Enterprise Singapore

BUILDING DIGITAL TRUST

A Guide on Standards for Digital Security

CONTENT

ABOUT THIS GUIDE	**3**
INTRODUCTION	**4-5**
STEP 1: SELECTING THE RIGHT STANDARDS	**6-8**
STEP 2: GET CERTIFIED TO ASSURE CUSTOMERS OF YOUR QUALITY & RELIABILITY	**9-10**
CASE STUDIES	**11-13**
Ensuring Privacy: Navigating Personal Data Protection with Payboy	11
Global Expansion: Adopting Universal S&C with I-Sprint Innovations	12
Fortifying cybersecurity: Getting Certified with Cyber Essentials and Cyber Trust with DigiPixel	13

ABOUT THIS GUIDE

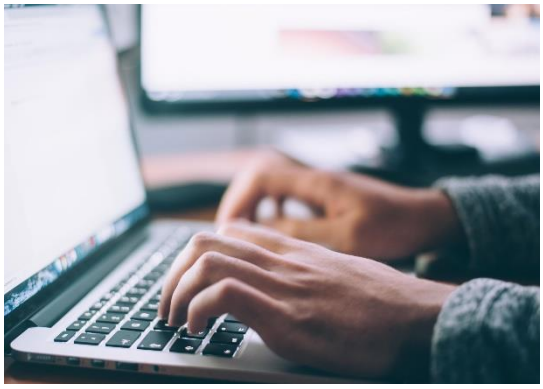
Differentiate your business by showcasing your commitment to strengthen cybersecurity and foster digital trust with clients. These can be done by adopting digital security-related Standards and Conformance that can safeguard your business from potential cyberthreats, maximising your company's growth potential.

Who is this guide for?

This guide is for companies in the Information and Communications Technology (ICT) sector and users of digital systems. Whether you are an engineer, consultant, contractor or solution provider, business owner, this guide will help you understand Standards & Conformance (S&C) in the digital space.

What is this guide for?

This guide helps SMEs adopt S&C to build trust with customers. With the right S&C, you can demonstrate your commitment to quality, digital security, and differentiate your business in a competitive landscape.



Through this guide:

1. Understand the importance and benefits of standards adoption in the management of Information and Communications Technology (ICT)-related applications and digital systems, such as Enterprise Resource Planning (ERP) systems, business intelligence software, and cloud-based solutions.
2. Identify the most relevant standards for your business through a self-guided questionnaire.
3. Discover how businesses in the ICT sector have successfully adopted and benefitted from S&C.
4. Explore certification as a next step after standards adoption.

Let's get started!

INTRODUCTION

The Digital Revolution and Rising cybercrime rates – what's at stake for businesses?

The global shift towards digitalisation has empowered companies with data-driven insights, enhanced productivity, and improved decision-making capabilities. The ICT sector is at the forefront of this revolution, providing essential systems and infrastructure that further enable businesses to undergo digital transformation.

