ENTERPRISE SECURITY MANAGEMENT SYSTEM

ASIS FEATURE

DYNAMICS IN SECURITY ENTERPRISE

The strategic imperative is clear: a unified view of risk. Security leaders must bring together physical and cyber functions under one governance model, ensuring that policies, technologies, and teams operate with shared visibility and accountability. This convergence is also what regulators and boards increasingly expect when they assess enterprise resilience.

- Page 4

Respect Beyond the Contract: How Jamaica Customs Agency Values Its Security Guards

Though our security guards are employed through external contractors, we have long believed that those who protect our people, property, and assets deserve to be treated as an integral part of our team.

- Page 6

Project Management as a Strategic Enabler for Security Transformation

In today's volatile business environment, organizations are under increasing pressure to modernize their security programs while maintaining operational efficiency. As threats evolve from physical intrusions to integrated cyber-physical risks the need for structured, strategic transformation within the security function has never been greater.

- Page 2

Contents

MESSAGE FROM THE CHAIRMAN:
Lt.Col. Dr. Oswald J Smiley, CPP, PSP

Rebuilding with Resilience: Standing Strong After Hurricane Melissa
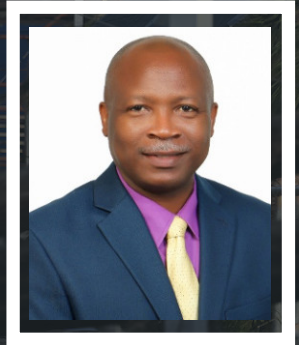
Photo courtesy of: abcnews.go.com/US/disastrous-images-emerge-jamaica-direct-hit-hurricane-melissa/story?id=126975245

As our beloved island continues to recover from the passage of Hurricane Melissa, I extend heartfelt thoughts and prayers to all our members, their families, and communities that have been affected. The past weeks have tested our resilience as a nation, but as Jamaicans, we have once again demonstrated strength, unity, and an indomitable spirit.

The ASIS Jamaica Chapter stands in solidarity with all security professionals who continue to serve tirelessly during this period of recovery. Many of our members have been on the frontlines, ensuring the protection of people, property, and critical infrastructure, while also lending a hand to rebuilding efforts within their organizations and communities. Your dedication embodies the true spirit of service and leadership that ASIS represents.

As we rebuild, let us also reflect on the lessons learned, about preparedness, adaptability, and the vital role of security management in national resilience. Together, we can emerge stronger, not only restoring what was lost but also reinforcing systems and partnerships that make us more robust for the future.

I encourage every member to stay engaged, support one another, and continue upholding the highest standards of professionalism. Let us turn this moment of challenge into an opportunity for growth and collaboration, both within our Chapter and across the wider ASIS community.

On behalf of the Executive Committee, I thank you for your unwavering commitment and extend appreciation to our regional and international ASIS partners who have offered their support and solidarity during this time.

Together, we rebuild. Together, we rise.

Members of ASIS International-Jamaica Chapter L-R: SSP Michelle Campbell, Aldean Campbell, Suzanne Scarlett, LLB (Hons), PSP, Det. Cpl. Chadwick Williams, and Capt. Basil Bewry, CPP, PCI, PSP pose for a photograph before handing over a symbolic care package at Black River Police Station on Nov 2 after the passage of hurricane Melissa.

Chapter members pose with members of the JCF after handing out care packages in Black River.

PROJECT MANAGEMENT AS A STRATEGIC ENABLER
FOR SECURITY TRANSFORMATION

THE NEED FOR STRUCTURED, STRATEGIC TRANSFORMATION WITHIN THE SECURITY FUNCTION HAS NEVER BEEN GREATER.

Lt.Col. Dr. Oswald J Smiley, CPP, PSP, *Chairman, Jamaica Chapter*

In today's volatile business environment, organizations are under increasing pressure to modernize their security programs while maintaining operational efficiency. As threats evolve from physical intrusions to integrated cyber-physical risks the need for structured, strategic transformation within the security function has never been greater.

While security professionals are adept at assessing risks and deploying protective measures, success in large-scale transformation requires more than technical expertise. It demands a disciplined approach to planning, governance, and execution the very principles found at the heart of project management.

Security Transformation: A Strategic Imperative

Security transformation refers to the modernization of systems, infrastructure, and processes to align with organizational objectives and emerging threats. This may include introducing new surveillance technologies, upgrading access control systems, or implementing enterprise risk management platforms.

