The essential guide to Digital Communications Governance & Archiving

Alex de Lucena
Product Strategy Director
Shield

Michele Torti
EMEA Sales Director
LeapXpert

shield. | LEAP XPERT

In this handbook

3 Introduction

4 — 8 Part 1: DCGA Demystified

9 — 12 Part 2: The Drivers of DCGA

13 — 15 Part 3: Taming the Communications Chaos

16 — 22 Part 4: Implementation Considerations

22 — 25 Part 5: The Differentiators

26 — 28 Part 6: The Future of DCGA

29 — 31 Conclusion

Introduction

So, what's Digital Communications Governance & Archiving anyway?

As the landscape of digital communications continues to evolve, Gartner® has recently recognized the escalating intricacy of communication tools, and the need to govern their use, by retiring the category of Enterprise Information Archiving and replacing it with "Digital Communications Governance & Archiving."

Since then, DCGA has been popping up everywhere–but what does it really mean? We're here to break down the details behind the acronym.

Broadly, DCGA refers to a set of tools and practices that organizations use to manage, monitor, regulate, and store employee communications across various digital channels.

But even that broad description covers a lot of ground and leaves experts wondering: How does this impact me?

With guidance from specialists at Shield and LeapXpert, this eBook will help you understand the importance of DCGA, and how you can unlock the power of intelligent communications surveillance while safeguarding your organization's data and reputation.

Part 1: DCGA Demystified

Understanding Digital Communications Governance & Archiving

As more of life takes place on WhatsApp and the like, so does business.

This shift means that regulated industries, including financial institutions, must ensure their staff can communicate via apps and other digital channels while capturing these records for regulatory reporting.

But unlike Enterprise Information Archiving, a traditional category that was focused on financial institutions and their need to archive and access information for compliance purposes, DCGA holds a broad mandate and promise. And it goes well beyond regulations. Essentially, any enterprise wishing to govern and retain critical information exchanged over digital channels is now looking – or will soon be on the market – for effective DCGA solutions.

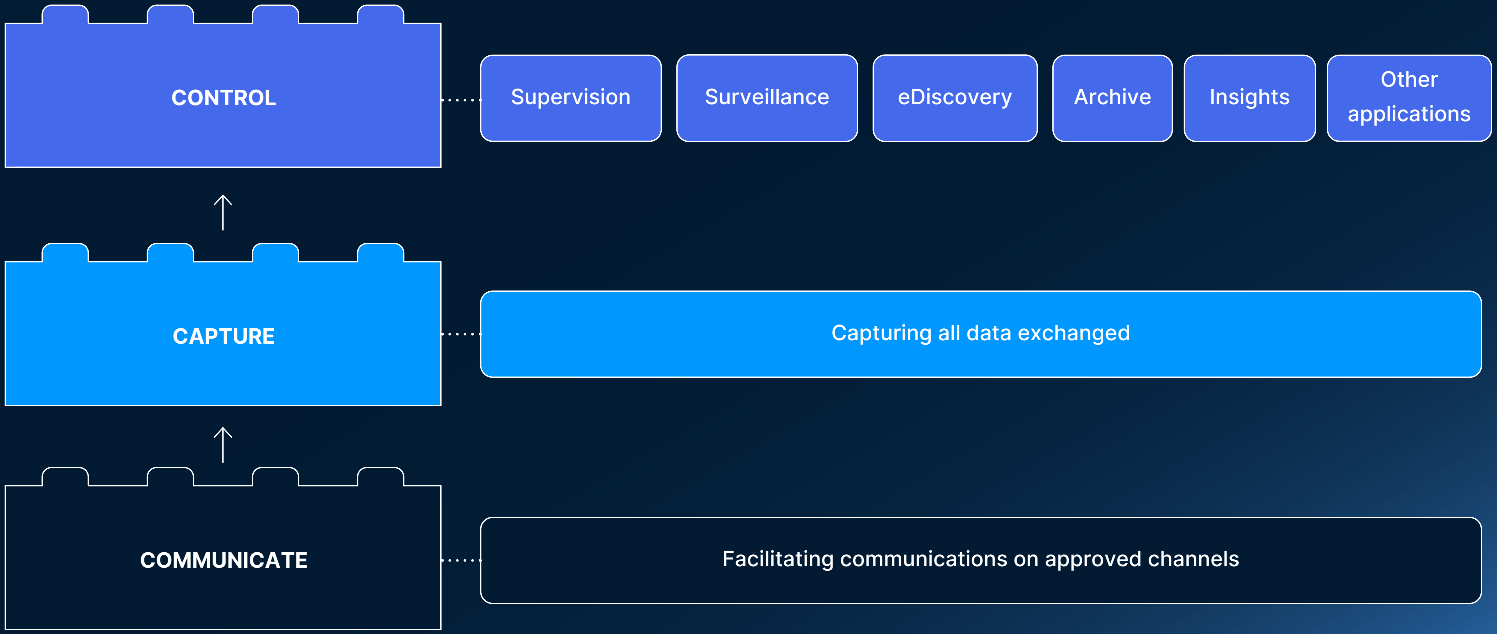
Although the trends were evident long before the Covid-19 pandemic, the rise of remote working arrangements require an expansion of monitoring capabilities beyond the traditional channels of voice and email. With approximately 2.4 billion monthly active users of WhatsApp, 800 billion of Telegram, 1.3 billion WeChat, and over a billion people using Apple's iMessage, there's a clear trend towards messaging as the primary mode of business communication, relegating email and phone calls to secondary status.

