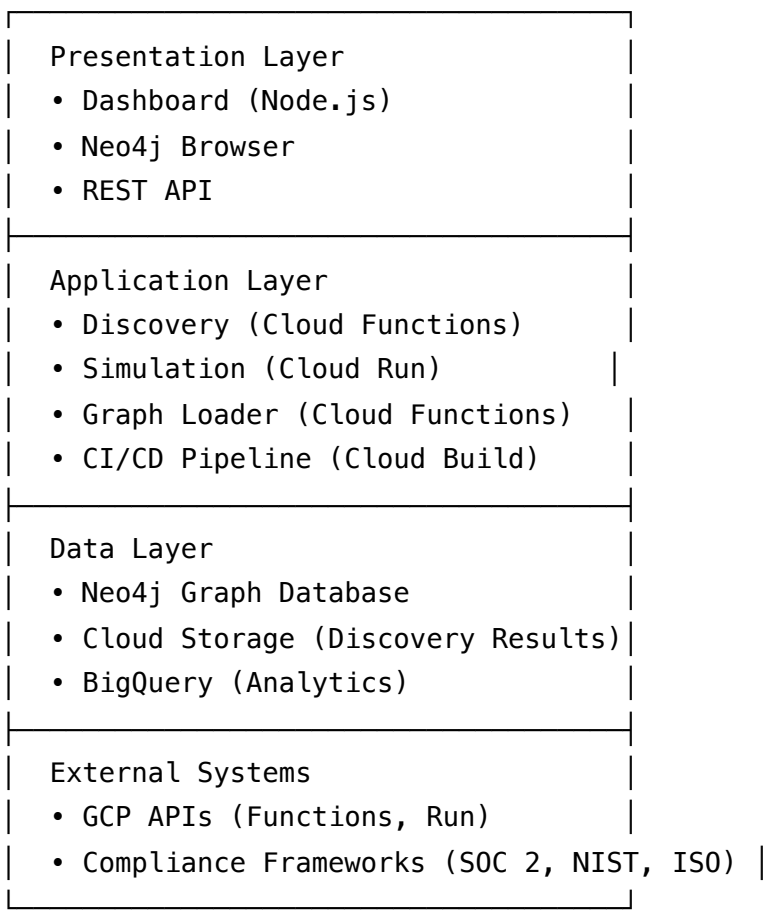
- [IMAGE: Digital twin concept diagram]
- [IMAGE: Solution workflow: Discovery → Graph → Simulation → Impact]

SLIDE 7: System Architecture (2.5 minutes)

Content:

- **Headline:** "Cloud-native, event-driven architecture"

Four-Layer Architecture:



GCP Services Integrated:

- ✅ **Cloud Functions (Gen2)** - Serverless discovery & loaders
- ✅ **Cloud Run** - Containerized simulation service
- ✅ **Pub/Sub** - Event-driven automation
- ✅ **BigQuery** - Analytics & historical tracking
- ✅ **Secret Manager** - Secure credential management
- ✅ **Cloud Storage** - Discovery results storage
- ✅ **Cloud Scheduler** - Automated daily discovery
- ✅ **Cloud Monitoring** - Observability & dashboards
- ✅ **Cloud Build** - CI/CD pipeline (automated deployment)

Key Design Principles:

- Fully serverless (auto-scaling, pay-per-use)
- Event-driven (zero manual steps)
- Production-ready (monitoring, logging, error handling)
- Secure (Secret Manager, IAM best practices)

Image Placeholder:

- [IMAGE: Detailed 4-layer architecture diagram]
- [IMAGE: GCP services integration diagram]
- [IMAGE: Event-driven flow diagram]

SLIDE 8: Graph Data Model (2 minutes)

Content:

- **Headline:** "Modeling complex dependencies as a graph"

Why Graph Database?