Without structured project oversight, these initiatives risk falling behind schedule, exceeding budgets, or failing to achieve intended outcomes. That's where project management becomes indispensable turning ambitious visions into measurable, achievable results.

How Project Management Enables Security Success

Project management methodologies such as PMBOK®, PRINCE2®, and Agile provide a proven framework for delivering complex security projects. They introduce governance, accountability, and a repeatable process for success.

> **With project management in place, clear scope definition, milestone tracking, and risk controls ensure consistent delivery across all facilities.**

How project management strategically empowers security transformation:

- Governance and Clarity: Clearly defines objectives, timelines, and ownership across all project stages.
- Risk Integration: Aligns security threats with enterprise risk management practices, ensuring proactive mitigation.
- Resource Efficiency: Optimizes the use of people, technology, and capital to achieve maximum value.
- Stakeholder Engagement: Improves communication between security, IT, operations, and leadership.
- Performance Tracking: Establishes key metrics to evaluate project success and alignment with strategic goals.
- In essence, project management turns security upgrades from reactive responses into proactive, strategic investments.

A Practical Example

Consider an organization deploying a new multi-site access control system. Without a project framework, the rollout might face inconsistent implementation or cost overruns. With project management in place, clear scope definition, milestone tracking, and risk controls ensure consistent delivery across all facilities.

The Leadership Connection

For today's security leaders, understanding project management is no longer optional it is a core competency. Applying structured methodologies helps security departments communicate in the language of business: strategy, return on investment, and performance.

> **By combining the precision of project management with the foresight of security leadership, organizations can achieve transformation that is both protective and progressive.**

When security transformation initiatives are managed as strategic projects, they attract greater executive buy-in, foster cross-department collaboration, and deliver outcomes that support long-term organizational resilience.

Project management is more than an administrative tool, it's a strategic enabler of effective, sustainable transformation. By combining the precision of project management with the foresight of security leadership, organizations can achieve transformation that is both protective and progressive.

In this era, success belongs to those who don't just secure assets, but manage change with vision, structure, and purpose.

SECURING THE CONVERGED ENTERPRISE:

Why PIAM Must Anchor the Future of Security

By Warren Smith CPP, PCI, PSP, CRISC, CISSP
ASIS Member

In today's environment, the most dangerous assumption a security leader can make is that physical and cyber domains can be managed independently. Threat actors don't think in silos, and neither should we. The ability to seamlessly integrate Physical Identity and Access Management (PIAM) with cybersecurity and logical access control is no longer optional, it is fundamental to building resilient organizations.

PIAM AS THE CORNERSTONE OF CONVERGENCE

For too long, PIAM has been underestimated, seen primarily as an operational tool for managing badges, biometrics, and visitor passes. PIAM has become the cornerstone of security convergence. When integrated effectively, PIAM provides:

- Identity lifecycle management that unifies HR, IT, and security processes.
- Automated, policy-driven controls that reduces insider threat exposure.
- Real-time threat correlation, linking physical events with cyber alerts.

- Stronger compliance frameworks, particularly in regulated industries.

This isn't about efficiency alone, it's about ensuring that every identity, every credential, and every access request is continuously validated against the organization's most critical risks.

THE STRATEGIC IMPERATIVE OF CONVERGENCE

The risks we face today often cut across both domains. A compromised digital credential can open a physical door. A stolen badge can serve as the entry point to a cyber intrusion. These are not theoretical risks, they are scenarios we see play out in real time across industries.

The strategic imperative is clear: a unified view of risk. Security leaders must bring together physical and cyber functions under one governance model, ensuring that policies, technologies, and teams operate with shared visibility and accountability. This convergence is also what regulators and boards increasingly expect when they assess enterprise resilience.

> ❝ *The convergence of PIAM, physical security, and cybersecurity is not just a technological shift, it is a leadership challenge. AI and quantum computing will test our models, our resilience, and our ability to adapt.*

THE DISRUPTORS WE CANNOT IGNORE: AI AND QUANTUM COMPUTING

Two forces will profoundly test our ability to maintain secure, converged ecosystems: artificial intelligence and quantum computing.

- **Artificial Intelligence (AI):** Attackers are already exploiting AI to generate deepfakes capable of bypassing biometric verification, or to identify patterns in employee behavior that can be manipulated. At the same time, AI strengthens our defenses, driving predictive analytics, anomaly detection, and automated response. The opportunity is enormous, but so is the risk of over-reliance. AI should augment human judgment, not replace it.