Today, businesses must consider how to capture and analyze a much broader array of channels, and how to piece conversations together that may span instant messaging, social media, video conferencing, and other digital platforms in the context of an executed trade. They cannot afford to lose control over the critical business information shared over these channels. And so, DCGA solutions ensure that these communications are secure, compliant with relevant regulations, and fully governed so that they are aligned with an organization's internal policies and interests.

WHATSAPP	TELEGRAM	WECHAT	iMESSAGE
2.4 billion	800 billion	1.3 billion	+ 1 billion

MONTHLY ACTIVE USERS

The Building Blocks: Communicate, capture, control



CONTROL

Supervision

Surveillance

eDiscovery

Archive

Insights

Other applications

CAPTURE

Capturing all data exchanged

COMMUNICATE

Facilitating communications on approved channels

Climbing the corporate agenda

“DCGA represents a mindset shift in how we think about communication assets,” says Alex de Lucena, director of product strategy at Shield. “The concept has been driven by Gartner, who was previously less invested in surveillance, but has now observed a real change in mood across the market. Now, eComms are viewed as assets in and of themselves.”

“Businesses have been forced to acknowledge communication preference changes happening in the wider world, and how they impact operations,” Michele Torti, EMEA sales director at LeapXpert says. “The current generation of enterprise employees and their customers are native in mobile phones, and those attitudes have permeated regulated industries, too.”

Torti explains, “DCGA is crucial for understanding your strategic position. How does a business address DCGA? You obviously cannot ban mobile phones entirely, right? So what’s left is a combination of implementing policies to manage their use, and leveraging technology to maximize their potential and derive the greatest value.”

Innovative businesses are increasingly adopting a comprehensive approach that begins with enabling communications and capturing them on channels such as WhatsApp and iMessage, as well as email, social media, MS Teams, and Zoom, followed by robust surveilling and archiving.

Surveillance teams now have the ability to move beyond the capturing and alerting approach to active monitoring. They can create a DCGA framework using advanced machine learning tools that can add contextual analysis to enormous archives of communication data, gain previously hidden insights, and better protect their business from risk.

Part 2: The Drivers of DCGA

Navigating regulatory waters

How traders communicate has changed dramatically over the last decade, and whilst societal and generational shifts have had an impact in the way business is done, regulatory requirements have also evolved in lockstep.

Various guidelines around the world require regulated firms to monitor and record communications in order to maintain market integrity and protect investors.

Sanctions for record-keeping lapses have ballooned in recent years, with some Wall Street banks landing penalties of $200 million for lax supervision of staff who used WhatsApp and other chat apps to discuss investments.

Data protection laws around the world have also complicated the picture, and forced businesses to review the way they process and store sensitive information. Security concerns stemming from data breaches and hacks are growing, which also opens communications channels to abuse from bad actors.

Here are some of the most notable regulatory requirements related to record-keeping and communications monitoring:

Markets in Financial Instruments Directive II (MiFID II)
Requires the recording of telephone conversations and electronic communications for 5-7 years that relate to the reception, transmission, and execution of orders.

Dodd-Frank Wall Street Reform and Consumer Protection Act
Requires the recording of oral communications that result in the execution of commodity interests and swaps.

Financial Conduct Authority (FCA) rules
Although no longer part of the European Union, the UK has broad crossover with MiFID II record-keeping requirements.

Securities and Exchange Commission (SEC) rules
Various, including Rule 17a-4, which requires broker-dealers to retain communications, including emails, instant messages, and other electronic communications.

