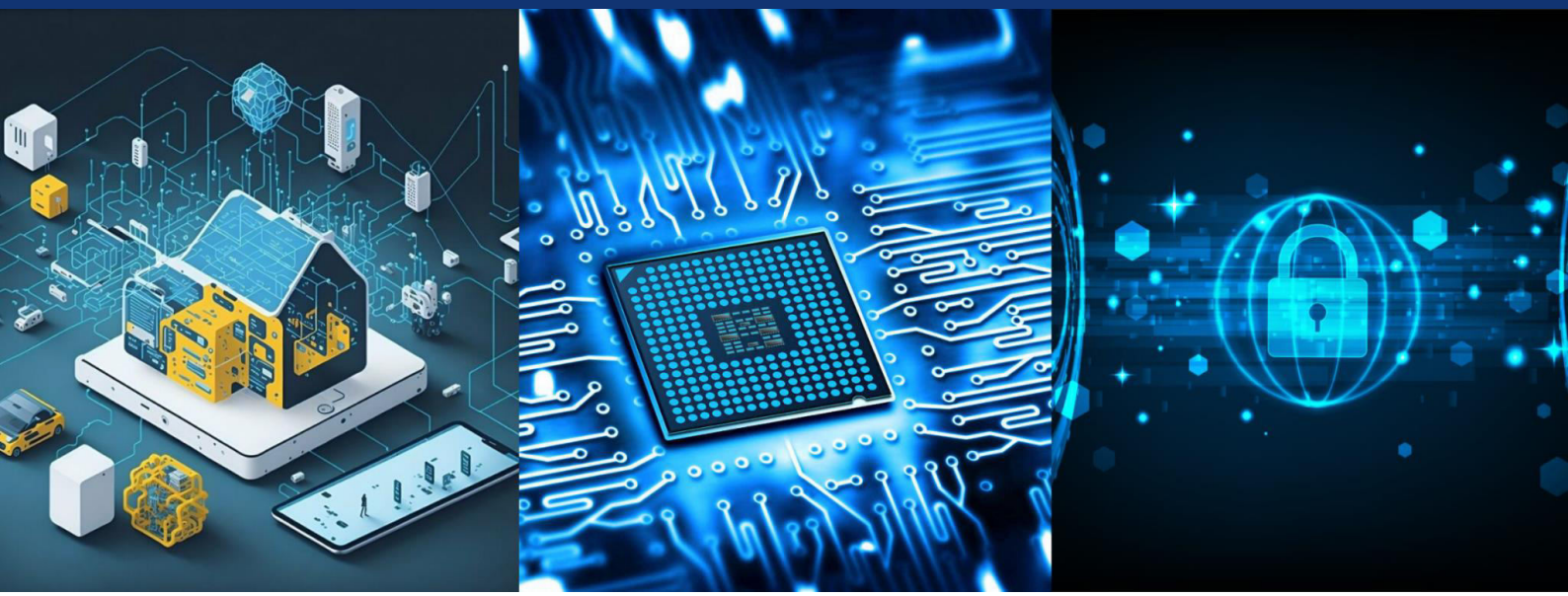
IJIRCCE

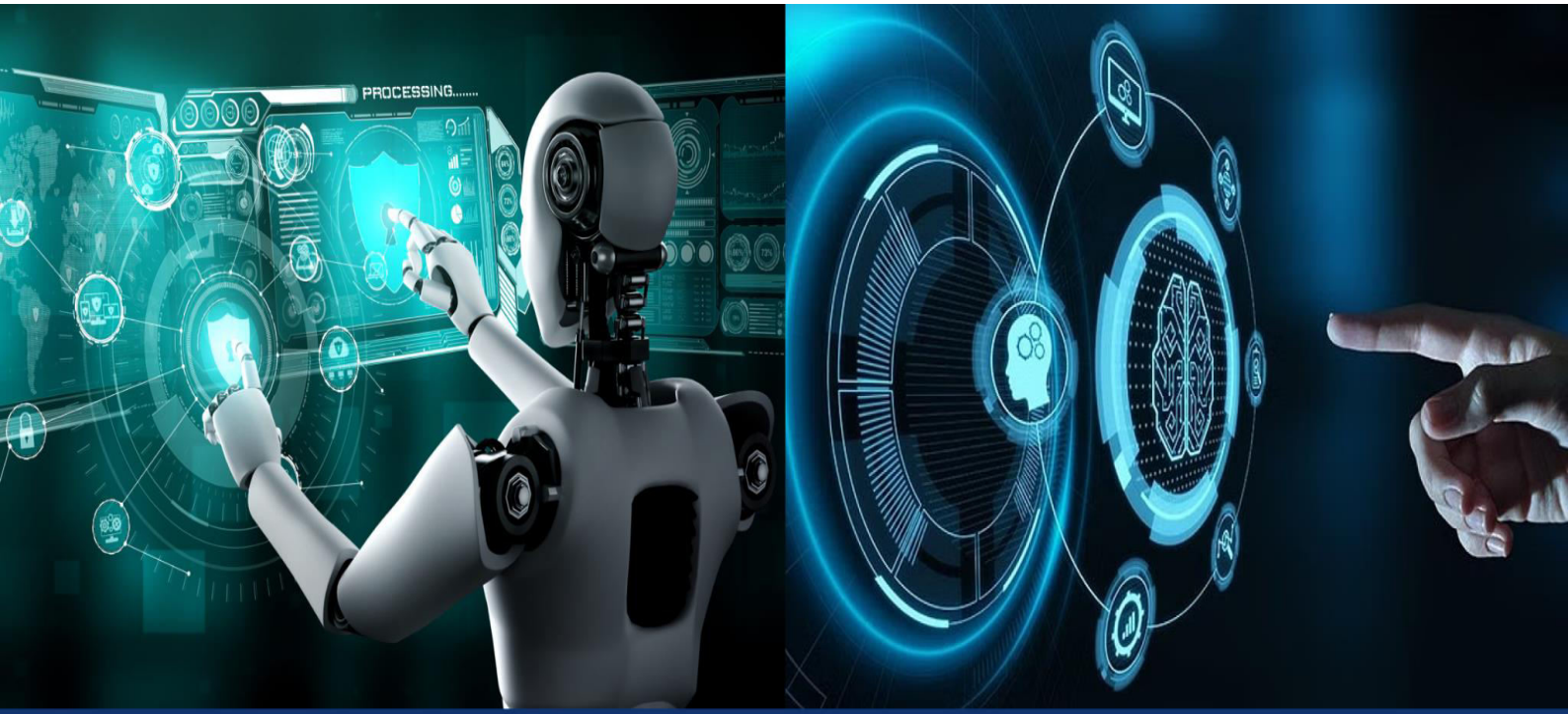
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 9, September 2026

© 2026 IJIRCCE | Volume 14, Issue 9, September 2026 DOI: 10.15680/IJIRCCE.2026.1409006

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Mitigating Cloud-Edge Shared Responsibility Risks in Digital Banking: A Case Study of Cyber Risk Management Practices in Indian Banks

Akshit Singh Walia

Department of Science, Sri Chaitanya Techno School, Chandigarh, India

ABSTRACT: Indian banks use a mix of cloud infrastructure and edge devices - ATMs, point-of-sale terminals, and devices used within branches which are IoT enabled - that exist outside of the neat boundaries of the cloud, shared responsibility model. This paper posits that the produced uncertainty of who controls which security boundary, and not any one of the many lacking technologies, is what enabled events of this nature to be successful, such as the 2018 Cosmos Bank ATM switch heist. The shared responsibility model is analyzed and extended beyond to edge computing and the evolving cyber security and outsourcing framework of the Reserve Bank of India is surveyed, as well as the Cosmos Bank case, the City Union Bank and its SWIFT breach case. A small, CSV-based, Python, and browser tool is then created to score "residual risk" based on actual assessment evidence, for example, audit results, VAPT, patching, and so on, as opposed to typical, "guess-timated" scores. This tool allows risk teams to establish an ordered, prioritized list of governance issues/cases that require the most attention. This paper ends with various recommendations for banks, and regulators, as well as technologists, and describes the potential of the tool within its limits.

I. INTRODUCTION

Rapid growth in digital banking has occurred in India. Bank transactions run in the billions monthly. Core banking workloads run in the cloud. Banks are moving the workloads further from the core to ATMs (Automated Teller Machines), POS (Point of Sale devices), and branch sensors (Lambropoulos et al., 2026). This is being done to reduce latency and maintain services when there are outages. Banks have also fully embraced cloud banking. Implementing edge computing has no equivalent to the shared responsibility model. Edge computing is either owned physically by the bank, or a vendor, runs legacy embedded systems, and has little to no coverage in cloud contracts.

