BIKANER BRANCH OF CIRC OF ICAI

Members E-Newsletter DEC- 2025

Chairman Message

Dear All,

As I look back on the events organised by the Bikaner Branch of ICAI in December, I'm thrilled with the enthusiasm and participation of our members and students!

The CA Members Cricket Tournament was a resounding success, bringing together professionals for a fun-filled day of sports and camaraderie. Our seminars on Code of Ethics, Direct Taxes, and GSTR 9 were insightful, helping us stay updated and compliant. And the Mock Tests for CA Final, Intermediate, and Foundation students provided a valuable opportunity to assess preparation and fine-tune strategies.

These events underscore our commitment to continuous learning and professional growth. I'm grateful to everyone who participated and contributed to making December productive.

As we step into the New Year, we're excited to build on this momentum and bring more value to our members and students. We'll continue to focus on initiatives that enhance skills, foster networking, and support your professional journey. Stay tuned for more updates!

Warm regards,

CA Hetram Poonia

A Pragmatic Path to Strengthening Data Loss Prevention

Organizations often attempt to implement data loss prevention (DLP) through extensive upfront planning. Governance frameworks are drafted, ownership models are defined, and standard operating procedures are created long before any tangible benefit is delivered. While structure is important, this approach frequently results in slow progress, declining momentum, and reduced business confidence.

A more effective strategy is to deliver value early through focused implementation. Rather than attempting to perfect governance from the outset, organizations benefit from beginning with a limited, practical scope and allowing controls to mature through real operational experience. This approach supports continuous risk management while demonstrating relevance and impact at each stage.

Data protection remains a core element of cybersecurity regardless of the broader defensive model an organization adopts. A clear data security direction is therefore essential. The financial consequences of data breaches are substantial, reinforcing the need for prevention programs that extend beyond technology deployment. DLP should be treated as an integrated capability that combines people, processes, and systems to protect sensitive information, support regulatory compliance, preserve organizational reputation, and safeguard intellectual assets.

Framing DLP as an Organizational Responsibility

When DLP is positioned solely as a technical initiative, accountability tends to remain confined to IT or security teams. This framing limits business ownership and reduces long- term effectiveness. Instead, DLP must be communicated as a business-driven requirement, with risks articulated in terms that resonate with leadership—such as regulatory exposure, legal liability, and reputational impact.

Stakeholder engagement must be deliberate and proportionate. If responsibilities are unclear, key participants may be excluded. Conversely, excessive involvement—particularly in technical detail—can lead to disengagement. Effective DLP programs strike a balance by engaging the right stakeholders at defined points in the lifecycle.

Equally important is adopting a risk-based perspective on information protection. Treating all data with the same level of sensitivity increases complexity and cost without proportional benefit. Early data discovery and exposure analysis help ensure that investments and controls are guided by actual risk rather than assumptions.

Why DLP Programs Struggle to Deliver Results

Many DLP initiatives fail to achieve their intended outcomes. A recurring cause is the perception that DLP exists only to stop data leakage rather than to protect business processes and manage enterprise risk.

At a strategic level, insufficient involvement from business leadership weakens alignment. Programs driven exclusively by technical teams often lack the authority needed to influence operational behavior. Additionally, inadequate change management undermines adoption. Because DLP controls can affect how employees work, organizations must explain their purpose clearly and prepare users for changes in workflow.

Support during and after implementation is equally critical. Even well-planned controls may temporarily disrupt operations. If issues are not addressed quickly, confidence in the program erodes and sponsorship declines.

Process and Operational Weaknesses

The effectiveness of a DLP program becomes visible when policies are triggered. Without clearly defined operating procedures, alerts may be ignored, escalated inconsistently, or handled incorrectly.

Programs often falter when use cases are not clearly articulated or when data handling expectations are not documented. Without clarity on how information should be used and shared, alignment across teams becomes difficult. Similarly, failure to understand how data moves through the organization limits the ability to design enforceable and meaningful controls.

DLP policies must also evolve. Business processes, regulatory expectations, and technology environments change continuously. Controls that are not reviewed and updated lose relevance and effectiveness over time.

Technology Limitations and Design Risks

The technical layer of a DLP program is critical but frequently misunderstood. Poor integration between components increases administrative effort and reduces visibility, leaving gaps in monitoring. Solutions must operate cohesively across endpoints, networks, and storage environments to provide meaningful coverage.