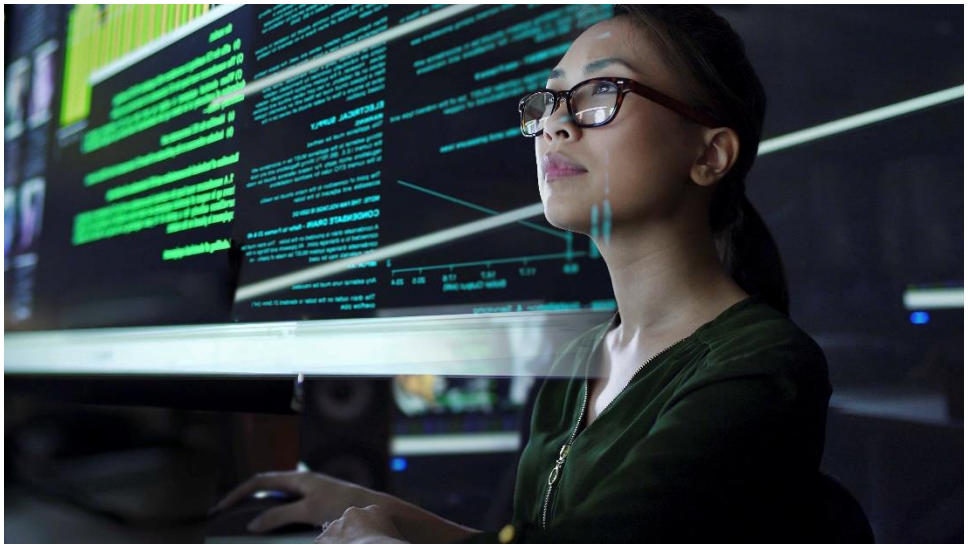
The World Bank projects that the global digital economy will reach a value of USD$20.8 trillion by 2025. At the same time, market indicators also reflect growing concerns on cybercrime, as its frequency continues to rise alongside the increasing reliance on technology in today's business landscape. The global cost of cybercrime is expected to soar to US$10.5 trillion, equivalent to 50% of the digital economy, by the same year. According to IBM's Data Breach Report, a concerning 83% of businesses experienced multiple data breaches in 2022.

Increased regulatory and public scrutiny in the ICT space is expected, and potential consequences from cybersecurity incidents will exacerbate. A key amendment in the Personal Data Protection Act (PDPA) in 2023 increased the maximum amount that a company can be fined for a data breach to S$1 million, or 10% of their annual turnover. McKinsey forecasts that market spending on cybersecurity service providers will reach US$101.5 billion in 2025.

Those that successfully build and establish digital trust with stakeholders are likely to gain a long-term competitive advantage. But how can this be achieved?

Source: World Economic Forum on "Why digital trust is key to building thriving economies"; US-ASEAN Business Council Whitepaper on Cybersecurity Standards and Conformance; McKinsey on "Cybersecurity trends looking over the horizon"

Enhancing your cybersecurity with standards



No business is spared from cybercrime threats. In fact, 43% of data breaches involve small enterprises, who are particularly vulnerable to malware, ransomware, brute-force attacks, and social attacks, which can cause serious negative impact. According to a 2021 report by IBM and the Ponemon Institute, the average cost of a data breach for businesses with fewer than 500 employees is US$2.98 million. These expenses include ransom payments, lost revenues to business downtime, remediation, legal fees, audit fees, and more.

Source: IBM Cost of a Data Breach Report 2023; Verizon 2023 Data Breach Investigation Report (DBIR)

Standards & conformance offers robust and systematic approaches to protect your organisation and mitigate potential risks, in the following ways:

The benefits of standards adoption

Facilitates Business Growth and Resilience

Standards serve as a valuable management tool, emphasising the significance of data security among employees and fostering organisational commitment by promoting a culture of continuous evaluation and optimisation of security management systems.

Enhances Reputation & Trust

Standards help assure your customers that their data and information is protected. It sends a clear signal to stakeholders your rigorous approach to information security and shields you from the negative publicity associated with security breaches.

Identifies and Manages Risk

Implementing standards tailored to your business ensures that controls and protocols are in place to minimise the likelihood of successful cyberattacks, enabling uninterrupted business operations and minimising disruptions.

Mitigates Financial Penalties

In addition to the direct costs incurred from cyberattacks, regulatory authorities impose stringent penalties on companies affected by data breaches. Adopting standards help keep you accountable and ensures that regulations are complied with, reducing the risk of fines or prosecution.

Adopting standards can aid in your business' journey by encouraging a culture of vigilance, streamlining processes, minimising costs associated with data breaches, and improving stakeholder trust and confidence.

STEP 1: SELECTING THE RIGHT STANDARDS

Ready to get started?

Consider the following standards for your business.