Hong Kong Securities and Futures Commission (SFC) Code of Conduct
Requires the retention of records of all transactions, including related communications, for a minimum of 7 years.

Financial Industry Regulatory Authority (FINRA) Rule 3110
Requires member firms to establish and maintain a system to supervise the activities of their associated persons, including the review and retention of electronic communications.

Australian Securities and Investments Commission (ASIC) rules
ASIC requires firms to maintain records of financial services provided, including relevant communications, for at least 7 years.

The genie is out of the bottle

“In the past three years, a whopping 3 billion dollars worth of fines have underscored the serious nature of regulatory pressure,” says Torti. “This should come as no surprise. Financial institutions must acknowledge and address this reality.”

Regulators expect robust policies or technologies to capture, monitor, and archive all communications, regardless of the channel used. This is not a technicality; governing digital communications enables both internal and external audits, which goes to the core of fairness and accountability in the financial system.

These regulatory drivers have heightened the need for a robust DCGA strategy, and have led businesses to explore ways in which AI can be leveraged to assist communications surveillance and strengthen compliance.

“AI-backed DCGA solutions allow banks to gain insights from large, unwieldy and disparate archived communications”, de Lucena says, which is a generational leap from the previous iteration of surveillance tools which were primarily alert driven and trained to look for keywords.

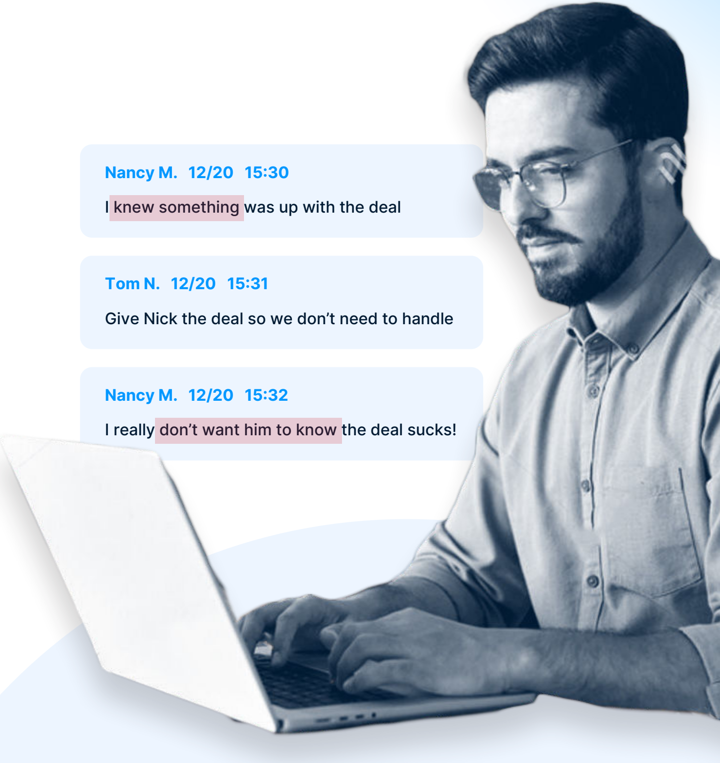
“We can contextualize within the communication, meaning digital communication becomes a broader asset for the business, and DCGA can significantly enhance risk management processes,” de Lucena goes on.

By meticulously adhering to record-keeping regulations, organizations can turn what might seem like mundane communication records into valuable assets.

These records not only meet legal requirements but also provide critical insights and data that support decision-making, enhance transparency, and protect the organization in legal or compliance reviews.

This communications data, when properly managed and analyzed, can reveal trends and patterns, offer evidence in case of disputes, and provide a rich source of information for strategic planning.

A proactive approach to regulatory compliance can transform communication records into a valuable repository of knowledge and evidence.



Nancy M. 12/20 15:30

I knew something was up with the deal

Tom N. 12/20 15:31

Give Nick the deal so we don’t need to handle

Nancy M. 12/20 15:32

I really don’t want him to know the deal sucks!

Part 3: Taming the Communications Chaos

DCGA challenges and complexities

As businesses integrate more communication channels, the complexity of managing these channels increases exponentially. Traditional methods of capturing and monitoring are no longer sufficient, given the diversity and volume of digital interactions, and the amounts of data generated.