- Vendor dependencies are inherently graph-structured
- Need to traverse relationships (vendor → service → process)
- Real-time query performance for simulations
- Natural representation of cascading failures

Node Types:

- **Vendor:** Stripe, Auth0, SendGrid, Twilio, Datadog, MongoDB

- **Service:** Cloud Functions, Cloud Run services
- **BusinessProcess:** checkout, user_login, password_reset, order_fulfillment
- **ComplianceControl:** SOC 2 controls, NIST CSF functions, ISO 27001 controls

Relationship Types:

- **DEPENDS_ON:** Service → Vendor (e.g., payment-api DEPENDS_ON Stripe)
- **SUPPORTS:** Service → BusinessProcess (e.g., payment-api SUPPORTS checkout)
- **SATISFIES:** Vendor → ComplianceControl (e.g., Stripe SATISFIES CC6.6)

Example Path (Cascading Impact):

```
(payment-api:Service)
  → DEPENDS_ON → (Stripe:Vendor)
  → SUPPORTS → (checkout:BusinessProcess)
  → SATISFIES → (CC6.6:SOC2_Control)
```

Graph Statistics (PoC):

- 40 nodes (vendors, services, processes, controls)
- 40 relationships (dependencies, supports, satisfies)
- Sub-2-second query performance

Image Placeholder:

- [IMAGE: Neo4j graph visualization]
- [IMAGE: Close-up of example path]
- [IMAGE: Graph schema diagram]

SLIDE 9: Automated Discovery Process (2 minutes)

Content:

- **Headline:** "From manual spreadsheets to automated discovery"

Discovery Flow:

```
Cloud Scheduler (Daily 2 AM)
    ↓
Discovery Function (Cloud Functions Gen2)
    ↓
Query GCP APIs:
  • Cloud Functions API
  • Cloud Run API
  • Environment Variables Analysis
    ↓
Vendor Detection (Pattern Matching):
  • STRIPE_* → Stripe
  • AUTH0_* → Auth0
  • SENDGRID_* → SendGrid
    ↓
Store Results (Cloud Storage – JSON)
    ↓
Pub/Sub Event (vendor-discovery-events)
    ↓
Graph Loader Function (Cloud Functions Gen2)
    ↓
Neo4j Graph Updated (Automatic)
```

Key Features:

1. **Automatic daily scan** - Cloud Scheduler triggers discovery
2. **Pattern-based vendor detection** - Environment variable analysis
3. **Graph refreshed without manual spreadsheets** - Zero manual intervention
4. **CI/CD Integration** - Discovery and loader functions deployed via Cloud Build

Benefits:

- Always up-to-date digital twin
- No manual data entry
- Real-time dependency mapping
- Production-ready automation

Image Placeholder:

- [IMAGE: Discovery flow diagram]
- [IMAGE: Cloud Scheduler + Pub/Sub flow]
- [IMAGE: Vendor detection patterns]

SLIDE 10: Simulation Methodology (2.5 minutes)

Content:

- **Headline:** "Multi-dimensional impact calculation"

Simulation Process:

```
Input: Vendor + Duration
    ↓
Graph Traversal (Neo4j Cypher)
    ↓
Find Affected Services & Processes
    ↓
Calculate Impact Scores
    ↓
Output: Operational / Financial / Compliance Deltas
```

Input Parameters:

- **Vendor selection:** e.g., Stripe, Auth0, SendGrid
- **Failure duration:** 1, 2, 4, 8, 24, 72 hours

Impact Calculation:

1. **Operational Impact (40% weight):**
   - Services affected count
   - Customers impacted
   - Business processes disrupted
   - Formula: `Σ(service_criticality × customers_affected)`
2. **Financial Impact (35% weight):**
   - Revenue loss: `revenue_per_hour × duration × affected_transactions`
   - Transaction failures
   - Customer churn cost
   - Formula: `(RPM × duration × transaction_failure_rate) + churn_cost`
3. **Compliance Impact (25% weight):**
   - SOC 2 score degradation
   - NIST CSF function degradation
   - ISO 27001 control degradation