This paper tries to answer the following question: when responsibility is shared by the cloud provider, bank, and edge device vendor, what is actually the case at the seams? A seam is not a technical weakness, such as a missing firewall or an unpatched library. Instead, seams are governance gaps. Since, by definition, seams and governance gaps are hard to find, will remain this way until a malicious actor decides to look for them. The goal of this paper is to show these governance gaps before they are exploited, as this is the theoretical goal as well.

This paper provides a case study of a seam being exploited by using the 2018 Cosmos Bank attack. It also describes a working tool that creates ranked lists of "responsibility risk" by using evidence rather than an unverified memory, reading inputs from a CSV export, as would be done by a real risk team. The first section describes the concept of a shared responsibility model. The second section shows its applicability to the edge. The third section discusses the regulatory framework of India. The fourth section describes the Cosmos Bank case. The fifth section describes the tool and its evidence pipeline. The sixth to the eighth sections are devoted to the findings and offer closing thoughts on this work.

II. THE SHARED RESPONSIBILITY MODEL

Cloud service providers allocate security responsibilities in a way Amazon Web Services terms "security of the cloud" (provider responsibility for physical data centers, hardware, virtualization, etc. and "security in the cloud" (customer responsibility for data, identities, applications, configuration, etc.) (Gadde et al., 2023). Microsoft Azure describes the same allocation of controls as customer, provider, and shared controls, where the shared controls vary based on the type of service ("Shared Responsibility in the Cloud - Microsoft Azure | Microsoft Learn," n.d.).

© 2026 IJIRCCE | Volume 14, Issue 9, September 2026 DOI: 10.15680/IJIRCCE.2026.1409006

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This shift is significant. In Infrastructure-as-a-Service (IaaS), the customer handles the bulk of the responsibility, owning the entire stack above the operating system. In Platform-as-a-Service (PaaS), the provider manages the operating system and the runtime. In Software-as-a-Service (SaaS), the provider manages nearly the entire stack, leaving the customer with primary responsibility for data governance and access (Humayun et al., 2022). The clear extremes of this spectrum don't present the greatest difficulties, but rather the gray areas where the responsibility overlaps. The confusion that results from overlapping responsibilities is what security researchers warn against, as teams tend to assume some degree of control is being enforced and do not verify in writing. In the banking industry, this is the same gap of assumption that leads to a breach.

The ISACA Journal reviews the shared responsibility of community clouds, and like banking, there is some ambiguity. With community cloud arrangements, the infrastructure is shared among organizations in the same regulated sector, which sits between public and private clouds. Once more, and in any arrangement, the split of responsibility only becomes meaningful if it is documented and signed by both parties with a contractual obligation to review it. It is, after all, a written agreement and not a default assumption (Understanding the Shared Responsibilities Model in Cloud Services, n.d.).

Table 1 shows a responsibility matrix across service models and edge devices. The term “MSP” stands for Managed Service Provider, for example, an ATM vendor.

Security Domain	IaaS	PaaS	SaaS	Edge Device
Physical facility & hardware	Provider	Provider	Provider	Bank / MSP
Network & host OS	Provider	Provider	Provider	Bank / MSP
Guest OS / runtime	Bank	Provider	Provider	Bank / MSP
Middleware & applications	Bank	Bank	Provider	Bank
Identity & access management	Bank	Bank	Bank	Bank
Data (encryption, classification)	Bank	Bank	Bank	Bank
Physical device tamper security	n/a	n/a	n/a	Bank / MSP
Firmware / embedded patching	n/a	n/a	n/a	Bank / MSP

Table 1 Simplified responsibility matrix across cloud service models and edge devices.

III. EXTENDING THE MODEL TO THE EDGE

Edge computing results in better services by relocating computation closer to data, such as at a branch, ATM, or point of sale. Edge computing allows for local fraud-scoring in real-time, enables branch operations even during system outages, and facilitates other data residency requirements (gaotek, n.d.). Although, edge devices do not comply with the model in Section 2. In a cloud framework, a provider's data boundary ends at the provider's data center and an ATM in one of the branches is located outside that boundary.