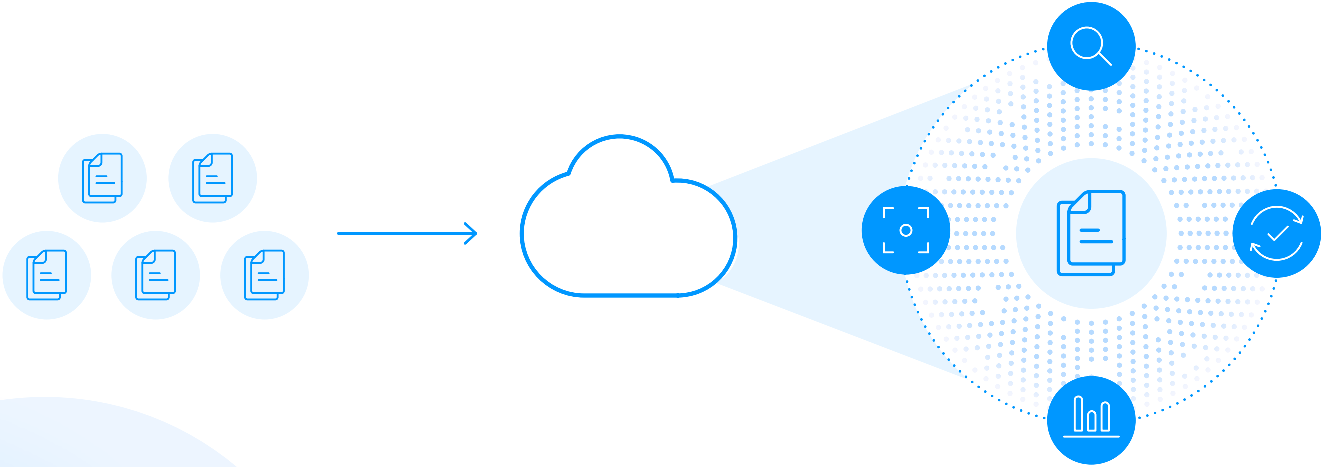
Historically, much of this data was housed on-premises, but more and more large businesses are turning to the cloud, and tapping vendors to help manage the implementation and put in place systems that allow for detailed analysis of the data.

"The introduction of more channels into play increases volume and adds complexity, but this is where AI can help and is having a massive impact" says de Lucena. "Vendors can provide solutions that make the organization's relationship with data more holistic and alert driven."

The role of AI and machine learning

Moving archived data to the cloud allows for faster, streamlined applications of machine learning algorithms which can uncover valuable insights for the business, and identify a much broader range of compliance issues with greater efficiency.

These advances in AI introduce the aspect of governance, prompting the C-suite and boards to create a strategy that will extract maximum value and business intelligence from the analytics.



Holistic data management

"In the past, the focus on communications data was simply on books, records, and archiving," says de Lucena. "Now there is a much bigger umbrella, along with the idea of bringing all that data together."

Modern business environments demand a holistic approach to communications data, and the integration of diverse communication channels. Effective surveillance solutions must capture and integrate data from these platforms seamlessly, ensuring compliance without disrupting the user experience.

"Flexibility is key, especially if staff prefer using native applications like WhatsApp or iMessage," says Torti. "Remember, compliance tools are only effective if they are fully adopted by employees. So businesses need platforms that allow compliant use of these apps without disrupting the user experience."

Integrating these communications into a unified platform, such as MS Teams, allows employees to maintain their real-life communication habits while adhering to compliance requirements. This underlines how evolving consumer experiences can significantly impact business operations. Comprehensive integration ensures businesses can track and manage all interactions within a familiar platform, supporting both compliance and operational efficiency.

Additionally, providing a centralized repository for this data is essential. Organizations need robust solutions to store and manage communications data, ensuring they remain compliant with standard monitoring requirements. This capability is particularly critical for large and complex organizations striving to maintain regulatory compliance and operational transparency.

Part 4: Implementation Considerations

Key considerations for DCGA implementation

Businesses creating a DCGA framework generally have 3 major challenges to address from the outset:

- **The complexity and diversity of communication channels.**
- **The importance of centralized data storage for effective DCGA.**
- **Overcoming traditional risk aversion and embracing new technologies.**

"Organizations are evaluating which communication channels are most important based on factors like client location—WhatsApp in Europe, WeChat in China, and so on," says Torti. "Senior management must first determine that a specific channel is necessary for the team to perform more efficiently. Once that decision is made, the discussion then often involves IT and compliance teams."

"The options have become so vast and complex, but these channels are what everyone is using," says de Lucena. "There's no sense that we will go backwards, so it becomes about how to stay current whilst addressing the complexity."

