ISSN: 2473-4901
v12 n6703

Governing Cybersecurity in Food and Agriculture Critical Infrastructure: An Applied Case Study of Archer Daniels Midland (ADM)

RJ Podeschi
rpodeschi@millikin.edu
Millikin University
Decatur, Illinois, 62522, U.S.A.

Abstract

The food and agriculture sector represents one of sixteen federally designated critical infrastructure categories in the United States, yet it operates without a mandatory cybersecurity framework comparable to those governing the energy or financial services sectors. This paper examines cybersecurity governance in food and agriculture critical infrastructure through a qualitative, document-based governance assessment using Archer Daniels Midland Company (ADM) as an illustrative case. ADM's scale, public disclosure obligations, and IT/OT (Information Technology/Operational Technology) convergence challenges make it a theoretically significant exemplar for the sector. Drawing on ADM's 2024 Securities and Exchange Commission (SEC) Form 10-K filing and publicly available governance disclosures, the analysis applies two complementary theoretical lenses: the Three Lines of Defense Model and the governance isolation framework. Findings indicate that while ADM satisfies current voluntary framework and regulatory requirements, gaps in publicly disclosed governance practices exist in OT security program depth, the structural independence of governance functions, and the formalization of supply chain cybersecurity risk management. The paper argues that the sector's cybersecurity challenge is not primarily technical but structural and regulatory, rooted in governance architectures that isolate security risk from strategic decision-making and in the absence of mandatory baseline requirements that would sustain board-level attention to OT risk. Three sector-level recommendations are offered addressing OT security program maturation, governance independence, and supply chain security. The paper also discusses implications for information systems (IS) governance research, regulatory policy development, and the pedagogical use of SEC 10-K disclosures as applied learning resources in cybersecurity and IS education.

Keywords: cybersecurity, governance, food, agriculture, operational technology, compliance

Governing Cybersecurity in Food and Agriculture Critical Infrastructure: An Applied Case Study of Archer Daniels Midland (ADM)

RJ Podeschi

1. INTRODUCTION

The security of the global food supply chain is a critical cybersecurity concern. As industrial operations become increasingly dependent on interconnected information technology (IT), the organizations that produce and supply food ingredients and products to the world have become high-value targets for sophisticated cyber adversaries. Archer Daniels Midland (ADM), headquartered in Chicago, Illinois, sits at the center of this intersection. Founded in 1902 and now a Fortune 35 multinational operating in over 190 countries, ADM functions as an essential player in the global agricultural supply chain, processing crops that supply approximately 70% of the average American's diet (Dager, 2024). ADM's operations span grain origination, transportation, oilseed crushing, carbohydrate processing, and nutritional ingredient manufacturing across hundreds of processing facilities globally. Each of these relies on a complex web of enterprise IT, supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLC), and an expanding portfolio of Internet of Things (IoT)-connected devices (ADM, 2024; Stouffer et al., 2023). A successful cyberattack against ADM's operational infrastructure would not merely disrupt a single company's production; it could cascade through the food supply chains of billions of people worldwide. This is why the U.S. Department of Homeland Security designates food and agriculture as one of 16 critical infrastructure sectors requiring national-level protection.

Despite the scale of this risk, food and agriculture organizations face a fragmented and demanding compliance landscape with no single regulatory framework designed specifically for the sector (Bustamante et al., 2025). As a publicly traded multinational organization, ADM must simultaneously satisfy myriad requirements across more than 190 operating countries. This paper examines ADM as a case study in the IT policies, compliance frameworks, and legal requirements that govern cybersecurity in the food and agriculture critical infrastructure sector and provides strategic recommendations necessary for an organization of ADM's scope, complexity, and global reach to manage cyber risk effectively in the era of escalating threats. This paper contributes to the applied information systems (IS) literature by examining how a leading food and agriculture multinational navigates a fragmented compliance landscape and where structural gaps remain. The analysis is grounded in two complementary theoretical lenses: Bongiovanni et al.'s (2024) Three Lines of Defense Model, which frames cybersecurity governance effectiveness in terms of structural independence across operational, risk and compliance, and audit functions, and Parenty and Domet's (2019) governance isolation argument, which holds that cybersecurity failures in industrial organizations originate not from technical deficiencies but from structures that prevent security risk from reaching strategic decision-making channels. This paper addresses the following research question: To what extent do publicly available governance disclosures from a major food and agriculture critical infrastructure organization reveal alignment with and gaps in established cybersecurity governance frameworks?