- **Quantum Computing:** While timelines remain uncertain, the impact is not. Once quantum computing achieves scale, it will render today's encryption standards obsolete, directly threatening the cryptographic backbone of PIAM and identity systems. Security leaders must start preparing now, demanding crypto-agility from vendors and shaping roadmaps toward post-quantum cryptography. Waiting for certainty is not a strategy; preparation is.

LEADING THE WAY FORWARD

Our role as security leaders is not simply to defend against today's risks, but to anticipate tomorrow's disruptions. The immediate priorities are:

1. Embed zero trust everywhere, from firewalls to front doors.
2. Integrate PIAM into the enterprise security architecture, connecting Identity and access management (IAM), security information event management (SIEM), and governance.
3. Balance AI adoption with human oversight, ensuring decisions that affect enterprise resilience never rest solely with machines.
4. Plan for the quantum transition now, making crypto-agility a standard part of security conversations with stakeholders and vendors.

The convergence of PIAM, physical security, and cybersecurity is not just a technological shift, it is a leadership challenge. AI and quantum computing will test our models, our resilience, and our ability to adapt. Those who succeed will be the leaders who embrace convergence as strategy, not simply as integration. They will recognize that the future of security is not divided into physical and digital domains, but unified under a single principle: trust must be earned, validated, and enforced everywhere, all the time.

> ❝ *Attackers are already exploiting AI to generate deepfakes capable of bypassing biometric verification, or to identify patterns in employee behavior that can be manipulated.*

RESPECT BEYOND THE CONTRACT:

How The Jamaica Customs Agency Values Its Security Guards

Kingsley A.M. Henry, JP, psc
ASIS Member

At the Jamaica Customs Agency, security is not just a contracted service—it's a vital pillar of our organization's strength and integrity. Though our security guards are employed through external contractors, we have long believed that those who protect our people, property, and assets deserve to be treated as an integral part of our team. After all, respect and inclusion form the foundation of true security.

Our approach is simple: we refuse to draw unnecessary lines between "staff" and "contracted personnel." Every individual who contributes to the safety and success of the Jamaica Customs Agency is treated with the dignity and appreciation their role deserves. We recognize that while guards may wear a different uniform, they stand as our first line of defence—maintaining vigilance, order, and professionalism in an environment where trust is essential.

Importantly, security guards are often the first and last representatives of the Jamaica Customs Agency that customers, visitors, and staff interact with. From the moment someone enters our premises to the time they leave, the guard's demeanour, communication,

> **Security guards are often the first and last representatives of the Jamaica Customs Agency that customers, visitors, and staff interact with.**

and conduct shape the perception of our entire organization. For that reason, it is essential that they feel motivated, respected, and supported to embody our CAPIT values—Customer-focused, Accountability, Professionalism, Integrity, and Transparency. These values guide not only our internal operations but also how every member of the extended Jamaica Customs Agency family interacts with the public we serve.

This belief comes to life in tangible ways, when the Agency hosts events for staff such as fundays or Christmas parties, our security guards are always invited. They celebrate alongside administrative and operational staff, sharing in the laughter, camaraderie, and sense of belonging that strengthen workplace

morale. During Easter, when we distribute bun and cheese, our guards are not left out. They too receive this small token of appreciation, reinforcing that they are valued members of the wider Customs family.

This culture of respect extends beyond celebrations. We do not tolerate any form of disrespect toward our security personnel. Every employee is expected to treat guards with the same courtesy and professionalism they would show a colleague or supervisor. Security guards carry a unique responsibility—one that demands composure, alertness, and courage. Recognizing their efforts isn't merely good management; it is a matter of organizational ethics.

Photo courtesy of: facebook.com/KingAlarmJA

When guards feel respected, they perform their duties with greater pride and commitment. They become more than sentinels at the gate—they become ambassadors of the Jamaica Customs Agency's CAPIT values, representing the spirit of service and integrity that defines who we are.

Photo courtesy of: https://richmondjamaica.com/wp-content/uploads/2018/03/1517377875-05_-_View_from_Main_Gate.jpg

BUILDING RAPPORT:
A Key to Liaison Relationships

Carlos Pipher, BSc (Hons) CPP, PCI, PSP
Newsletter Editor

> *Rapport serves as the bedrock of effective communication and teamwork. When individuals feel seen, heard, and valued, they are more likely to collaborate*

In today's interconnected world, the ability to build strong relationships with individuals and organizations is a critical skill for success. Whether you are working on a collaborative project, joining a new workplace, or seeking partnerships for a cause, building rapport is more than just being friendly. It is about creating a foundation of trust, understanding, and mutual respect.