The consolidation game

“To effectively manage this complexity, organizations need to consolidate their communication data into a single, centralized system,” says de Lucena. This approach enhances the ability to monitor and analyze all interactions, ensuring comprehensive compliance and risk management at policy level.

“We are seeing digital transformation teams inside banks really thinking about having all the data in one place and how that can help DCGA,” de Lucena says. “It’s been influenced by the broad shift to the cloud, and how businesses have become comfortable with it. Consolidating artifacts gives you a view across everything, and there are major advantages to pooling the data in such a way.”

Centralization allows for better oversight, easier access to records, and more efficient regulatory reporting. It also supports the growing trend of digital transformation and the shift to cloud-based solutions as part of a robust DCGA strategy.

Overcoming traditional mindsets

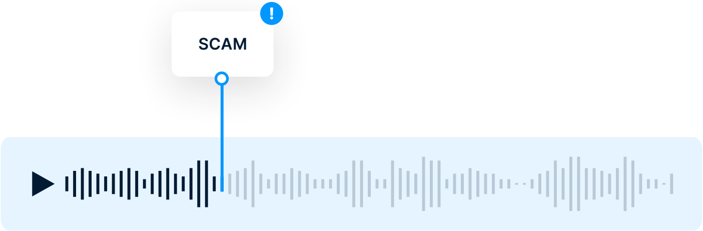
Some firms still adhere to traditional methods, storing communications data across both on-premise systems and the cloud. However, this risk-averse mindset is gradually fading as businesses recognize the benefits of fully embracing digital transformation, Torti adds.

"The scalability isn't the issue," he explains. "The problem is the complexity and the ability to manage that. How do you capture all the channels and have evidence of capture? Until recently, banks had in-house tech teams working on these issues, and whilst they are supposed to let you know if something is missing, perhaps you don't have as much insight as you thought you did, or would have with AI."

Leveraging real-time insights

The ability to provide real-time insights is a significant advantage for firms building out DCGA. Real-time data allows compliance teams to replay messages, drill down into details, and identify missing information quickly, making their work more effective and efficient.

"This is where the ability to play around really frees up the compliance team and makes their work more effective," de Lucena says. **"They can replay messages, drill down and really understand what information is missing, and why it is missing."**



Implementing DCGA: Challenges and strategic importance

Transitioning from scattergun surveillance to DCGA can be a complex process, and businesses, particularly larger and more complex organizations, often encounter significant challenges to smooth implementation.

Making the jump

"One of the primary hurdles we see is businesses grappling with the capture of mobile communications for the first time," Torti explains. "They frequently face a steep learning curve as they move from traditional methods to more sophisticated solutions."

Businesses must not only adopt new technologies but also ensure that their employees, especially traders, adapt quickly to these systems.

"It's not just about replacing existing solutions but also about managing the transition for users accustomed to older methods," de Lucena adds.

Keeping up with the change

Another significant challenge is the relentless pace of technological change.

"Communication channels are evolving at an unprecedented rate," Torti says. "Businesses need solutions that can quickly integrate new platforms and technologies to stay ahead."

This constant evolution necessitates a flexible approach, enabling organizations to adapt without major disruptions.

"It's about having a system that is not only robust but also agile enough to incorporate new forms of communication as they emerge,"
says Michele Torti.

Bringing it all together

The rationale behind centralizing DCGA is rooted in the fragmented nature of modern communication. Conversations occur across a multitude of platforms, from emails and phone calls to various mobile apps and social media channels. Robust platforms must be able to capture everything and piece it together to replicate the story of the trade when necessary.

"When communication is scattered across different platforms, it creates silos of information," de Lucena explains. "A centralized approach breaks down these silos and enables businesses to view the entire communication landscape."

By capturing and integrating all communication channels into a single platform, businesses can maintain a cohesive compliance strategy with enhanced data management capabilities.

"A centralized system provides comprehensive visibility," Torti says. "This holistic view is crucial for monitoring and compliance, as it ensures that no communication falls through the cracks.

When all the data is aggregated into one system, it becomes easier to analyze patterns, identify risks, and make informed decisions. This level of insight is only possible with an integrated approach."

Strategic outcomes

Robust DCGA more than just enhances compliance; it is a strategic asset that can transform how businesses operate.

"Ultimately, it's about creating a unified communication environment," de Lucena concludes. "One that is secure, compliant, and capable of adapting to the ever-changing technological landscape."

Part 5: The Differentiators

Key elements for success

A strong DGCA framework hinges on extensive coverage across all communication channels.