- Physical accessibility: an ATM or POS system is in a physically public location, while a data center rack is secured behind multiple forms of access control.
- Legacy software: Numerous edge devices rely on legacy embedded operating systems, which are infrequently updated outside of the vendor's discretionary timeline.
- An additional party: edge computing systems are operated under contract by a managed services provider.

The impact results in a chain with four links - cloud provider, bank, managed service provider, edge device - with the freedom to place a security control between each two links, since no single contract typically covers the entire chain.

This is decidedly a real world problem. Documented deployments evidence banks embedding IoT sensors into ATMs and Kiosks and using edge analytics to monitor health and transactions. Other deployments include edge-based image processing applied for transaction-based point fraud and identity checks (marketing et al., 2025). Deploying new edge processing modules is a valuable, yet significant, addition to a banks' security posture. Individual care must be allotted new device, data links, and vendor partnerships. Each deployment creates a new threat surface for a risk team to deal with, yet also provides a real improvement to the customer experience.

© 2026 IJIRCCE | Volume 14, Issue 9, September 2026 DOI: 10.15680/IJIRCCE.2026.1409006

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. REGULATORY LANDSCAPE GOVERNING INDIAN BANKS

Expecting cyber intrusions will happen, the Reserve Bank of India's Cyber Security Framework (2016) focuses on detection and recovery, in addition to prevention, and requires Master Direction's IT Services Outsourcing Policy (2023) to include incident reporting to the RBI CSITE cell, the mandatory appointment of a Chief Information Security Officer (CISO), and board approval of the cyber policy (RBI, 2016). The most recent Master Direction (2023) on the Outsourcing of Information Technology Services incorporates a separate annex for Cloud Computing, and requires a risk assessment, and the location of data at all times to be within the borders of India (Thales, n.d.). It additionally requires the assessment of cloud service providers to be continuous. The Master Direction on Governance of IT, Risk, Control & Assurance (2023) outlines the expectations for internal governance (Keshav Malik & Aakanksha Khanna, 2026).

The RBI Digital Lending Guidelines (2022) address the non-technical dimension of the shared responsibility problem whereby banks engage with various data aggregator and lending partner platforms. The Master Directions on Cyber Resilience and Digital Payment Security Controls (2024) expand the cyber-resilience requirements to non-bank payment operators, card networks, and payment aggregators as part of the broader bank payment- processing ecosystem (Data Protection Laws of the World, n.d.). In addition to the RBI framework, the Digital Personal Data Protection Act, 2023, and its implementing Rules, notified in November 2025 (Government of India, 2025), create a comprehensive data protection framework for banks with a protection of personal data focus.

Commentary on this framework repeatedly observes that small and cooperative banks usually have less capacity than large commercial banks to implement these controls. This has been the case even after RBI's implementation of a tiered system of the cybersecurity framework specifically for Urban Cooperative Banks (UCBs). This example directly applies to the case under consideration (Hod Gavriel & Meir Brown, 2018).

V. CASE STUDY: THE COSMOS BANK ATTACK

In August 2018, Cosmos Cooperative Bank, the second largest urban cooperative bank of India at that time, was compromised, and lost approximately ₹ 94 crores (about US$ 13.5 million) over a span of three days (Shiv Kumar, 2018). Malware targeted the bank's "switch", which is essentially a server that handles card authorisation between ATM networks, the Visa and RuPay networks, and the bank's core system. Malware was used to create a rogue parallel switch. This switch authorisation was able to bypass the check for actual balance present in the account, and, as a consequence, fraudulent transactions were sent for authorisation and were approved (Colortokens, 2024). There were approximately 14,000 such transactions that were carried out over the two-day period (i.e., 11th and 12th August), in addition to two fraudulent and unauthorized SWIFT transactions that were sent to Hong Kong. These transactions were also carried out using counterfeit cards, and were withdrawn from ATMs that are located in more than twenty different countries.

Post incident-reporting indicated that the network used for the bank's payment processing was not fully encrypted. As a result, attackers who gained access to the bank's networks were able to modify authorization responses to allow transactions that were supposed to be declined to be approved, all without being detected (Oleg Kolesnikov, n.d.). There are three main failings of responsibility: the encryption of the bank's payment network was patently the bank's responsibility, regardless of which hosting model was used, and was therefore incomplete; the network segmentation that was supposed to separate the core system from the switch was ineffective in containing the parallel switch; and the responsibility for detection was transferred to the external parties, Visa and RuPay, instead of the bank (VARINDIA, n.d.). The lesson to be learned from this incident is that security technology was present; the problem was that no single entity had unambiguously and verifiably taken the responsibility for monitoring that connection.