Why Rapport Matters

Rapport serves as the bedrock of effective communication and teamwork. When individuals feel seen, heard, and valued, they are more likely to collaborate openly, share ideas freely, and commit to common goals. Within organizations, this strengthens culture, encourages innovation, and drives productivity. On a personal level, strong rapport helps you influence, lead, and connect more deeply with your peers or colleagues.

Build Rapport with Colleagues

1. **Be Present and Attentive.** Building rapport starts with active listening. When engaging with colleagues, give them your full attention. Avoid interrupting and respond thoughtfully. Small actions like remembering names, asking about someone's day, or showing genuine interest in their views go a long way.

2. **Find Common Ground.** Shared experiences or interests foster quick connections. During conversations, look for commonalities such as hobbies, values, or professional goals. These shared elements help establish familiarity and trust.

3. **Show Respect.** Understanding another person's perspective is essential in building rapport. Acknowledge their feelings and experiences without
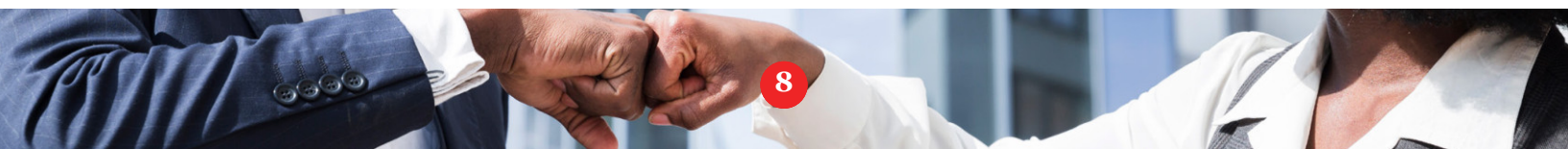
judgment. Respect their time, contributions, and boundaries. Even when disagreements arise, maintain civility and openness.

4. **Be Authentic.** People tend to respond positively to sincerity. Be honest about your intentions, and don't pretend to be someone you are not. Authenticity creates a safe space where others feel comfortable reciprocating trust.

5. **Follow Through on Promises.** Reliability is a cornerstone of rapport. If you commit to something no matter how small ensure you follow through and avoid the excuses. Consistency builds credibility and reinforces dependability.

Building Rapport with Organizations

While building rapport with individuals is rooted in interpersonal connection, developing rapport with organizations requires a strategic and respectful approach.

1. **Understand Their Mission and Culture.** Before reaching out or partnering with an organization, take time to research its mission, vision, values, and work culture. This not only shows respect but allows you to tailor your communication in a way that aligns with their principles.

2. **Mutual Value.** Relationships with organizations should be mutually beneficial. Think about what you bring to the table; skills, resources, networks, or fresh perspectives and be clear about how both parties can gain from the relationship.

3. **Communicate Professionally and Transparently.** Whether via email, presentations, or meetings, your communication should be clear, concise, and respectful. Transparency about your goals and expectations sets the stage for honest collaboration. Your communication should be speaking for you long after it has been received.

4. **Be Patient and Consistent.** Building organizational rapport takes time. Be patient, follow up respectfully, and continue to show engagement without being overbearing. Regular, positive interactions help reinforce your presence and build familiarity.

5. **Honor the Organization's Protocols.** All Organizations has internal processes. Whether it's submitting proposals, requesting meetings, or engaging in partnerships, following established protocols demonstrate professionalism and respect.

Sustaining Rapport Over Time

Building rapport is not a one-time effort, it requires ongoing care. Regular check-ins, appreciation for others' efforts, and a willingness to adapt help maintain strong relationships. Celebrate shared wins and navigate challenges with empathy. Most importantly, prioritize integrity in all your interactions. In a world where relationships often define outcomes, investing time and effort in building rapport is one of the most valuable things a security professional can do.

SECURITY TIPS

☑ Always practice vigilance.

☑ Examine the ID card of utility personnel coming to do repairs.

☑ When at home never leave your front or back door open if you cannot see it.

☑ Never enter your car or home if it's obvious that it was broken into, contact the police.

☑ When leaving or entering your home always check your surroundings for strange vehicles or people.