Limiting the ways in which employees can chat often increases the risk of employees using unapproved and non-governed channels. In the financial sector this is known as 'off-channel communications' In general, this is part of a broader issue known as 'shadow IT,' the use of tech tools by employees outside the approved and governed systems of the enterprise.

And so, comprehensive coverage is essential to ensure all communication remains within the scope of surveillance and compliance.

Roll with the changes

Flexibility in DCGA ensures that enterprise employees can use their preferred communication tools without compromising on compliance. The use of native chat applications on corporate devices is growing in popularity as availability broadens, giving monitored employees more choice, and fewer incentives to dodge the proper recorded channels.

Successful implementation with platforms like MS Teams can allow businesses to maintain seamless communication across various channels without losing oversight.

“You can use the native chat application with a corporate phone and have the ability to record,” Torti concludes. “This versatility allows traders, for example, to switch between channels without losing surveillance coverage, which is crucial from a compliance standpoint.”

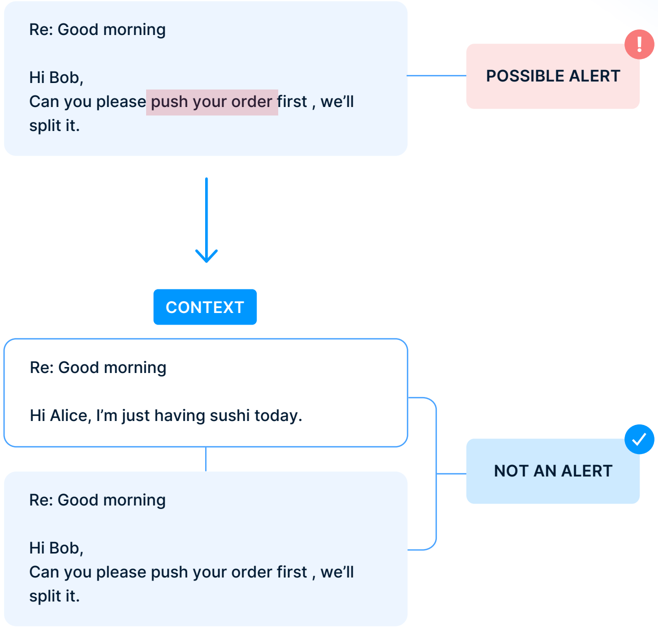
Enter the machines

The success of a DCGA framework depends on comprehensive coverage, flexibility, seamless integration, and the intelligent use of AI.

“How much data a firm is willing to allow risk management teams to validate the logic is enormously important,” says de Lucena. “AI can revolutionize the way a business gains from data analysis within DCGA.”

One significant advantage AI-powered surveillance platforms have over the previous generation of tools is the ability of models to understand context. This can help identify a much wider range of potential issues long before they crystallize into business threats.

“Modern AI models work in a generalized way, drawing a circle around instances of misconduct and accounting for variables more effectively,” says de Lucena. “This means identifying overlapping signals and filtering out noise, thus providing a more accurate and comprehensive understanding of communication patterns.”



Re: Good morning

Hi Bob,
Can you please push your order first , we’ll split it.

Re: Good morning

Hi Alice, I’m just having sushi today.

Re: Good morning

Hi Bob,
Can you please push your order first , we’ll split it.

Best use cases for AI within DCGA

AI significantly enhances the ability of a compliance function to manage and analyze large volumes of communications data. Advanced models reduce false positives and negatives, providing more precise identification of potential compliance breaches and saving staff crucial time.

Here are some of the main uses cases for AI when building out a DCGA framework:

Utilizing AI to contextualize communications can help the system understand nuances of conversations, **identifying risks more accurately.** “AI can differentiate between benign and potentially harmful interactions, which improves the overall accuracy,” says de Lucena.

Effective data governance requires managing the volume of data AI systems analyze by setting clear guidelines on data usage, storage, and validation. These practices build a solid foundation for AI operations within the DCGA framework.

Risk management can be significantly enhanced when AI is used to validate the logic and patterns it identifies.

“This proactive risk management strategy helps in the early detection and mitigation of potential compliance issues,” adds Torti. “It gives confidence that a business can spot risks before they develop into more significant threats.”

Implementing AI models that continuously learn and adapt to new communication trends and patterns ensures the system remains relevant and effective over time.

“As, as communication channels and behaviors evolve, **flexibility allows AI to continue accurately identifying and addressing emerging compliance risks**,” says de Lucena.