A similar pattern, from a structural standpoint, can be observed in the breach that occurred at City Union Bank in February 2018 (Hod Gavriel & Meir Brown, 2018). In this instance, attackers were able to use compromised SWIFT credentials to facilitate unauthorized remittances in the amount of approximately USD 2 million. SWIFT is a globally distributed network used for facilitated financial messaging; the bank interfaces with the SWIFT network in a manner that is not wholly controlled by the bank, and membership of SWIFT entails participating in a network with thousands of other banks. Also, in practical terms, the responsibility for detecting an atypical transaction resides wherever the monitoring of the bank is configured to be, which is an internal decision, and is not a guarantee of SWIFT itself. Like

© 2026 IJIRCCE | Volume 14, Issue 9, September 2026 DOI: 10.15680/IJIRCCE.2026.1409006

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Cosmos Bank, the technology to detect the transaction fraud was present in the operational ecosystem, the only requirement was a determination to monitor a high value link that was operated in conjunction with other banks.

VI. A PROGRAMMATIC APPROACH: MODELLING SHARED-RESPONSIBILITY RISK

Sections 2 and 5 suggest that ambiguities in ownership rather than absent technologies are driving recurrent risks. Here, I will convert that suggestion into a small tool and address a concern that the model raises autonomously: of what provenance are the numbers that the model quantifies?

6.1 The scoring model

Each security control is evaluated and scored along two dimensions: who owns the control (Provider, Bank, or Shared) and control maturity (on a scale of 0 for absence to 5 for full maturity and testing). Shared control scores residual risk:

residual_risk = ownership_weight(owner) x (5 - maturity)

The weighted value of 'Shared' controls is 1.6 (compared to the standard 1.0 for fully owned controls). The reason is that control(s) of which no one is unequivocally accountable for is/are likely to be unimplemented and/or neglected (this is also what the Cosmos Bank switch is/was about).

6.2 Where the maturity score comes from

A maturity score is not guesswork. It is a conversion from the documentation to a numeric value that is comparable and is determined by the team that is tasked with the control. The following two examples clarify the explanation above.

- Control for the patching of an ATM operating system was assigned a score of 1/5: the result of a VAPT for the first quarter of 2026 showed that 40% of the sample ATM set was found running an operating system that was unpatched for the last 18 months, the Vendor of the ATM system for their part showed no evidence of scheduling a patch for the last two quarters. The IT risk team assigned the control a low score using their internal scoring (5 = no findings and in compliance with SLA; 3 = delays in compliance; 1 = major findings and compliance issues, 0 = total absence).
- SWIFT / RTGS gateway monitoring, rating 2/5: monitoring tools are available, but the incident post-mortem noted that the fraud was detected by Visa and RuPay, and not by bank alerts - this shows that a tool exists but failed. Because of this, a low-better-than-zero score was warranted.

In both examples, the score is supported by a specific piece of evidence, a specific team, and a specific date - not written from memory. The tool below is created around this discipline.

6.3 From typed-in values to a CSV-driven assessment

The scoring logic is the same, but both the Python script and the browser dashboard are updated to read their data from a CSV file instead of hard-coded data, which is in line with the way the risk, audit, and VAPT teams keep this data. The required schema is in Table 2. A sample that is filled and a blank template are provided in separate files.

Layer	control	owner	maturity	evidence_source
Edge Device	ATM operating system patching	Shared	1	ATM vendor patch log - two quarters overdue
Core Network	SWIFT / RTGS gateway monitoring	Shared	2	Incident post-mortem - alert missed
Cloud (IaaS)	Physical data-centre security	Provider	5	CSP SOC 2 Type II report (2026)

Table 2. Required CSV schema (excerpt); full file also carries assessed_by and date_assessed columns.