2. DISCUSSION AND LITERATURE

2.1 IT and Cyber Policies, Issues, and Challenges

The cybersecurity challenges confronting ADM begin at the architecture level, where IT enterprise data and supply chain management systems converge with operational technology (OT) systems governing production processes across hundreds of globally distributed facilities. Stouffer et al. (2023) document how this convergence expands the attack surface available to cyber adversaries where previously, OT environments relied on air gaps to isolate critical machinery from external networks. The emergence of Agriculture 4.0, Internet of Things (IoT), precision agriculture, and digital supply chain optimization has eroded the air gap separation as more equipment connects to corporate networks. Legacy integrated control systems (ICS) components, including systems designed decades before network connectivity was contemplated, now communicate with enterprise platforms that are themselves exposed to the

broader internet, creating pathways that adversaries can traverse from a phishing email to a physical process controller. At a large multinational food and agriculture production organization like ADM, the drive toward real-time production data, predictive maintenance, and enterprise resource planning (ERP) integration has connected OT systems to corporate networks in ways that exponentially expand the attack surface.

The operational implications of this convergence are compounded by the characteristics of legacy OT equipment in food and agriculture facilities. Unlike enterprise IT systems that receive regular software updates and vendor-issued patches, OT devices frequently operate on proprietary operating systems built for stability with update cycles measured in years or decades, or not at all. The Cybersecurity and Infrastructure Security Agency (CISA) has specifically documented the authentication challenges that arise in OT environments, noting that many communication protocols in common industrial use were designed without authentication mechanisms and that retrofitting cryptographic controls onto legacy hardware is technically difficult and operationally disruptive (CISA, 2024). ADM disclosed in its fiscal year 2024 Form 10-K that technology risk represents a material enterprise concern, despite no recorded events, and the company is actively working to improve its cybersecurity posture. The 10-K acknowledges that operational disruptions from cyberattacks could damage physical assets and impair business continuity, which reflects an awareness that IT and OT risk are now inseparable at the enterprise level (ADM, 2024). ADM's chief information security officer (CISO) further disclosed in 2024 that the company manages approximately 55 million security alerts annually, reflecting the breadth of a network footprint that has made food and agriculture organizations high-priority targets for motivated cybercriminals (Dager, 2024). Kulkarni et al. (2025) confirm this trajectory through their systematic review of 30 cybersecurity incidents in the food and agriculture sector between 2011 and 2023, documenting a measurable increase in ransomware attacks, supply chain intrusions, and OT-targeted incidents. ADM’s cybersecurity risk is further elevated given their ongoing enterprise resource planning (ERP) system upgrades per their 10-K (ADM, 2024), as technology platforms change and business processes are redefined to meet new system requirements.