Part 6: The Future of DCGA

Evolving trends

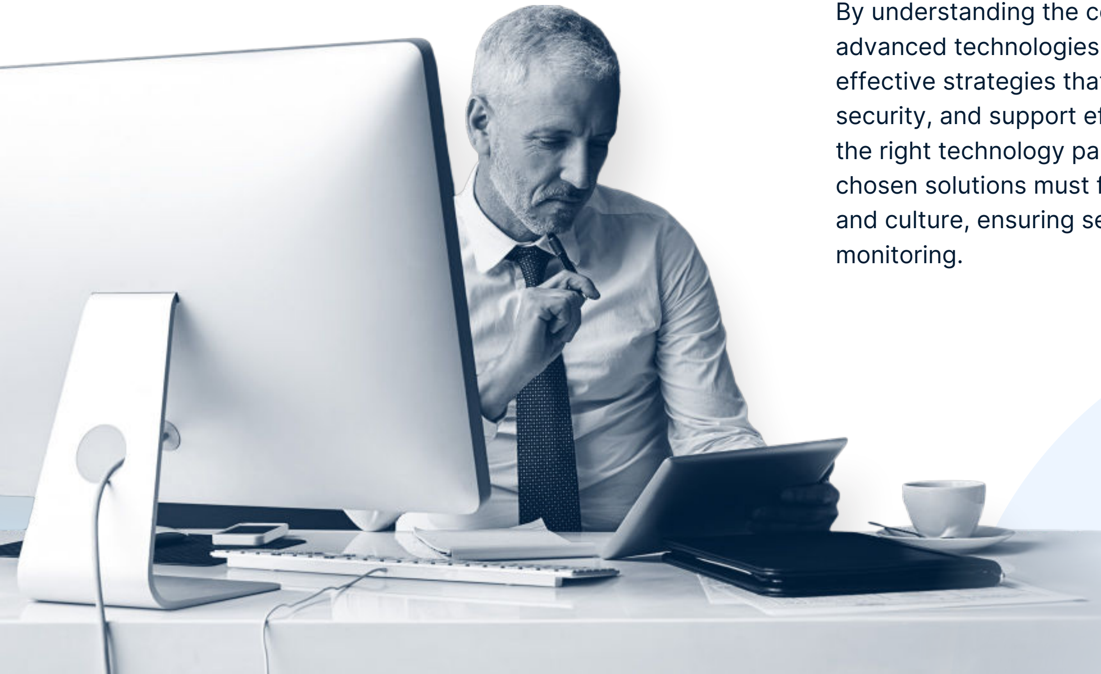
As the DCGA agenda continues to turn heads inside the boardroom, solutions providers are already mulling the next set of challenges to overcome. The landscape of communication technology is constantly evolving as are trader behaviors, and the efficacy of DCGA solutions must move with both.

“While AI-driven tools have significantly enhanced compliance monitoring, there’s a looming question: Are we adequately prepared for the shift towards channels predominant in our private lives?” says Torti. “We need to ensure that the technology we create becomes more helpful in that regard, reproducing communications with the same level of security and control that banks once applied to emails.”

As personal and professional realms continue to intertwine, the resilience of DCGA frameworks to adapt to as-yet-unknown future changes is paramount.

Managing the pace of change

The fast-evolving landscape of communications channels also requires DCGA solutions that are adaptable and future-proof. Businesses must be ready to onboard new channels as they emerge, maintaining compliance and operational efficiency.



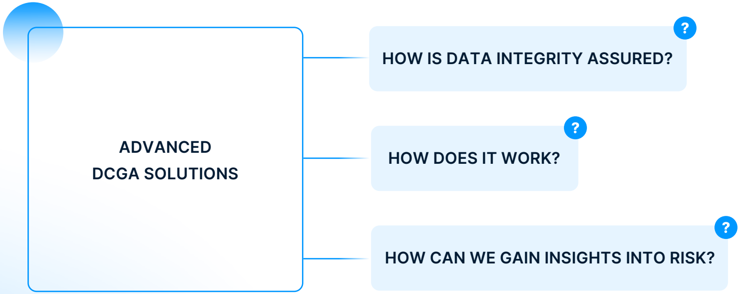
"In a few years, today's popular channels might be replaced. It's vital to have a solution that is future-proof in the sense that it can follow these changes and quickly onboard new channels," Torti explains.

By understanding the complexities of DCGA and leveraging advanced technologies, organizations can implement effective strategies that ensure compliance, enhance security, and support efficient business operations. Selecting the right technology partner is crucial for success. The chosen solutions must fit the organization's specific needs and culture, ensuring seamless integration and effective monitoring.