The loader for Python scripts goes through direct validation and parsing of this file:

```
def load_assessments(csv_path):
    """Read and validate a control-assessment CSV exported by a risk team."""
    assessments = []
    with open(csv_path, newline="", encoding="utf-8") as f:
        reader = csv.DictReader(f)
        required = {"layer", "control", "owner", "maturity"}
        missing = required - set(reader.fieldnames or [])
```

© 2026 IJIRCCE | Volume 14, Issue 9, September 2026 DOI: 10.15680/IJIRCCE.2026.1409006

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

```
    if missing:
        sys.exit(f"CSV is missing required column(s): {', '.join(missing)}")
    for row_num, row in enumerate(reader, start=2):
        owner = row["owner"].strip()
        if owner not in OWNERSHIP_WEIGHT:
            sys.exit(f"Row {row_num}: owner '{owner}' must be Provider, Bank, or Shared")
        maturity = int(row["maturity"])
        assessments.append(ControlAssessment(
            layer=row["layer"].strip(), control=row["control"].strip(),
            owner=owner, maturity=maturity,
            evidence_source=row.get("evidence_source", "").strip(),
            assessed_by=row.get("assessed_by", "").strip(),
            date_assessed=row.get("date_assessed", "").strip(),
        ))
    return assessments
```

Figure 1 Core CSV loader from responsibility_risk_model.py (full script in the accompanying file).

The code will provide output as below

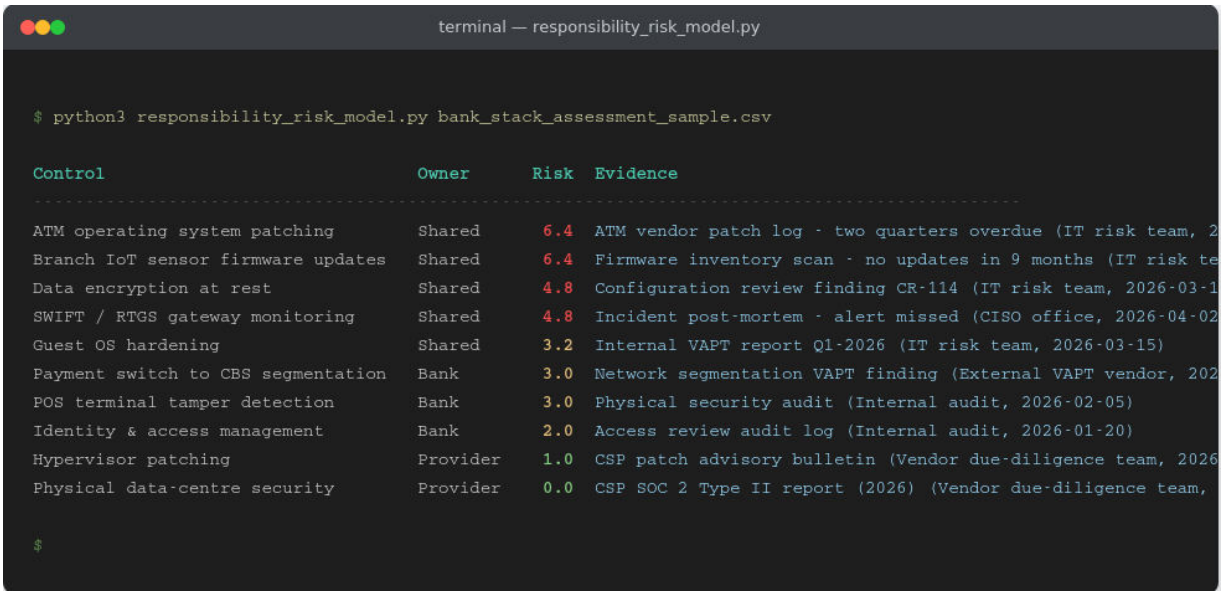


Figure 2 : Terminal output of responsibility risk mode run against bank stack assessment sample.csv

6.4 Output, ranked from the sample CSV

The script and the sample CSV produce the ranking, for which each score is substantiated with evidence, as seen below:

Control	Owner	Risk	Evidence
ATM operating system patching	Shared	6.4	Vendor patch log, 2 quarters overdue
Branch IoT firmware updates	Shared	6.4	Firmware scan, 9 months stale
Data encryption at rest	Shared	4.8	Config. review finding CR-114
SWIFT / RTGS gateway monitoring	Shared	4.8	Incident post-mortem
Physical data-centre security	Provider	0.0	CSP SOC 2 report (2026)

Table 2: Ranked residual risk from bank_stack_assessment_sample.csv (abridged; full ranking in the CSV output).