2.2 Compliance and Governance

ADM’s compliance obligations span multiple overlapping frameworks that collectively impose significant governance demands. As a publicly traded company, ADM is subject to the U.S. Securities and Exchange Commission (SEC) cybersecurity disclosure rules adopted in July 2023, which require public companies to disclose material cybersecurity incidents within four business days of determination and to provide annual disclosures describing their risk management programs, governance structures, and board oversight mechanisms (SEC, 2023). Chen et al. (2025) highlight how this pivotal change in SEC disclosures adds to investor confidence, increases transparency, and prioritizes cybersecurity as an integral component of any enterprise. ADM’s 2024 10-K filing reflects these requirements where the board of directors receives cybersecurity briefings through the Sustainability and Technology Committee on a quarterly basis and the company’s Enterprise Risk Management (ERM) framework integrates cybersecurity risk alongside other risk categories (ADM, 2024). ADM's own 10-K (2024) identifies IT interruptions, cybersecurity breaches, and generative artificial intelligence (AI) among its greatest risks. Furthermore, their disclosures discuss formal processes for identifying risks associated with third-party vendors and escalation processes. Bongiovanni et al. (2024) identify a key determinant of cybersecurity governance effectiveness through their Three Lines of Defense Model, which include structural independence between operational management, risk and compliance functions, and internal audit. ADM's public disclosures do not provide sufficient detail to confirm whether second- and third-line functions operate independently. This disclosure gap is itself analytically significant: Bongiovanni et al. (2024) identify structural independence as a key determinant of governance effectiveness, and organizations whose disclosures do not address it cannot demonstrate this characteristic to external stakeholders, investors, or regulators. Parenty and Domet (2019) argue that cybersecurity governance failures frequently originate not from technical deficiencies but from organizational structures that allow security risk to be managed in isolation from strategic decision-making, a pattern particularly prevalent in industrial organizations where OT security has historically been treated as an engineering concern rather than a governance one. Although ADM satisfies current disclosure requirements, reliance on chief information officer (CIO) and CISO-generated reports at the board and C-suite levels raises the governance independence concerns Bongiovanni et al. (2024) identify.

NIST CSF 2.0, released in 2024, has emerged as the dominant voluntary governance architecture for critical infrastructure organizations in the United States, including food and agriculture sector participants. The framework expanded its original five functions, Identify, Protect, Detect, Respond, and Recover, by adding a sixth: Govern (NIST, 2024). The Govern function is particularly significant for organizations of ADM's complexity because it explicitly elevates cybersecurity from a technical operational matter to a strategic governance responsibility, requiring organizations to establish policies, roles, and accountability structures at the board and executive level. NIST CSF 2.0 also introduced organizational profiles, which allow enterprises to document their current cybersecurity state against a target state, facilitating gap analysis and measurable improvement planning (NIST, 2024). For a publicly traded multinational facing SEC disclosure requirements, this structured self-assessment capability creates a natural linkage between internal governance maturity and the public disclosures that investors and regulators now expect.

2.3 Legal Requirements

The legal landscape for food and agriculture cybersecurity in the United States is characterized by voluntary frameworks and sector-specific guidance rather than mandatory baseline requirements (Grama, 2022). Unlike the energy sector, which is subject to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, or the financial services sector governed by federal prudential regulation, food and agriculture organizations face no comparable mandatory baseline. This means that ADM's primary cybersecurity obligations come from SEC disclosure rules, the European Union's (EU) General Data Protection Regulation (GDPR), and obligations embedded in contractual agreements (Grama, 2022; SEC, 2023). Bustamante et al. (2025) argue this regulatory gap represents a system vulnerability, as organizations face strong economic incentives to defer security investment in the absence of mandatory requirements. Yusa et al. (2023) provide additional context by finding ADM's exposure to state-sponsored cyber threats has grown in proportion to global food trade, which underscores the tension between the company's strategic importance to global food security and the voluntary nature of cybersecurity governance. Mandatory baseline requirements carry the risk of compliance burden concentration among larger organizations and competitive disadvantage for smaller sector participants, a tradeoff that any regulatory design must explicitly address (Grama, 2022).

2.4 Systemic and Supply Chain Risk

The 2024 CrowdStrike outage demonstrated that critical infrastructure organizations face systemic risks that extend well beyond their own network perimeter. Santos-Reyes (2025) analyzes the systemic risk implications of major technology disruptions in critical infrastructure, using the 2024 CrowdStrike global IT outage as a case study to illustrate how dependencies on common technology platforms can translate a single point of failure into a multi-sector crisis. Ogundipe and Aweto (2024) similarly examine the CrowdStrike incident to argue that the concentration of critical infrastructure dependence on a small number of technology vendors creates systemic vulnerabilities that no individual organization's security program can fully mitigate. For an organization of ADM's disclosed profile, a Fortune 35 enterprise with hundreds of global facilities and an expanding third-party technology portfolio, Santos-Reyes' (2025) findings suggest that a targeted or incidental disruption to a shared platform could simultaneously affect grain origination, processing, and logistics systems. Parenty and Domet (2019) argue that senior leaders in organizations of this scale must move beyond asset-level risk thinking to understand cybersecurity as a strategic governance challenge with implications for national and global food security, a framing that uniquely applies to ADM's position in global agricultural supply chains.