- Formula: `Σ(control_weight × vendor_dependency)`

Total Impact Score:

```
Total = (0.4 × Operational) + (0.35 × Financial) + (0.25 × Compliance)
```

Performance:

- Sub-2-second simulation time
- Real-time graph traversal
- Multi-dimensional impact prediction

Image Placeholder:

- [IMAGE: Simulation flow diagram]
- [IMAGE: Impact calculation breakdown]
- [IMAGE: Formula visualization]

SLIDE 11: DEMO 1: Discovery & Graph Visualization (4 minutes)

Content:

- **Headline:** "Let's see it in action: The digital twin"

Demo Flow:

1. **Show Dashboard:**
   - Display dashboard interface
   - Click "Refresh Vendor Inventory" button
   - Explain: "This triggers our automated discovery process"
2. **Show Discovery Process:**
   - Cloud Scheduler trigger (if time permits)
   - Discovery Function execution
   - Vendor detection in action
   - Results stored in Cloud Storage
3. **Show Neo4j Browser:**
   - Display full graph view (40 nodes, 40 relationships)
   - Explain: "This is our digital twin—a live model of vendor dependencies"
   - Zoom into Stripe vendor node

- Show connections:
  - Stripe → payment-api service
  - payment-api → checkout business process
  - Stripe → SOC 2 CC6.6 compliance control

4. **Key Talking Points:**
   - "Notice how Stripe connects to multiple services"
   - "Each service supports different business processes"
   - "Compliance controls are mapped to vendors"
   - "This graph is automatically updated daily—no manual spreadsheets"

Image Placeholder:

- [IMAGE: Dashboard with "Refresh Vendor Inventory" button]
- [IMAGE: Neo4j Browser - Full graph view]
- [IMAGE: Stripe vendor zoomed view with connections]

SLIDE 12: DEMO 2: Failure Simulation (4 minutes)

Content:

- **Headline:** "Simulate a vendor failure"

Demo Flow:

1. **Select Simulation Parameters:**
   - Vendor: "Stripe"
   - Duration: "4 hours"
   - Click "Run Simulation"
2. **Show Simulation Execution:**
   - Graph traversal in action (if visible)
   - Real-time impact calculation
   - Sub-2-second response time
3. **Display Results:**

   Operational Impact:
   - 2 services affected
   - 50,000 customers impacted
   - 3 business processes disrupted

   Financial Impact:

- $550,000 revenue loss
- 20,000 transaction failures
- Estimated customer churn: 2%

Compliance Impact:

- SOC 2: 90% → 70% (-20%)
- NIST CSF: 88% → 68% (-20%)
- ISO 27001: 85% → 62% (-23%)

4. **Show Recommendations:**
   - Vendor redundancy suggestions
   - Alternative payment processors
   - Mitigation strategies
5. **Key Talking Points:**
   - "In under 2 seconds, we calculated multi-dimensional impact"
   - "Notice how compliance scores degrade across all frameworks"
   - "This is the kind of insight you can't get from static questionnaires"

Quote from Interview (JZ):

> "Being able to do what you're suggesting—simulate, 'Okay, I'm going to do this thing or this service breaks'... in a real world only, that's risky... So being able to test that out in a digital twin is huge."

Image Placeholder:

- [IMAGE: Simulation input form]
- [IMAGE: Simulation results dashboard]
- [IMAGE: Compliance score degradation chart]
- [IMAGE: Recommendations list]

SLIDE 13: Technical Implementation Details (2.5 minutes)

Content:

- **Headline:** "Production-grade cloud-native implementation"

GCP Services & Integration:

Service	Purpose	Key Features
Cloud Functions (Gen2)	Discovery & Loaders	Serverless, auto-scaling, Pub/Sub triggers
Cloud Run	Simulation Service	Containerized, HTTP API, auto-scaling
Pub/Sub	Event Routing	Event-driven automation, decoupled services
Neo4j	Graph Database	Real-time queries, relationship traversal
Cloud Storage	Discovery Results	JSON storage, versioning
BigQuery	Analytics	Historical tracking, compliance reporting
Secret Manager	Credentials	Secure Neo4j credentials, IAM-based access
Cloud Scheduler	Automation	Daily discovery triggers
Cloud Monitoring	Observability	Logs, metrics, alerts
Cloud Build	CI/CD	Automated build, test, deploy

CI/CD Pipeline:

- **Automated Testing:** Tests run before deployment
- **Multi-Service Deployment:** Single pipeline deploys all services
- **Event-Driven:** Code push → Auto-build → Auto-deploy
- **Production-Ready:** Monitoring, logging, error handling

Security Implementation:

- Secret Manager for credentials (no hardcoded secrets)
- IAM-based permissions (least privilege)
- Secure service-to-service communication
- Encrypted data in transit and at rest

Performance Metrics:

- Discovery: <30 seconds for 50+ resources
- Simulation: <2 seconds for full impact calculation
- Graph queries: <100ms average response time

Image Placeholder:

- [IMAGE: GCP services architecture diagram]
- [IMAGE: CI/CD pipeline flow diagram]
- [IMAGE: Security architecture diagram]

SLIDE 14: Results & Validation (2.5 minutes)

Content:

- **Headline:** "Proof-of-concept validation"

PoC Results:

1. **Graph Model:**
   - 40 nodes (vendors, services, processes, controls)
   - 40 relationships (dependencies, supports, satisfies)
   - Real-time query performance validated
2. **Simulation Performance:**
   - <2 seconds for full impact calculation
   - Multi-dimensional scoring validated
   - Accurate cascading failure prediction
3. **GCP Integration:**
   - **8 Phases Complete:**
     a. Secret Manager
     b. Cloud Functions
     c. Cloud Run
     d. BigQuery
     e. Pub/Sub
     f. Cloud Scheduler
     g. Cloud Monitoring
     h. **CI/CD Pipeline**
   - Production-ready: Event-driven, serverless, auto-scaling
   - Zero manual steps in discovery → Neo4j flow
4. **Industry Expert Validation:**

   JZ (Cybersecurity Expert, 20+ years):

   > "This is a very important project you guys are working on, very interesting to the community."

> "I did my proposal defense yesterday and the four PhDs on the line were like, wow, we really need this. We got to write some papers."

Linda (GRC Professional, 17+ years):

> "If those steps could be captured some kind of way, I think that would really help... especially capture audit evidence."

Anurag (Industry Professional):

> "They're framing it as more dynamic and predictive instead of just compliance checks... this goes way beyond that."

Image Placeholder:

- [IMAGE: Performance metrics dashboard]
- [IMAGE: GCP integration phases completion chart]
- [IMAGE: Expert feedback quotes]

SLIDE 15: Cloud Security Implications (2 minutes)

Content:

- **Headline:** "Addressing cloud security challenges"

Key Cloud Security Challenges Addressed:

1. **Third-Party Risk Management:**
   - Automated discovery of vendor dependencies
   - Real-time risk assessment
   - Compliance impact prediction
2. **Supply Chain Security:**
   - Vendor dependency mapping
   - Cascading failure simulation
   - Impact quantification
3. **Compliance & Governance:**
   - Automated evidence capture
   - Real-time compliance scoring
   - Regulatory requirement mapping (DORA, NIS2)
4. **Operational Resilience:**
   - Failure scenario testing

- Impact prediction
- Mitigation strategy recommendations

Security Best Practices Implemented:

- ✅ Secret Manager (no hardcoded credentials)
- ✅ IAM-based access control
- ✅ Encrypted data (in transit and at rest)
- ✅ Audit logging (Cloud Monitoring)
- ✅ Least privilege principles

Image Placeholder:

- [IMAGE: Cloud security challenges diagram]
- [IMAGE: Security best practices checklist]