SECURITY METRICS:
A Case for Better Numbers

Keron Thomas, PCI, PSP
Chapter Secretary

"

Security Metrics considers the application of quantitative, statistical and/or mathematical analyses in measuring functional costs, benefits, successes, failures, trends and workload

Whether you attribute it to Peter Druker or Lord Kelvin, the popular adage of, "That which cannot be measured, cannot be managed", is a central principle in any operation, and more so in security management, when you consider the protection mission of security professionals. In the October 2015 edition ASIS International Security Management magazine, George Campbell, put it this way, "…simply counting isn't metrics, but rather the first step in digging into data to determine root causes and connections". Identifying root causes and connections from data requires numerical values obtained through security metrics.

"Security Metrics considers the application of quantitative, statistical and/or mathematical analyses in measuring functional costs, benefits, successes, failures, trends and workload" (Kovacich & Halibozek, 2006). Fast track to 2025, the sentiments has not changed, as many security professionals will agree that a well thought out, and implemented security management program involves far more than the collection of metrics or data at an access point or information contained in reports. Data that is collected and not converted into smart security metrics is only a metric, and it does little to improve security efficiency and effectiveness

Take the case of a store detective patrolling the isles of a retail facility, actively scouting for would be criminals, doing their equivalent counter patrols to defeat the security system. Typically, merchandise that is illicitly taken from a shelf is removed from its package and subsequently left in the store. The loss is then documented by the store detective, and the abandoned package is submitted to management for a write-off. This action does little to either deter or mitigate the loss. Using the same scenario, smart security metric management can influence the design and implementation of a robust security program, which in turn can lead to reduced incidents and making the business case for the security program. To achieve this, security practitioners must engage greater details of the incident than the usual time, date, cost and description of the item, that serves to properly explain both the facility's operation and the adversary' profile.

Smart security metrics would include among other things, data on the dump point for the discarded

merchandise box, the isle number where the item is kept, the item's department, quantity taken over time, and the organisations accounting period to review the loss(es) over time. The collection and analysis of these additional data can provide security metrics into trends in theft, security gaps (little or no systems in place), security justification (ROI) or establish the risk management strategy (eliminate, reduce, transfer or accept the loss).

These and similar security metrics have served numerous security programs well in telling the story of incidents with succinct clarity. Security metrics allow for easy persuasion, and both the selling and driving

> *The collection and analysis of these additional data can provide security metrics into trends in theft, security gaps (little or no systems in place), security justification (ROI) or establish the risk management strategy*

of the organisation's security strategy to the C-Suite, in a way that energizes action and supports unbiased conclusions. "Security metrics are to steer us where we are going, and not just to log from whence we came" (Jaquith, 2007).

SECURITY TIPS

☑ When driving, if a vehicle bumps you at a lonely or isolated place, do not stop, drive to a populated area or the nearest Police Station.

☑ Always check your surroundings when entering and exiting an ATM. When an ATM is being serviced by security personnel, do not stay too close, because a robbery or shooting could occur.

NAVIGATING DATA PROTECTION LAWS:

Operational Realities and Strategic Advantages for Professional Investigators

Conroy Samuda, CPP, PCI, FIoL
ASIS Member

Introduction

In this era of digital forensics, cloud investigations, and global data sharing, investigators face growing scrutiny over how personal data is obtained and managed. Data protection laws are reshaping private investigations, demanding both regulatory discipline and operational agility. For Certified Protection Professionals (CPP), and Professional Certified Investigators (PCI), compliance is now integral to ethical and effective practice. While privacy laws introduce challenges, they also create opportunities for leadership, innovation, and trust. This article outlines how investigators can align with these regulations to strengthen professional standards and expand service capability.

Operational Realities and Strategic Advantages

Restricted Data Access and Compliance Demands

Privacy laws require explicit consent before processing personal data. Though this slows information gathering,

it reinforces professionalism and transparency. Consent and documentation procedures protect investigators from liability and build client confidence—hallmarks of disciplined, ethical practice.

Evidentiary Constraints and Legal Exposure

Strengthened legal boundaries restrict certain investigative techniques and increase the risk of sanctions for misuse. However, innovation within lawful limits—using open-source intelligence, behavioral analysis, or anonymized data—maintains effectiveness while upholding compliance. A PCI's structured approach to evidence validation ensures accuracy and legal defensibility.

Cross-Border Data Challenges

International cases often span jurisdictions with varying privacy laws such as the EU's General Data Protection Regulation (GDPR) or the UK's Data Protection Act. Investigators who understand these frameworks gain a competitive edge, managing complex cases confidently

and lawfully. Mastery of cross-border compliance builds credibility and expands investigative reach.