3. METHODOLOGY

This study employs a qualitative, single-case study design using systematic analysis of publicly available corporate documents. Primarily, ADM's 2024 SEC 10-K filing and associated annual report as well as a CISO disclosure (ADM, 2024; Dager, 2024) were used as source evidence. Yin (2018) distinguishes between single-case designs selected for their typicality and those selected for their theoretical significance, arguing that a case need not be statistically representative to generate transferable insights when it exemplifies a broader phenomenon. ADM satisfies this criterion on multiple dimensions as it is a publicly designated critical infrastructure operator, a publicly traded multinational subject to SEC cybersecurity disclosure requirements, and a food and agriculture sector participant whose IT/OT convergence challenges, voluntary compliance posture, and governance structure are characteristic of

large organizations across the sector (Bustamante et al., 2025; Kulkarni et al., 2025). The two theoretical lenses applied in this analysis are the Three Lines of Defense Model (Bongiovanni et al., 2024) and the governance isolation framework (Parenty & Domet, 2019). These provide the evaluative structure through which ADM's disclosed governance practices are assessed. Both frameworks are applied deductively, whereby ADM's public disclosures are examined for evidence of structural independence across governance lines and for indicators that security risk reaches board-level decision-making through channels independent of operational leadership. However, the absence of disclosure was treated as the inability to confirm rather than a gap in compliance.

ADM was selected through purposive sampling on four criteria: federal designation as a critical infrastructure operator, public company status creating mandatory disclosure obligations, Fortune 50 scale reflecting the sector's largest governance challenges, and a documented IT/OT convergence footprint spanning hundreds of global facilities. Document selection was bounded to disclosures published between January 2023 and December 2024 to capture the post-SEC disclosure rule environment. The two theoretical lenses were operationalized as coding categories: the Three Lines of Defense Model (Bongiovanni et al., 2024) directed analysis toward evidence of structural separation between operational management, risk and compliance functions, and internal audit; the governance isolation framework (Parenty & Domet, 2019) directed analysis toward evidence of whether security risk information reaches board-level decision-making through channels independent of operational leadership.

Data were drawn exclusively from publicly available sources, including ADM's 2024 annual report and SEC Form 10-K filing, peer-reviewed journal articles, NIST and CISA guidance publications, and practitioner sources where academic literature had not yet addressed emerging developments. This reliance on public disclosures is itself analytically significant as SEC 10-K filings represent a standardized, audited, and legally consequential disclosure that captures governance posture in ways that are comparable across publicly traded organizations in the sector. This methodology has a practical implication, as publicly available corporate disclosures such as SEC 10-K filings are underutilized resources for IS and cybersecurity education, and the analytical approach demonstrated here is transferable to graduate and upper-division undergraduate course assignments.

4. RECOMMENDATIONS

The analysis of governance structures across the food and agriculture critical infrastructure sector and the broader cybersecurity literature surfaces three recurring themes: the structural vulnerability introduced by IT/OT convergence in legacy industrial environments, the governance independence gaps that voluntary compliance frameworks leave unaddressed, and the systemic risk exposure created by third-party technology dependencies. Appendix A maps the literature findings from each of these themes to the three strategic recommendations that follow. Food and agriculture organizations should weigh each recommendation against their implementation complexity, opportunity cost, and strategic objectives, recognizing the disclosure patterns identified here are consistent with governance challenges Bustamante et al. (2025) and Kulkarni et al. (2025) document across the sector broadly.