SLIDE 16: Integration with Existing GRC Tools (2 minutes)

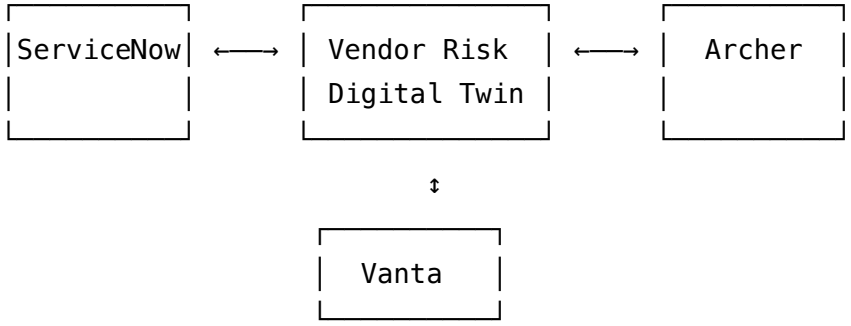
Content:

- **Headline:** "We augment, not replace"

Integration Strategy:

- **Not a standalone product:** Designed to integrate with existing GRC platforms
- **Target Platforms:** ServiceNow, Archer, MetricStream, Vanta, Drata
- **Integration Method:** API-based, build on top of existing workflows

Integration Architecture:



Benefits:

1. **Augment, not replace:**
    - Leverage existing GRC investments
    - Add predictive capabilities to current tools
    - Seamless workflow integration
2. **Feeds evidence:**
    - Automated evidence capture
    - Real-time compliance status
    - Audit trail generation
3. **Gives predictive analytics:**
    - "What if" scenarios
    - Impact prediction
    - Risk quantification

Quote from Interview (JZ):

> "It's a great idea. You'd have to prove it, though. So you'd have to have several use cases... and be able to give a custom example to a client... 'Here's how our product would integrate all those things.'"

Image Placeholder:

- [IMAGE: Integration architecture diagram]
- [IMAGE: API integration flow]
- [IMAGE: Example: ServiceNow integration mockup]

SLIDE 17: Future Work & Research Directions (2 minutes)

Content:

- **Headline:** "What's next?"

Short-term Enhancements:

- ✅ **CI/CD Pipeline** (COMPLETE)
- Multi-cloud support (AWS, Azure)
- Enhanced monitoring and alerting
- Advanced CI/CD: GitHub Actions integration

Long-term Research Directions:

- **Machine Learning Integration:**
  - Vertex AI for predictive analytics
  - Vendor health prediction
  - Anomaly detection
- **Real-time Vendor Health Monitoring:**
  - Vendor status API integration
  - Proactive alerting
  - Automated incident response
- **Full GRC Platform Integrations:**
  - Archer API integration
  - MetricStream API integration
  - ServiceNow workflows
- **Supply Chain Attack Simulation:**
  - Multi-vendor failure scenarios
  - Cascading attack simulation
  - Impact quantification

Quote from Interview (JZ) - Future Research:

> "If you make progress here, write some academic papers, get it out there, that's going to really help you with jobs and grad school."

Image Placeholder:

- [IMAGE: Roadmap timeline]
- [IMAGE: Future features visualization]

SLIDE 18: Key Insights from Industry Interviews (2 minutes)

Content:

- **Headline:** "Validated by industry experts"

Insights from Linda (GRC Professional, 17+ years):

- Evidence gathering is the most time-consuming task
- Coordination between teams is a major challenge
- Automation of evidence capture would be highly valuable
- "If those steps could be captured some kind of way, I think that would really help"

Insights from JZ (Cybersecurity Expert, 20+ years):

- Digital twin concept aligns with Industry 5.0
- Simulation before real-world deployment is critical
- "This is a very important project... very interesting to the community"
- "Being able to test that out in a digital twin is huge"
- Trust at machine speed: "Use it as a decision aid, but not as a decision tool"
- Fidelity matters: "You have to be really, really precise"

