Hear first about SASIG events and industry news
Follow us on:

# Financial Services SASIG

## In association with

We're extremely grateful to be returning to Standard Chartered to continue the Financial Services resilience conversation. As a regulated industry, the financial sector is subject to far more scrutiny than others, both from regulators and from cyber threat actors. As with all sectors though, assuring a secure ecosystem relies on cooperation, collaboration and mutual understanding of the threats and risks. Well-delivered client and third-party security, coupled with risk-based exposure management can help organisations strengthen operational resilience, improve incident readiness and meet regulatory expectations.

This event looks at effective leadership and teamwork in high-pressure environments, and the growing governance and financial challenges created by autonomous AI agents, especially in light of legislation such as ECCTA (fraud regulations) and CSRB.  A day not to be missed.

**Thursday 26 November 2026**

**9am to 4pm**

**London**

# Chair

**Liz Murray**
Chief of Staff, The SASIG

---

**9.00am** **Registration, coffee, and networking**

---

**9.30am** **Welcome and introductions**
**Benedict Peet** UK/Europe CISO, Standard Chartered Bank

**9.45am** **Information and cybersecurity in Standard Chartered Bank: The CISO view in a rapidly changing environment including our client and third-party security capabilities**
**Benedict Peet** UK/Europe CISO, Standard Chartered Bank

**The evolving cyber security landscape**
Building on the 2025 Financial Services SASIG, join Ben Peet, ICS UK/Europe CISO, for an insight into Standard Chartered Bank's information and cyber security operations. The session will examine the significant challenges facing this UK-based FTSE 100 international bank - an organisation whose global scale may surprise many.

Ben will also explore the Bank's rapidly evolving client and third-party security capabilities, including how collaboration in both "peacetime" and "wartime" can strengthen relationships, and build trust with clients and third parties.

**10.15am** **Client & third-party security**
**Benedict Peet** UK/Europe CISO, Standard Chartered Bank

Over recent years, regulators have focussed on how the financial sector ensures that client money and data is secure, coupled with tightening the requirements for the overview that must be maintained of third-party providers to banks and building societies. This session will look at how both can be achieved and what needs to be in place to meet regulatory and legal requirements.

**10.45am** **From blind spots to action: Risk-based exposure management for financial services**
**Greg Baylis** Director Account Executive, Qualys

Financial institutions face a unique bind: stringent regulatory obligations on one side, and an ever-expanding attack surface across cloud, third-party, and legacy infrastructure on the other. Traditional vulnerability management with endless patch lists with no business context simply now cannot keep pace with either demand.

In this session, we will explore how risk-based exposure management helps security leaders in financial services move from reactive patching to a prioritised, business-context view of risk; one that supports operational resilience objectives and third-party risk oversight while standing up to regulatory scrutiny. Drawing on real world examples, we'll explore how teams can strengthen incident response readiness and reduce exposure before attackers, or auditors, find it first.

---

**11.15am** **Tea, coffee, and networking break**

---

**11.45am** **Mitre fraud framework**

**James Kwaan** Senior Manager, Lloyds Banking Group

Financial fraud is a global and rapidly escalating threat. In the UK alone, 2025 saw over 4.06 million confirmed payment-fraud cases, around eight every minute, with losses reaching £1.28 billion. Fraud is increasingly online, telecoms-enabled and technology-driven, with criminals exploiting digital platforms, social engineering and cyber capabilities to identify, manipulate and monetise victims. Notably, 66% of authorised push payment fraud cases originate online.

The MITRE Fight Fraud Framework (F3) offers a structured, industry-backed approach to understanding and combatting this threat.

**12.30pm** **Starting from scratch - how I built a security function with no framework, no CISO and limited budget**

**Andy Papastefanou** CEO and Founder, Talanos Cybersecurity
**Freddie Leadsom** CTO, Klearium Group

Eighteen months ago, Freddie Leadsom became the first CTO, and the first senior technical hire, at Klearium - a fast-growing payments business. Cyber security was his responsibility from day one, but his credibility and focus depended on building the product. Plus, as CEO of the London entity, the compliance and payments liability lay with him if things went wrong.