4.1 OT Security Program Maturation

Food and agriculture organizations operating converged IT/OT environments should pursue formal OT security program maturation aligned with NIST SP 800-82 Rev. 3 as a baseline governance requirement rather than a voluntary aspiration. Stouffer et al. (2023) provide implementation guidance for network segmentation between IT and OT environments, vulnerability management programs, and continuous monitoring architectures that accommodate the real-time performance constraints of industrial control systems. CISA (2024) specifically recommends that critical infrastructure operators prioritize legacy OT authentication weaknesses as near-term risk reduction measures, given that many industrial communication protocols were deployed without authentication mechanisms and cannot be easily patched. Organizations subject to SEC cybersecurity disclosure requirements can further leverage OT security roadmap development as a mechanism for strengthening the specificity and defensibility of their annual disclosures.

4.2 Governance Independence

Food and agriculture organizations should strengthen the structural independence and resourcing of their second- and third-line cybersecurity governance functions, particularly where governance structures have been added incrementally rather than designed from the outset. Bongiovanni et al. (2024) find that independent risk and compliance functions and a well-resourced internal audit capability with cybersecurity expertise produce more consistent identification of governance deficiencies, though organizations should anticipate additional administrative overhead in implementation. Parenty and Domet (2019) argue that security risk visibility must reach the board through channels not filtered through the same operational leadership responsible for managing those risks, which can be traced to industrial organizations' longstanding treatment of cybersecurity as an engineering function rather than a governance responsibility. For organizations subject to SEC disclosure requirements, this means board oversight mechanisms should provide direct access to security leadership and should include OT security assessments conducted by auditors with ICS expertise, ensuring that board-level risk awareness reflects operational realities rather than upward-filtered reporting.

4.3 Supply Chain Security

Food and agriculture organizations should develop formal supply chain security risk management programs that extend governance requirements to critical technology vendors and business partners. NIST CSF 2.0 recommends that organizations establish minimum security requirements for technology suppliers and implement mechanisms for monitoring supplier security posture on a regular basis, a recommendation that carries weight given the sector's accelerating adoption of Agriculture 4.0 technologies and the AI-driven decision systems that introduce new third-party dependencies (NIST, 2024; Bustamante et al., 2025). The systemic risk implications of shared platform dependencies documented by Santos-Reyes (2025) in the CrowdStrike case illustrate that supply chain security failures in critical infrastructure rarely confine themselves to a single organization. Moreira et al. (2025) further identify blockchain-based integrity verification as an emerging option for securing supply chain data flows in agriculture OT environments, one that could simultaneously address cybersecurity and food safety traceability objectives.

5. FUTURE RESEARCH

Three directions for future research emerge from this analysis. The first concerns the effectiveness of voluntary cybersecurity governance frameworks in producing measurable security outcomes in the food and agriculture sector. Kulkarni et al. (2025) document the threat landscape and propose framework enhancements, but limited empirical evidence connects adoption to reduced incident frequency or severity at the sector level. A comparative study examining incident rates, disclosure practices, and framework adoption maturity across food and agriculture multinationals would provide valuable evidence for regulatory policy development and inform industry governance practice.

The second area concerns the governance implications of technology adoption in agricultural OT environments. Bustamante et al. (2025) document the acceleration of Agriculture 4.0 technology adoption within areas like autonomous equipment, precision sensing, and AI-driven decision systems. Existing cybersecurity frameworks were not designed to address the governance challenges these new technologies introduce. Moreira et al. (2025) explore blockchain as one potential OT security tool but acknowledge the evidence for its effectiveness in food sector deployments remains limited. Research examining how food and agriculture organizations govern the introduction of new OT-connected technologies would address a gap that neither NIST CSF 2.0 nor sector-specific guidance has yet filled.

Finally, this case study also has implications regarding pedagogy. The methodology employed in this study, specifically the analysis of SEC 10-K cybersecurity disclosures alongside public framework guidance, is readily transferable to IS and cybersecurity course assignments at the graduate and advanced undergraduate levels. Marquardson and Asadi (2023) provide a case analysis project related to risk registers using a fictitious company. Given enough information, this could be expanded to include publicly traded companies using SEC disclosures and secondary research. Future work could develop and assess structured assignments built around corporate disclosure analysis as a mechanism for developing students' applied governance reasoning skills.