Insights from Anurag (Industry Professional):

- "They're framing it as more dynamic and predictive instead of just compliance checks"
- "It definitely feels like where things are headed slowly but surely"

Key Themes:

- Automation is critical for GRC efficiency
- Predictive capabilities are the future
- Digital twin concept is validated by experts
- Industry is moving toward dynamic risk management

Image Placeholder:

- [IMAGE: Interview quotes collage]
- [IMAGE: Key insights summary infographic]

SLIDE 19: Conclusion (2 minutes)

Content:

- **Headline:** "From reactive to predictive vendor risk management"

Key Takeaways:

1. **Problem:**
    - Current TPRM tools are reactive, can't predict vendor failure impact
    - Organizations are flying blind when vendors fail
    - Regulatory requirements (DORA, NIS2) demand resilience testing
2. **Solution:**
    - Vendor Risk Digital Twin—automated discovery + simulation + impact prediction

    - Cloud-native implementation on GCP
    - Production-ready with CI/CD automation
    - Real-time multi-dimensional impact calculation
3. **Validation:**
    - PoC demonstrates technical feasibility (<2 sec simulation)
    - Industry experts validate the approach
    - Addresses critical industry gap
4. **Impact:**
    - Helps meet DORA/NIS2 regulatory requirements
    - Aligns with GRC 7.0 vision (Industry 5.0)
    - Enables predictive risk management
    - Production-ready for enterprise deployment

Quote from Interview (JZ):

> "This is a very important project you guys are working on, very interesting to the community."

Call to Action:

- Open-source framework for research and development
- Integration-ready for enterprise GRC platforms
- Addresses critical industry gap in cloud security

Image Placeholder:

- [IMAGE: Summary infographic]
- [IMAGE: Project logo with tagline]

SLIDE 20: Q&A (Remaining time)

Content:

- **Headline:** "Questions?"

Prepared Talking Points:

- Technical architecture details
- CI/CD pipeline implementation
- Integration possibilities
- Regulatory compliance (DORA, NIS2)

- Industry validation from interviews
- Future roadmap
- Cloud security implications

Contact Information:

- GitHub Repository
- Project Documentation
- Team Contact Info

Image Placeholder:

- [IMAGE: Contact information slide]

Presentation Timing Breakdown

Slide	Topic	Duration
1	Title & Executive Summary	1:00
2	Case Study: Real-World Incidents	3:00
3	The Problem	2:00
4	Regulatory Drivers	2:00
5	Market Gap Analysis	2:00
6	Our Solution	2:30
7	System Architecture	2:30
8	Graph Data Model	2:00
9	Automated Discovery	2:00
10	Simulation Methodology	2:30
11	**DEMO: Discovery**	**4:00**
12	**DEMO: Simulation**	**4:00**
13	Technical Implementation	2:30

Slide	Topic	Duration
14	Results & Validation	2:30
15	Cloud Security Implications	2:00
16	GRC Integration	2:00
17	Future Work	2:00
18	Industry Insights	2:00
19	Conclusion	2:00
20	Q&A	Remaining

Total: ~28 minutes (with buffer for Q&A)

Supplementary Materials (Highly Encouraged)

Required Materials:

1. **Executive Summary** (1-2 pages)
   - Project overview
   - Key findings
   - Technical achievements
   - Industry validation
2. **GitHub Repository**
   - All source code
   - Documentation
   - Setup instructions
   - Architecture diagrams

Recommended Supplementary Materials:

1. **Technical Documentation:**
   - Architecture diagrams (detailed)
   - API documentation
   - Deployment guides