Overly restrictive policies introduce another risk. Excessive false positives overwhelm users and administrators, reduce confidence in alerts, and can disrupt legitimate business activity. Technical controls must balance enforcement with usability.

Encrypted data presents an additional challenge. Without appropriate inspection capability, certain data movements may remain invisible. At the same time, inspection methods must be carefully selected to avoid disrupting applications or services.

Detection methods based solely on static pattern matching are also limited. Similar data formats and simple obfuscation techniques can bypass controls. More advanced approaches that incorporate contextual analysis and learning mechanisms improve accuracy and reduce noise.

Technology selection must align with the organization's broader architecture. Deployment models, integration requirements, and compatibility with existing platforms should guide decision-making rather than isolated feature comparisons.

The Role of People and Partners

Human behavior remains a significant factor in data exposure. Without consistent education and awareness, users may inadvertently violate policies. DLP programs must therefore include ongoing training that reinforces expectations, explains controls, and supports correct behavior.

External partners also influence program success. Vendors and service providers should be evaluated not only for technical capability but also for strategic alignment. Clear service expectations, measurable outcomes, and exit provisions reduce long-term dependency risks. Advisory support should remain independent from technology sales to preserve objectivity.

Establishing a Practical Operating Structure

An effective DLP capability rests on visible management support. Because controls can affect multiple business functions, leadership endorsement is necessary to align expectations around effort, resources, and change.

Sustained operation depends on four foundational elements:

- Business participation ensures that controls reflect real workflows and that accountability is clear.
- Data classification establishes a shared understanding of sensitivity and handling requirements, with simplicity preferred to avoid unnecessary complexity.
- Analysis of data movement highlights exposure points and informs policy design.
- Defined response procedures ensure that alerts lead to consistent and proportionate action.

Trust in both the program and the supporting technology is essential. Without it, stakeholders may view DLP as disruptive rather than protective.

Iterative Execution and Continuous Improvement

DLP should operate as a cycle rather than a one-time deployment. Discovery activities identify where sensitive data resides across systems and platforms. Detection rules must be tested, validated, and refined to control false positives and maintain credibility.

Policy management requires ongoing adjustment to reflect legitimate business needs. When controls interrupt operations, rapid support and clear communication are essential to preserve confidence.

Change management and training must be continuous. Awareness initiatives, role-specific instruction, and accessible guidance help ensure that users understand expectations and responsibilities.

Ongoing monitoring allows organizations to assess effectiveness, identify gaps, and validate controls through testing and review. Adjustments should be made systematically rather than reactively.

Managing Risk through Controlled Expansion

Attempting to deploy DLP across the entire organization at once often generates excessive alerts and administrative burden. A phased approach—starting with a limited scope and expanding gradually—allows controls and response processes to mature before wider rollout. This approach reduces disruption and improves precision.

Defining use cases early also supports focus. Clear success criteria and validation steps help ensure that controls deliver measurable outcomes aligned with organizational priorities.

Conclusion

Implementing data loss prevention requires sustained investment and careful execution. While structure is necessary, progress depends on delivering value early, learning from experience, and refining controls in practical settings.

By starting with a manageable scope, aligning stakeholders, and allowing governance to evolve alongside real-world application, organizations improve their chances of maintaining momentum and achieving the core objective of DLP: protecting critical information in a way that supports, rather than hinders, business operations.

CA. Yogesh K. Jangid
CA., B.Com, LL.B, LL.M, PGDBCL, CISA
C-CCA, C-FAFD, C-Public Fin & Govt. Accounting, CGEIT(US), CFE(US), CPA (Aus)

Photo Gallery

CA Members Cricket Tournament

Mock Test for Jan-2026

Disclaimer: The views and opinions expressed or implied in this E-Newsletter are those of the authors and do not necessarily reflect those of Branch or CIRC or ICAI.

Editorial Board:

CA. Hetram Poonia
Editor in Chief
: - *8104844331*
: *cahetrampoonia@gmail.com*

Members	
CA Abhay Sharma	Co-Editor
CA Mukesh Sharma	Member
CA Sumit Nowlakha	Member
CA Rajesh Bhoora	Member
CA Mohit Baid	Member
CA Satish Gupta	Ex-Officio

Bikaner Branch of CIRC of ICAI

'ICAI BHAWAN' C-6-7-8, SHIV VALLEY, GANGA SHAHAR ROAD, BIKANER-334001