© 2026 IJIRCCE | Volume 14, Issue 9, September 2026 DOI: 10.15680/IJIRCCE.2026.1409006

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

6.5 The interactive dashboard

The same CSV can be uploaded to a web-based dashboard, giving a non-technical reviewer the ability to view the CSV without using a command line interface. A file picker reads the selected file and transfers its text to a small parser that splits the text into rows, and verifies the same four required columns as the Python script, to maintain a consistency between the two tools.

```
function loadFromCSV(text) {
  var rows = parseCSV(text);
  var header = rows[0].map(function (h) { return h.toLowerCase(); });
  ['layer','control','owner','maturity'].forEach(function (col) {
    if (header.indexOf(col) === -1) throw new Error('Missing column: ' + col);
  });
  // ...validate each row's owner and maturity, then return parsed objects
}
```

Figure 3 : Browser-side CSV validation from shared_responsibility_risk_simulator.html (full file in the accompanying download).

After the file is loaded, sliders and dropdowns allow the user to make the selection “what if this is Bank-owned” or “what if maturity improved to 3” and see the ranked bars update - an easy way to explain to a non-technical stakeholder why a control is important. Bars for “Shared” Controls have a diagonal stripe. This allows the paper’s visualization argument - the ambiguity of control ownership creates a danger signal - to be maintained. The sample data loaded is shown in the dashboard below in Figure 3.

Figure 4: The dashboard loaded with the sample assessment; striped bars denote “Shared” ownership.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

6.6 Scope and limits

Although this is still a heuristic model and not a risk engine, the real banks use NIST CSF or ISO 27001 aligned methodologies with continuously updated loss and audit data. The CSV driven version ("Level 1") is purposefully an intermediate step, as it does not live connect to any audit, VAPT or vendor system, but does require all scores be submitted along with named supporting evidence, to give a sense of the gap between "a number appears" and "a number becomes substantiated." A further step would read directly from a ticketing or GRC system; that is beyond this paper's scope but a natural extension.

VII. FINDINGS AND DISCUSSION

- With the Cosmos Bank switch, ambiguity was an issue, not the absence of technology: there was no identifiable ownership of its encryption and monitoring, and the technology was not lacking.
- The edge layer is the least standardized layer of the stack: organized and published cloud shared-responsibility documents are not matched with the documents for ATMs, POS, and IoT devices, whose documents depend on vendor contracts that are often undocumented.
- To evaluate is to substantiate: in the CSV schema, evidence_source, assessed_by, and date_assessed are not optional fields, they are the means to an appraisal and defend the assessment.
- Observably, Indian regulation has developed since 2018, but the development has not been consistent: the RBI's 2023–2024 directions have significantly developed since the post-Cosmos Bank guidance on outsourcing, cloud services, and IT and non-bank payments cyber-resilience, but the large commercial banks have been quicker to adhere to the guidance than the smaller commercial banks, meaning the compliance gap has significantly outpaced the regulatory gap.

This research paper used desktop studies, and for that reason, no primary data collection was done, and the example CSV used featured illustrative and not audited numbers. The only focus of this project was to describe and demonstrate a tool for the operationalization of shared-responsibility risks. The example used is not a valid assessment of an existing institution. The Level 1 tool described in Section 6 is, on purpose, only as good as the CSV provided to it. No assessments would be identified as missing, and instead the tool would only rank existing assessments. This describes clearly that a governance tool would take on the same gaps of accountability as the process that supports it. The following items show what can be done to help address the gaps of accountability.

VIII. RECOMMENDATIONS

8.1 For banks

- Every cloud workload and edge device vendor must have a clear responsibility matrix, and as changes in cloud vendors occur, the matrix must be reviewed.
- Internal assessments of risk must include cited evidence of the assessment and assessment of risk in the format of Table 2.
- Payment switch and SWIFT-adjacent systems must have end-to-end encryption and monitoring.
- Real incidents must include ownership questioning by external Managed Service Providers and Cloud Service Providers.

8.2 For regulators

- All other smaller and cooperative banks must adhere to the graded cybersecurity framework with validated enforcement deadlines.
- All edge computing devices must include a responsibility matrix in outsourcing contracts.
- Implement tagged evidence (source, assessor, date) in mandatory cyber-risk self-assessment submissions. Regulators would then be able to verify what evidence banks provide for cyber-risk self-assessment submissions instead of merely validating the scores provided.