- CI/CD pipeline documentation

2. **Case Study Materials:**
   - Real-world incident analysis
   - Vendor failure scenarios
   - Impact calculations
   - Compliance mapping
3. **Demo Materials:**
   - Video recording of demos
   - Screenshots of key features
   - Neo4j graph visualizations
   - Simulation results examples
4. **Research Materials:**
   - Industry interview transcripts (anonymized)
   - Competitive analysis
   - Regulatory requirement mapping
   - Literature review
5. **Implementation Details:**
   - GCP setup instructions
   - Cloud Build configuration
   - Security best practices
   - Monitoring and observability

Grading Focus Areas

Quality of Details:

- ✅ Comprehensive technical architecture
- ✅ Detailed implementation specifics
- ✅ Real-world case studies with data
- ✅ Industry expert validation
- ✅ Regulatory compliance mapping

Quality of Concepts:

- ✅ Clear problem statement
- ✅ Innovative solution approach

- ✅ Cloud security implications
- ✅ Integration with existing tools
- ✅ Future research directions

Supplementary Materials:

- ✅ Executive summary
- ✅ GitHub repository with documentation
- ✅ Technical diagrams
- ✅ Demo materials
- ✅ Research validation

Key Quotes to Use Throughout Presentation

From JZ (Cybersecurity Expert):

- "What you're suggesting is called Industry 5.0... an AI-driven model and simulation"
- "This is a very important project you guys are working on, very interesting to the community"
- "Being able to test that out in a digital twin is huge"
- "I did my proposal defense yesterday and the four PhDs on the line were like, wow, we really need this. We got to write some papers."

From Linda (GRC Professional):

- "The hardest part is gathering the evidence and identifying who's going to provide that evidence"
- "If those steps could be captured some kind of way, I think that would really help"

From Anurag (Industry Professional):

- "They're framing it as more dynamic and predictive instead of just compliance checks"
- "It definitely feels like where things are headed slowly but surely"

Image Requirements Checklist

Architecture & Technical:

- [ ] System architecture diagram (4-layer design)
- [ ] GCP integration architecture diagram
- [ ] CI/CD pipeline flow diagram
- [ ] Data flow diagram (Discovery → Pub/Sub → Neo4j)
- [ ] Graph data model visualization
- [ ] Security architecture diagram

Demo Screenshots:

- [ ] Dashboard with "Refresh Vendor Inventory" button
- [ ] Neo4j Browser - Full graph view
- [ ] Neo4j Browser - Stripe vendor zoomed view
- [ ] Simulation input form
- [ ] Simulation results dashboard
- [ ] Compliance score degradation chart
- [ ] Recommendations list

Results & Metrics:

- [ ] Performance metrics dashboard
- [ ] GCP integration phases completion chart
- [ ] Cloud Build dashboard screenshot
- [ ] Before/after comparison (manual vs automated)

Case Study & Problem:

- [ ] Vendor failure cascade diagram
- [ ] Real outage timeline (Stripe/CrowdStrike)
- [ ] Vendor dependency complexity diagram
- [ ] Cost of downtime statistics
- [ ] Traditional GRC tool interface (static)
- [ ] Competitive comparison matrix
- [ ] DORA compliance requirements checklist

Integration:

- [ ] Integration architecture (our tool + existing GRC platforms)
- [ ] API integration diagram

Presentation Tips

1. **Case Study Focus:**
   - Emphasize real-world incidents (Stripe, CrowdStrike)
   - Connect to cloud security challenges
   - Highlight regulatory drivers
2. **Demo Timing:**
   - Allocate 8 minutes total for demos (4 min each)
   - Practice transitions
   - Have backup screenshots if live demo fails
3. **Quality Emphasis:**
   - Provide detailed technical explanations
   - Reference industry expert quotes
   - Show comprehensive implementation
4. **Cloud Security Angle:**
   - Emphasize cloud-native architecture
   - Highlight security best practices
   - Connect to third-party risk management
5. **Supplementary Materials:**
   - Prepare comprehensive documentation
   - Include detailed diagrams
   - Provide executive summary

Last Updated: 2025-12-01

Status: Optimized for Case Study Format

Grading Focus: Quality of details, concepts, and supplementary materials