In conversation with Andy Papastefanou, CEO of Talanos, who has worked alongside him from a point-in-time assessment through a live incident to a managed SOC, Freddie will discuss how first principles determine his approach to managing cyber risk, what prompted his decision to invest in a SOC a year after first discussing it, and why a steady drumbeat of managed risk goes further than silence with a board.

---

**1pm** **Networking lunch**

---

**2pm** **Extreme teams in extreme contexts; small teams making a big impact**

**Shaun Pascoe** CEO, Lest We Forget Association

Sqn Ldr (Retd) Shaun Pascoe joins us to discuss how his career has shaped his retirement from the military. Used to stepping up, Shaun has set up, and run, truly lifechanging third sector projects and capabilities for veterans. During his 16-year career in the Royal Air Force (RAF), Shaun led a Medical Emergency Response Team (MERT) which treated injured troops while they were being transported by helicopter back to military bases. He served on operational tours in Kosovo, Sierra Leone, Iraq and Afghanistan.

Emerging from the military with a clear understanding of effective leadership Shaun discusses how lessons from these experiences influence his leadership style today and what we can all learn from him in terms of identifying a requirement and turning that idea into an effective reality.

**2.45pm** **Beyond the balance sheet: Quantifying the financial risk of agentic AI**
**Jake Anthony** Principal Solutions Engineer, Exabeam

Autonomous AI agents are rewriting the rules of insider risk by introducing a complex class of digital entities operating at machine speed. For financial services organisations, where data integrity and compliance are paramount, this shift presents an unprecedented governance challenge. Traditional monitoring tracks isolated actions, but it lacks the behavioural context needed to detect when an AI agent has exceeded its permissions, accessed sensitive records, or drifted into high-risk behaviour.

This session dives into key findings from Exabeam's global research, "The Agentic Insider." We will dissect a critical disconnect holding financial institutions back: while 93% of finance and security leaders align on cyber risk, 55% of security initiatives are delayed or scaled back because CISOs struggle to translate technical exposures into financial terms their CFOs require.

**3.15pm** **Panel discussion: When an AI agent, supplier or digital platform contributes to customer harm, fraud or operational failure, where does accountability ultimately sit - and how should financial institutions respond?**
**Facilitated by Liz Murray** Chief of Staff, The SASIG
**Charlotte Sadd** Market Engagement Lead, CIFAS
**James Kwaan,** Senior Manager, Lloyds Banking Group

All organisations operate in a complex environment. Control is key, but how do we know we've got a full view to enable true risk to be understood and accountability to be apportioned. Cross-business collaboration is required between Fraud, Financial Crime teams and Cyber. AI Architecture (beyond cyber protective) needs to be well understood throughout the organisation - Onboarding of suppliers for critical systems needs more scrutiny than before with Identity and access management being key. Are there "quick and effective wins" that organisations can use, or are we reliant on processes that are thorough but may not be agile enough to address control gaps?

---

**4pm** **Closing Remarks & End of meeting**

---

# About

**The Security Awareness Special Interest Group (SASIG)**

SASIG is a subscription-free networking forum, membership now represents thousands of organisations of all sizes from across the world and from all sectors, public and private. Its 11,200+ membership is drawn from CIOs, CISOs and their staff with responsibility for cybersecurity within their organisations. Professionals from other disciplines (risk, HR, legal, supply, etc.) and representatives from government, law enforcement and academia are also being increasingly welcomed at events. The Chatham House Rule is strictly enforced and universally respected at all meetings, and vendors and the Press are routinely excluded. Thus, the level of debate is extraordinarily revealing and rewarding.

SASIG has a members' website at www.thesasig.com. Please register here for membership.

## With thanks to our Supporters and Contributors…

Redflags · WAVESTONE · exabeam · Qualys · ncc group · CoreView · BREACHRX · Symantec by Broadcom · Carbon Black. by Broadcom · Arrow · MIMOTO · f5

CYBSAFE · censys · Bridewell · KUDELSKI SECURITY · Vanta · COFENSE · Patrowl · PENTERA · Talanos cybersecurity · cymulate · Qevlar AI · KYOCERA · Astran · SECURITY JOURNEY

020 4583 5030
info@thesasig.com
www.thesasig.com