If you offer ICT or cybersecurity-related services:

ISO/IEC 27001: 2022 Information Security, Cybersecurity and Privacy Protection	ISO/IEC 27001 is the one of the most widely used international standards for information security management systems (ISMS), offering guidelines for establishing, implementing, maintaining and continually improving an information secure management system. It is ideal for companies looking to enhance the security of their information assets for international markets. READ MORE: ISO/IEC 27001
SOC 2 Type II Service Organisation Control 2	A SOC 2 Type II report is a Service Organisation Control (SOC) audit that assesses how an organisation manages sensitive information. It is particularly useful for companies seeking to enhance the security of their information assets for American markets. READ MORE: SOC 2 Type II
IEC 62443 Industrial Automation Control Systems Cybersecurity Standard	IEC 62443 is an international standard addressing cybersecurity for operational technology in automation and control systems. It is useful for cybersecurity companies offering automation and control system-related services, to help prevent and manage security risks. READ MORE: IEC 62443
Cyber Trust Mark SG CYBER SAFE | CYBER TRUST	The Cyber Trust mark is a cybersecurity certification developed by the Cyber Security Agency of Singapore (CSA) and is published as a national standard in Singapore. It is targeted at organisations with more extensive digitalised business operations and provides a guided risk-based approach for organisations to implement appropriate level of cybersecurity measures that are commensurate with their cybersecurity risk profile. READ MORE: Cyber Trust Mark | CSA Website
Cyber Essentials Mark SG CYBER SAFE | CYBER ESSENTIALS	The Cyber Essentials mark is a cybersecurity certification developed by the Cyber Security Agency of Singapore (CSA) and is published as a national standard in Singapore. It is a 'lightweight' certification for cyber hygiene, targeted at organisations that are embarking on their cybersecurity journey, e.g. Small and Medium Enterprises (SMEs), and provide protection from common cyber-attacks. READ MORE: Cyber Essentials Mark | CSA Website

If you are looking to safeguard customers' and partners' personal information:

ISO/IEC 27701:2019 Security Techniques	As an extension to ISO/IEC 27001 and 27002, this standard specifies requirements and provides guidance for establishing, implementing, maintaining and improving a Privacy Information Management System (PIMS). It is useful for companies looking to manage their internal data. READ MORE: ISO/IEC 27701
Data Protection Trust Mark 	The Data Protection Trust Mark is a certification issued by the Information and Media Development Authority (IMDA) for companies to demonstrate accountable and responsible data protection practices, as per Singapore's Personal Data Protection Act (PDPA) and international best practices. It is useful for companies looking to demonstrate compliance with the PDPA. READ MORE: Data Protection Trust Mark | IMDA Website

If your business offers cloud services:

ISO/IEC 27018:2019 Information Technology Security Techniques	ISO/IEC 27018 establishes commonly accepted control objectives, controls, and guidelines for implementing measures to protect personally identifiable information, in line with privacy principles for the public cloud computing environment. It is useful for cloud service providers processing personal identifiable information. READ MORE: ISO/IEC 27018
ISO/IEC 27017:2015 Information Technology Security Techniques	Together with ISO/IEC 27018, ISO/IEC 27017 provides controls and implementation guidance for both cloud service providers and cloud service customers. It is useful for cloud service providers processing personal identifiable information. READ MORE: ISO/IEC 27017
MTCS SS 584 Multi-Tier Cloud Security Singapore Standard	The Multi-Tier Cloud Security (MTCS) Singapore Standard (SS) 584 covers multiple tiers of cloud security. It is useful for cloud service providers looking to meet to meet differing cloud user needs for data sensitivity and business criticality. READ MORE: MTCS Certification Scheme | IMDA Website

If your business needs to demonstrate IT/product security:

Cybersecurity Labelling Scheme 	Under the Cybersecurity Labelling Scheme for consumer Internet-of-Things [CLS(IoT)], smart devices will be rated according to their levels of cybersecurity provisions to enable consumers to identify products with better cybersecurity provisions and to incentivise manufacturers to develop more secure products. Under existing mutual recognition arrangements, the CLS(IoT) label is recognised by Germany and Finland. READ MORE: Cybersecurity Labelling Scheme | CSA Website
ISO/IEC 15408 Common Criteria (CC) 	The Common Criteria establishes general principles for IT security evaluation and is adopted by members of the Common Criteria Recognition Arrangement (CCRA) to facilitate mutual recognition of evaluation and certification results. The Singapore Common Criteria Scheme (SCCS) is a cost-effective way for companies to evaluate and certify their products in Singapore and be mutually recognised by all CCRA member nations. READ MORE: Common Criteria Singapore Common Criteria Scheme | CSA Website

If your business conducts cross-border data transfers:

APEC CBPR and PRP 	The APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) is designed for organisations who process data cross-border on behalf of client organisations. It is useful for companies offering services or processing data for overseas clients, especially in the Asia-Pacific Economic Cooperation (APEC) region. READ MORE: APEC CBPR | IMDA Website
EU GDPR General Data Protection Rules	The General Data Protection Rules (GDPR) is a European Union (EU) regulation on information privacy in the European Union, European Economic Area, and any other location where European data is processed. As a benchmark for laws in many other countries, it is particularly valuable for companies that process data for clients in the EU. READ MORE: EU GDPR | European Commission Website INFORMATION ON EU GDPR CERTIFICATION: Europrivacy™/®

Visit the Singapore Standards e-shop to purchase standards.

STEP 2: GET CERTIFIED TO ASSURE CUSTOMERS OF YOUR QUALITY & RELIABILITY

Now that you have identified relevant standards for your business, you may consider certification as the next step.

Certification assures your customers and other stakeholders that your company has undergone independent verification to meet or exceed the benchmarks prescribed in the standards.

Certification can be a powerful marketing tool as they help demonstrate compliance to industry benchmarks. This can provide a competitive edge in business tenders, especially if your competitions do not have similar certifications.

Furthermore, consider getting your certification through a Conformity Assessment Body (CAB) that has been accredited by the Singapore Accreditation Council (SAC) and reap even greater benefits.

The benefits of engaging a SAC-accredited CAB

1. Reduced risk and higher level of quality assurance
   Removes the guesswork when you are selecting a reliable CAB. SAC-accredited CABs have been assessed according to internationally recognised conformity assessment frameworks, ensuring that you receive high-quality service that aligns with your requirements.

2. Access more business opportunities worldwide
   Overseas markets are more ready to accept reports from an accredited CAB, minimising technical barriers to trade. The SAC has signatory status in Mutual Recognition Arrangements with various international organisations. This means that your goods and services will be more readily accepted in these signatory countries without re-testing or re-certification.

3. Time and cost savings
   By working with an accredited CAB, you save costs and time by reducing product failures and operational downtime. Furthermore, you minimise the need for re-testing, re-auditing, and re-certification of your products and services.

Recognising accredited CABs

An inspection body that has been accredited by SAC is granted exclusive use of the SAC logo, which appears alongside the International Laboratory Accreditation Cooperation (ILAC) mark for easier recognition cross-borders. An example of how it may look like is shown here.

Refer to SAC's website to browse through a comprehensive list of CABs and choose the most suitable accredited CAB for your company.