6. CONCLUSIONS

This paper examined ADM as a case study in the IT policies, compliance frameworks, and legal requirements governing cybersecurity in the food and agriculture critical infrastructure sector. ADM's scale, global reach, and public disclosure obligations make it a theoretically significant case whose governance posture reflects conditions characteristic of large organizations across the sector. The qualitative analysis suggests that ADM's public disclosures indicate alignment with current voluntary framework and regulatory requirements, while revealing limited visibility into OT security program depth, the structural independence of governance functions, and the formalization of supply chain cybersecurity risk management. This analysis is limited to publicly available disclosures, and primary access to internal governance documentation would enable a more granular assessment of control effectiveness for any organization.

The central finding of this paper is that the food and agriculture sector's cybersecurity challenge is primarily structural and regulatory. The two theoretical lenses applied in this analysis converge on a shared diagnosis. Bongiovanni et al.'s (2024) Three Lines of Defense Model reveals that governance structures added incrementally rather than by design are consistently prone to independence failures between operational, risk and compliance, and audit functions. Parenty and Domet's (2019) governance isolation framework explains why those structural failures persist: in industrial organizations, security risk has historically been managed as an engineering function rather than a strategic governance responsibility, limiting the visibility that boards and senior leaders need to allocate appropriate attention and resources to OT risk. Together, these lenses point toward a governance gap that voluntary frameworks alone are insufficient to close. The ADM case provides a useful foundation for understanding both what leading-edge voluntary compliance looks like and where its boundaries lie. Bustamante et al. (2025) argue that the regulatory vacuum surrounding Agriculture 4.0 technologies leaves even well-resourced organizations without the external governance pressure necessary to sustain board-level attention to OT security risk. Closing that gap will require coordinated action across industry and government.

7. REFERENCES

Archer Daniels Midland. (2024). *2024 Annual Report (Form 10-k).* https://www.sec.gov/cgi-bin/browse-edgar?action=getcompany&CIK=0000007084&type=10-K

Bongiovanni, I., Slapničar, S., Axelsen, M., & Stockdale, D. (2024, February 21). The three lines model in cybersecurity governance and risk management. *ISACA Journal*, 2024(1). Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2024/volume-1/the-three-lines-model-in-cybersecurity-governance-and-risk-management?utm_source=isaca_internal&utm_medium=share_link

Bustamante, D., Sánchez, L., Rosado, D., Santos-Olmo, & Fernández-Medina, E. (2025). Towards a sustainable cybersecurity framework for Agriculture 4.0 based on a systematic analysis of proposals. *Computers & Security, 159*, Article 104650. https://doi.org/10.1016/j.cose.2025.104650

Chen, Y., Lokuku, D., & Wu, T. (2025). A Pivotal Progression of SEC's Cybersecurity Disclosure Requirements. *Cybersecurity Pedagogy and Practice Journal.* v4, n1, pp 35-44. DOI# https://doi.org/10.62273/MMYQ9950

Cybersecurity and Infrastructure Security Agency (CISA). (2024). Barriers to secure OT communication: Why Johnny can't authenticate. U.S. Department of Homeland Security. https://www.cisa.gov/resources-tools/resources/barriers-secure-ot-communications

Dager, T. (2024, October 7). CISO of Fortune 35 company talks 55 million alerts. Check Point Blog. https://blog.checkpoint.com/executive-insights/ciso-of-fortune-35-company-talks-55-million-alerts/

Grama, J. L. (2022). Legal and privacy issues in information security. Jones & Bartlett Learning.

Kulkarni, A., Wang, Y., Gopinath, M., Sobien, D., Rahman, A., & Batarseh, F. A. (2025). A review of cybersecurity incidents in the food and agriculture sector. *Journal of Agriculture and Food Research*, *23*. https://doi.org/10.1016/j.jafr.2025.102245

Marquardson, J., & Asadi, M. (2023). Cybersecurity Assessment for a Manufacturing Company Using Risk Registers: A Teaching Case. *Information Systems Education Journal,* 21(3). pp 62-69.