Evolving Client Expectations

Clients increasingly demand transparency, confidentiality, and demonstrable data security. Meeting these expectations requires clear communication, lawful practice, and technological safeguards. Demonstrating privacy readiness distinguishes certified professionals and fosters lasting trust.

Technology as a Compliance Enabler

Strong data governance depends on secure systems—encryption, access control, and structured retention. Though requiring investment, these tools enhance accuracy, documentation integrity, and efficiency. Technology thus becomes both a compliance mechanism and a competitive advantage.

Operational Strategies for Compliance and Continuity

- Apply encryption and structured data controls to safeguard sensitive material.
- Implement documented consent and disclosure procedures.
- Conduct internal audits and maintain consultation with legal counsel.
- Automate compliance processes to improve consistency.
- Collaborate with privacy specialists to ensure regulatory alignment.

> " *Data protection laws are reshaping private investigations, demanding both regulatory discipline and operational agility.*

### Professional Value Proposition

CPPs and PCIs offer a unique advantage: the integration of investigative rigor, risk-based thinking, and ethical oversight. This combination allows for effective yet defensible outcomes and sets a benchmark for integrity within the investigative profession.

Expanding Professional Horizons

The emphasis on privacy invites investigators to diversify—offering data compliance audits, due diligence, and information-security consulting. These services align naturally with CPP and PCI competencies, enhancing reputation, resilience, and revenue potential.

Conclusion

Data protection laws are redefining investigative work, requiring a balance between intelligence gathering and privacy stewardship. For certified professionals, compliance is more than a legal necessity—it is a hallmark of credibility and leadership. By embedding privacy principles into investigative practice, investigators will reinforce integrity, protect clients, and reshape the profession.
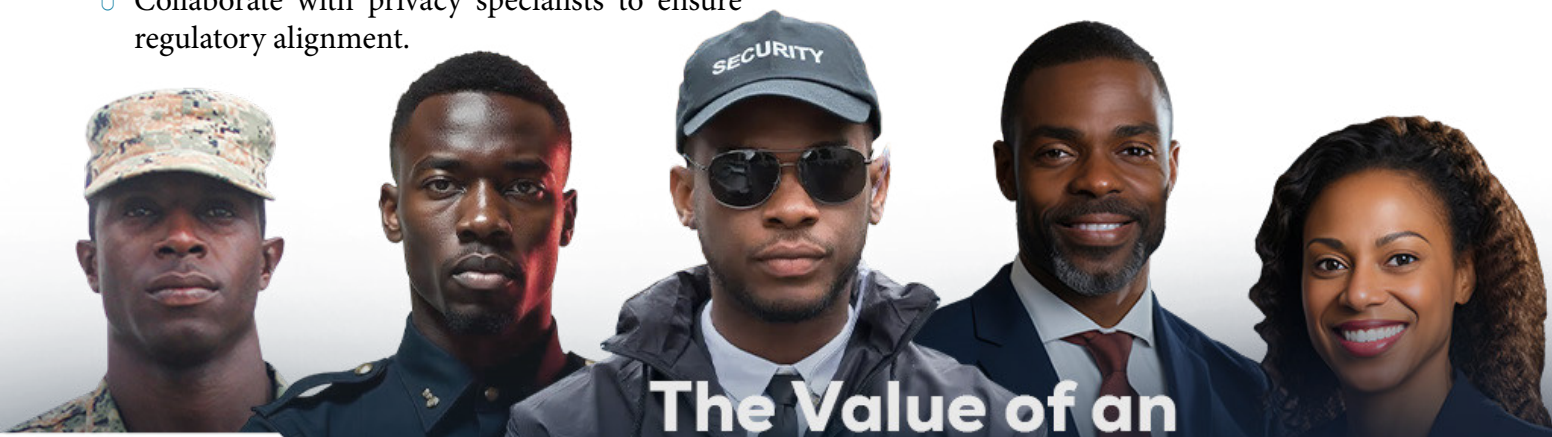
The Value of an
ASIS CERTIFICATION

MASTERY OF SECURITY PRINCIPLES | IMPROVED LEADERSHIP SKILLS
INCREASED EMPLOYABILITY | PROFESSIONAL GROWTH

Hosted by

ASIS INTERNATIONAL®
JAMAICA CHAPTER

Celebrating Excellence:
Honouring Our Award-Winning Chapter, Organizations, and Security Professionals
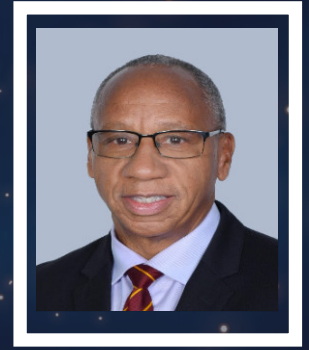
Capt. Basil Bewry, CPP, PCI, PSP | Latin America and Caribbean Regional Board Director

ASIS International has long celebrated excellence in security leadership, professional development, and volunteer service. The Jamaica Chapter and its members continue to distinguish themselves globally, earning some of the most prestigious honours across the ASIS ecosystem. This article highlights the outstanding achievements of our chapter, partner organizations, and exemplary security professionals whose dedication continues to elevate the profession.