8.3 For technologists and students

- Whenever something is "secure by design," make sure there is documented evidence of intentional design with "ownership by design." A security control will not be considered implemented until the condition has been satisfied, and a specific individual has documented evidence of their control and is responsible for maintaining the control.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IX. CONCLUSION

Digital banking security in India exists between the documented shared responsibility security model of the cloud and the more loosely defined security model of edge computing at branch locations, ATMs, and points of sale. Drawing from examples of the response from the RBI and the 2018 Cosmos Bank Incident, CIS has argued that the most severe gaps in security exist not from the absence of technology but the absence of the question, "who is accountable?" The CSV framework outlined here offers one of many possible ways to provide evidence for roles and responsibilities, making evident the risk associated with a lack of control ownership, and in ghost state, will elevate the issues of controls with the greatest risk vulnerability and least ownership the most. This is also the case for the Cosmos Bank incident, especially the lack control ownership and is the most urgent, most press.

REFERENCES

1. Colortokens. (2024, November 4). Cosmos Bank Cyber Fraud: Lessons in Cybersecurity for Banks.
2. Data Protection Laws of the World. (n.d.).
3. Gadde, S., Rao, G. S., Veesam, V. S., Yarlagadda, M., & Patibandla, R. S. M. L. (2023). Secure Data Sharing in Cloud Computing: A Comprehensive Survey of Two-Factor Authentication and Cryptographic Solutions. Ingénierie Des Systèmes d Information, 28(6), 1467–1477. https://doi.org/10.18280/isi.280604
4. gaotek. (n.d.). Applications of Edge Computing for IoT in the Finance and Insurance Industry [Information]. https://doi.org/https://gaotek.com/applications-of-edge-computing-for-iot-in-finance-and-insurance-industry/
5. Government of India. (2025, November 14). DPDP Rules, 2025 Notified A Citizen-Centric Framework for Privacy Protection and Responsible Data Use [Rules]. Government of India. https://doi.org/https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190655&reg=48&lang=2
6. Hod Gavriel, & Meir Brown. (2018, October 22). High Profile Cyber Attacks on Banks on the Rise. https://doi.org/https://www.cyberbit.com/endpoint-security/high-profile-cyber-attacks-on-banks-on-the-rise/
7. Humayun, M., Niazi, M., Almufareh, M. F., Jhanjhi, N. Z., Mahmood, S., & Alshayeb, M. (2022). Software-as-a-Service Security Challenges and Best Practices: A Multivocal Literature Review. Applied Sciences, 12(8), 3953. https://doi.org/10.3390/app12083953
8. Keshav Malik, & Aakanksha Khanna. (2026, January 22). RBI Cybersecurity Compliance Checklist for Banks & NBFCs in 2026.
9. Lambropoulos, G., Mitropoulos, S., & Douligeris, C. (2026). Emerging Technologies in Financial Services: From Virtualization and Cloud Infrastructures to Edge Computing Applications. Computers, 15(1), 41. https://doi.org/10.3390/computers15010041
10. marketing, team, SNUC, & January 15, 2025. (2025, January 15). Edge Computing in Financial Services: 21 Ways It Improves Efficiency and Security.
11. Oleg Kolesnikov. (n.d.). Cosmos Bank SWIFT/ATM US$13.5 Million Cyber Attack Detection Using Security Analytics. https://doi.org/https://www.securonix.com/blog/securonix-threat-research-cosmos-bank-swift-atm-us13-5-million-cyber-attack-detection-using-security-analytics/
12. RBI, C. G. M. (2016, June 2). Cyber Security Framework in Banks [Notice]. RBI.
13. Shared responsibility in the cloud—Microsoft Azure | Microsoft Learn. (n.d.). Microsoft Azure.
14. Shiv Kumar. (2018, August 15). Hackers siphon off Rs 94 crore from Pune bank via ATMs in 21 countries. https://doi.org/https://www.tribuneindia.com/news/archive/nation/hackers-siphon-off-rs-94-crore-from-pune-bank-via-atms-in-21-countries-637300
15. Thales. (n.d.). Data Security Compliance with Outsourcing of Information Technology Services Directions in India. https://doi.org/https://cpl.thalesgroup.com/compliance/apac/data-security-compliance-it-outsourcing-india
16. Understanding the Shared Responsibilities Model in Cloud Services. (n.d.).
17. VARINDIA. (n.d.). Learning from the COSMOS Bank Breach. https://doi.org/https://www.varindia.com/news/learning-from-the-cosmos-bank-breach

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details