Moreira, F., Araujo, A., Moreira, A., & Durães, D. (2025). A review on blockchain applications in operational technology for food and agriculture critical infrastructure. *Foods*, 14(2), 251. https://doi.org/10.3390/foods14020251

National Institute of Standards and Technology (NIST). (2024). *The NIST Cybersecurity framework (CSF) 2.0* (NIST Cybersecurity White Paper NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Ogundipe, O., & Aweto, T. (2024). The shaky foundation of global technology: CrowdStrike outage case study*. International Journal of Multidisciplinary Research and Growth Evaluation*, 5(5), 106-108.

Parenty, T. J., & Domet, J. J. (2019). A leader's guide to cybersecurity: Why boards need to lead—and how to do it. Harvard Business Review Press.

Santos-Reyes, J. (2025). Planning for the unexpected: 2024 GITO impact on critical infrastructures. Sustainable Futures, 9, Article 100480. https://doi.org/10.1016/j.sftr.2025.100480

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2023). Guide to operational technology (OT) security (NIST SP 800-82 Rev. 3). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/82/r3/final

U.S. Securities and Exchange Commission (SEC). (2023, July 26). SEC adopts rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies. https://www.sec.gov/newsroom/press-releases/2023-139

Yin, R. K. (2018). *Case study research and design methods* (6th ed.). SAGE Publications.

Yusa, M. Y., Nizam, A. H., & Sartika, D. (2023). Business strategy of ADM amid pandemic and geopolitical conflict. *Andalas Journal of International Studies*, 12(2), 136-150. https://doi.org/10.25077/ajis.12.2.136-150.2023

APPENDIX A

Literature Findings and Corresponding Recommendations

Source	Finding / Contribution	Sector Recommendation
IT and Cyber Policies, Issues, and Challenges		
Stouffer et al. (2023)	IT/OT convergence expands attack surface; legacy ICS creates pathways from enterprise networks to process controllers.	OT Security Program Maturation
CISA (2024)	OT communication protocols lack authentication; retrofitting cryptographic controls is technically difficult.	OT Security Program Maturation
Kulkarni et al. (2025)	Documented increase in ransomware, supply chain intrusions, and OT-targeted incidents in food and agriculture, 2011–2023.	OT Security Program Maturation Supply Chain Security
NIST CSF 2.0 (2024)	Govern function elevates cybersecurity to board-level governance; organizational profiles support gap analysis.	Governance Independence
Compliance and Governance		
ADM (2024)	10-K identifies IT interruptions, cybersecurity breaches, and AI as material risks; quarterly board briefings via Sustainability and Technology Committee.	Governance Independence
SEC (2023); Chen et al. (2025)	Mandatory incident disclosure and annual governance reporting requirements; advances investor transparency.	Governance Independence
Bongiovanni et al. (2024)	Three Lines of Defense requires structural independence; organizations that add governance structures incrementally are prone to second- and third-line gaps.	Governance Independence
Parenty & Domet (2019)	Governance failures originate from structures that isolate security risk from strategic decision-making in industrial organizations.	Governance Independence
Legal Requirements		
Grama (2022)	U.S. approach relies on voluntary frameworks; food and agriculture lacks mandatory baseline comparable to energy or financial services.	Governance Independence
Bustamante et al. (2025)	Regulatory gap creates economic incentives to defer investment; Agriculture 4.0 adoption outpaces governance frameworks.	OT Security Program Maturation, Supply Chain Security
Yusa et al. (2023)	Exposure to state-sponsored threats grows in proportion to global food trade footprint.	OT Security Program Maturation
Systemic and Supply Chain Risk		
Santos-Reyes (2025)	CrowdStrike outage illustrates how shared platform dependencies translate single points of failure into multi-sector crises across critical infrastructure.	Supply Chain Security
NIST CSF 2.0 (2024); Moreira et al. (2025)	CSF 2.0 recommends supplier minimum security requirements; blockchain offers emerging option for OT supply chain integrity in agriculture environments.	Supply Chain Security