Streamlined DCGA

The ability to consolidate tools must also enhance the level of control and compliance across all communication channels. Advanced DCGA solutions are built on robust controls and the ability to facilitate detailed trade reconstruction.

“Nobody wants to open 10 applications at the same time,” says Torti. “Enterprises are demanding more controls at all levels, seeking consolidation. They see the potential in solutions that raise the bar in this area for controls and trade reconstruction.”



ADVANCED DCGA SOLUTIONS
HOW IS DATA INTEGRITY ASSURED?
HOW DOES IT WORK?
HOW CAN WE GAIN INSIGHTS INTO RISK?

Agreeing, de Lucena says the advocates of a unified DCGA stategy will find themselves busy showcasing the capabilities of these advanced systems to senior stakeholders in the business.

“Presenting the entire stack in one place can be mind-blowing, sparking curiosity and a desire to learn more,” he says. “Businesses want to understand how it works, how data integrity is assured, and how they can gain insights into risk. It’s an exciting frontier to explore.”

In the pursuit of streamlined DCGA, organizations need solutions that consolidate tools and provide comprehensive controls and insights. By centralizing communication management and compliance functions, firms can enhance their ability to navigate the complexities of modern communication while maintaining regulatory compliance and data integrity.

Conclusion

A robust Digital Communications Governance & Archiving framework is essential to modern compliance operations. As finance and communications undergo rapid digitalization, the function faces challenges in harnessing the power of rising volumes of data generated. In the flood of communications chatter, red flags can be obscured, making regulatory adherence difficult.

The transformative potential of leveraging AI inside a DCGA framework promises to help businesses go further than simply tackling these challenges, but to find new insights within.

"DCGA has transcended mere archival compliance," says Torti. "It's about harnessing cutting-edge technology to integrate modern communication channels into the enterprise realm, ensuring their proper management and utilization."

This means capturing, retaining, and governing all exchanged data, ultimately minimizing risk and optimizing the benefits of responsible communication practices.

"Organizations that are innovative and forward-thinking when it comes to DCGA are best placed to position themselves for success," concludes de Lucena. "Investing in a comprehensive DCGA framework powered by AI can transform compliance into a valuable strategic partner to the business."

About Michele Torti

As EMEA Sales Director, Michele leads the expansion LeapXpert across EMEA through direct sales, partnerships and alliances. He is a SaaS expert with 13 years of experience helping Financial Services firms solve Regulatory and Compliance problems.

Prior to joining LeapXpert, Michele led the EMEA Team of Relativity Trace. Before that he was responsible for sales of Bloomberg Vault and spent 3 years at HP/Autonomy. Michele has a legal background and is a solicitor and a qualified lawyer in Italy.

About LeapXpert

LeapXpert, the responsible business communication pioneer, provides enterprises peace of mind through compliant and secure communication solutions. The LeapXpert Communications Platform enables compliant, governed, and secure communication between enterprise employees and their clients across consumer messaging and voice channels, while leveraging Communication Intelligence to enhance front-office employee productivity and decision-making. LeapXpert, a Gartner Cool Vendor, is headquartered in New York, with offices in London, Tel Aviv, and Asia. Hundreds of enterprise customers, with hundreds of thousands of users in more than 45 countries, depend on LeapXpert daily for Digital Communications Governance & Archiving (DCGA). For more information, visit www.leapxpert.com.

About Alex de Lucena

Alex de Lucena is Director of Product Strategy at Shield where he oversees development of competitive capabilities and aligned business growth. Prior to Shield, Alex worked for 15 years in communications surveillance, starting as a reviewer and ultimately heading a global comms surveillance program.

He has deep experience in the building of effective compliance programs with a focus on AI, voice and user efficiencies. Alex has a passion for detection and how behavior manifests across language.

About Shield.

Shield enables compliance teams in financial services and other highly regulated industries to read between the lines to see what their employee communications are really saying. Many of these organizations struggle with compliance because they are unable to gain visibility into the mass of scattered data across all of their communication channels to mitigate against market abuse, internal bad actors and increasing regulatory risk.

Powered by generative AI and large language models, Shield is the industry's only native full-circle platform, enabling proactive monitoring of digital communications, streamlining compliance workflows, and reducing false positives by 97%. Trusted by the world's largest financial institutions, Shield delivers unparalleled data control, security, and efficiency in adherence to regulations. Learn more at shieldfc.com.