ORGANIZATIONAL AWARDS

I.B. Hale Chapter of the Year Award

Widely regarded as one of ASIS International's most significant honours, the I.B. Hale Chapter of the Year Award recognizes outstanding chapters that consistently deliver timely, relevant, and high-quality resources to security practitioners worldwide. Chapters earning this recognition demonstrate excellence in knowledge sharing, best practices, professional networking, and member engagement.

The ASIS Jamaica Chapter has achieved this remarkable distinction for six consecutive years—2020, 2021, 2022, 2023, 2024, and 2025. This unprecedented achievement reflects the chapter's unwavering commitment to member development, innovative programming, and global leadership within the ASIS community.

Professional Certification Board (PCB) Organizational Award of Merit

This award honours organizations that display exceptional commitment to elevating the skills and competencies of their security teams through ASIS certification.

- **Hawkeye Electronic Security Limited** received the PCB Organizational Award of Merit in 2017, demonstrating its longstanding culture of professional development.
- **Guardsman Group Limited** earned the honour in 2022, further highlighting Jamaica's leadership in fostering certified security expertise across the region.

Roy Bordes Educational Grant

The Roy Bordes Award provides up to US$10,000 for a chapter to host a two-day educational program designed to advance security knowledge and capability.

In 2021, the **ASIS Jamaica Chapter** was awarded this prestigious grant, enabling the delivery of high-value security education on Enterprise Security Risk Management to members and industry stakeholders.

Chapter Website of the Year Award

This award recognizes chapters whose website content, design, and functionality provide exceptional value to ASIS members.

The **ASIS Jamaica Chapter** proudly won the Chapter Website of the Year Award in 2020, reflecting its commitment to digital excellence, accessibility, and member engagement before the category was later absorbed into the I.B. Hale Chapter of the Year Award.

INDIVIDUAL AWARDS

E.J. Criscuoli, Jr., CPP Memorial Volunteer Leadership Award

This award honours an ASIS member who demonstrates long-term commitment, exceptional volunteerism, and impactful leadership at the chapter and regional level.

- **Basil Bewry, CPP, PCI, PSP** was honoured in 2020, in recognition of his exceptional contributions to chapter leadership and member advancement.
- **John Richards, CPP, PCI, PSP** received the award in 2025, further solidifying Jamaica's reputation for producing exemplary ASIS leaders.

Women in Security Global Community – Karen Marquez Honours

This award recognizes a female security professional who demonstrates consistent dedication to advancing the security industry and contributing meaningfully to her community.

- **Suzanne Scarlett, LLB (Hons), PSP** received this prestigious honour in 2022, making her as one of the most influential women in global security leadership.

Ralph Day Memorial Security Officer Heroism Award

Presented to private security officers who risk their lives to save others, this award represents courage at the highest level.

- Christopher Deslandes received an Honourable Mention in 2022 for his bravery and selfless service in the line of duty.

PCB Outstanding Achievement Award

This award recognizes individuals who demonstrate exceptional leadership in promoting the ASIS certification designations—CPP, PCI, PSP, and APP—and advancing the professionalism of the security industry.

- **Basil Bewry, CPP, PCI, PSP; John Richards, CPP, PCI, PSP; and Francine Staple, PSP** were honoured in 2016 for their significant contributions to certification growth and advocacy.
- **Garfield Owen, PSP** was recognized in 2017 for his invaluable contribution towards the advancement of the Chapter's certification program.
- **Garth Gray, CPP, PCI, PSP and Wayne Ballen, CPP, PCI, PSP** received the award in 2020, establishing early leadership in elevating certification across the region.
- **Selbourne Webb, CPP, PCI, PSP** earned the award in 2022, continuing Jamaica's legacy of excellence in professional certification.

CONCLUSION

These achievements reflect years of dedicated service, professional commitment, and leadership within the ASIS community. From organizational excellence to individual heroism and volunteer leadership, Jamaica continues to shine as a global force in security management.

Congratulations to all awardees as your accomplishments have helped inspire the entire security profession.

SECURITY TIPS

- ☑ Never leave expensive gadgets or high value assets on your car seat when you are not in your motor vehicle, place them in the trunk.

- ☑ Be careful how you dispose of packaging material, it can indicate that you bought a particular item, this may attract thieves.

- ☑ Lock your vehicle doors immediately after you get into your vehicle.

Members of the Jamaica Chapter pose with the I.B. Hale Chapter of the Year Award. The Jamaica Chapter has won the award for six consecutive years from 2020 to 2025.

Jason Robinson, PCI, PSP (centre), collects his plaque for being the Jamaica Chapter Member of the Year 2024.

Captain John Richards, CPP, PCI, PSP was the winner of the 2025 E. J. Criscuoli, Jr., CPP, Memorial Volunteer Leadership Award.

SECURITY TIPS

☑ Always lock the ATM door when inside. Never leave the ATM with cash in your hand, put it away before exiting.

☑ If you reside in a controlled gated community, ensure all guests, visitors and vendors to your property are documented in the gate management system.

Chapter Members of the Quarter for 2025

Tania Rhoden, CPP, PSP
Member of the Quarter
January – March 2025

Keron Thomas, PCI, PSP
Member of the Quarter
April – June 2025

Carlos Pipher, CPP, PCI, PSP
Member of the Quarter
July – September 2025

Review the Certification Handbook for more details on policies, procedures, eligibility requirements, testing options (test center or remotely proctored exams), and fees for the ASIS certification program. It also contains the domains, tasks, and knowledge statements for all four of our certifications.

CLICK HERE

ASIS International
Board Certification Handbook

Advance Your Security Career

Enhance your expertise in key areas of security through ASIS certificate courses. These focused learning programs are designed to build and reinforce professional competencies, whether you're new to the field or a seasoned practitioner. Successful completion earns you Continuing Professional Education (CPE) credits.

Click Here to Read More
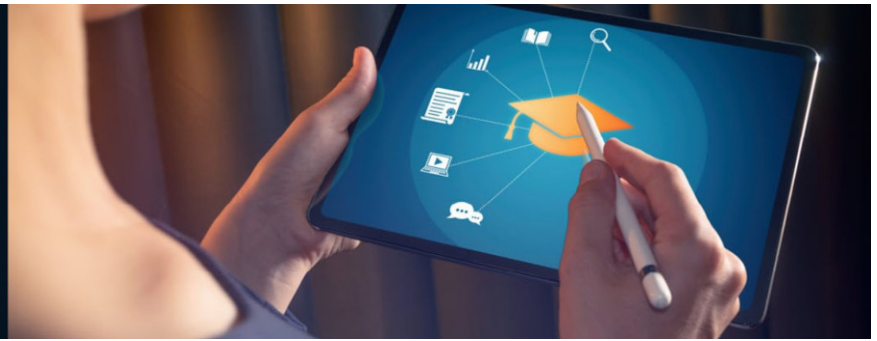
GAIN EVERY ADVANTAGE

More possibilities.
More responsibilities.
More trust.

An ASIS International certification offers limitless opportunities to advance in your career. Whether you're new to the field or a security management veteran, you can find a credential that aligns with your objectives and raises your profile among our global community of security professionals. Our four certifications are widely recognized symbols of excellence that establish your mastery. This expertise gives you an unmatched advantage in your threat-prevention strategies—and in the marketplace.

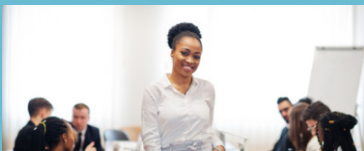**JOIN TODAY**

Congratulations

Georgia Sanderson, PSP

The Executive and Members of ASIS International Jamaica Chapter proudly congratulates

Georgia Sanderson, PSP

For her recent
Exam Success.

Georgia was successful in the PSP exam on July 31, 2025.

Steps to Certification

When you earn an ASIS board certification, you have a visible acknowledgment of a mastery of core security principles.

Click Here to Read More

Jamaica Chapter

For Information on ASIS International Jamaica Chapter, Contact:
Chairman: ojsmiley@gmail.com
Vice Chairman: swebbwoc@gmail.com
Latin America and Caribbean Regional Board Director: bewryba@gmail.com
Newsletter Editor: carlospipher@gmail.com