CASE STUDY 1

Ensuring Privacy: Navigating Personal Data Protection with Payboy

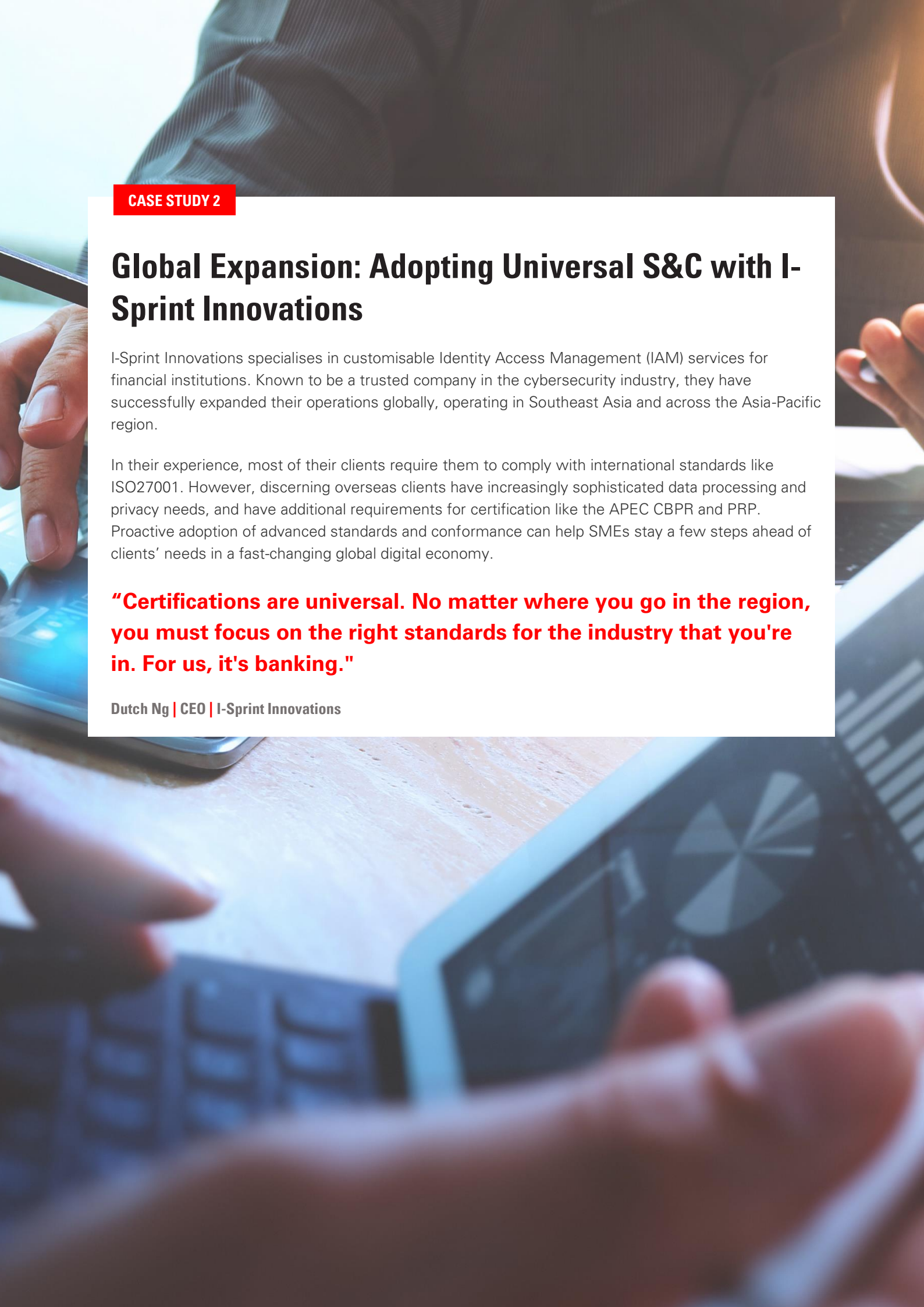
For Payboy, a software-as-a-service company which provides Human Resource Management systems, having strict processes in place to handle large amounts of personal data is one of their biggest priorities.

Adopting IMDA's Data Protection Trust Mark (DPTM) has made it easier to safeguard clients' data, benchmarked against industry standards.

Having the DPTM also enabled Payboy to assure their clients about the credibility of their services. This is a critical factor as Payboy engages a wide range of clients as they have faith that its processes have been verified to meet prevailing industry benchmarks and have peace of mind that their data is secure with Payboy.

"I believe all SMEs handling personal data on behalf of their customers should go through the DPTM certification to have peace of mind that their processes are in order and necessary safeguards are in place to prevent data incidents."

Nigel Lim | CEO | Payboy Pte. Ltd.



CASE STUDY 2

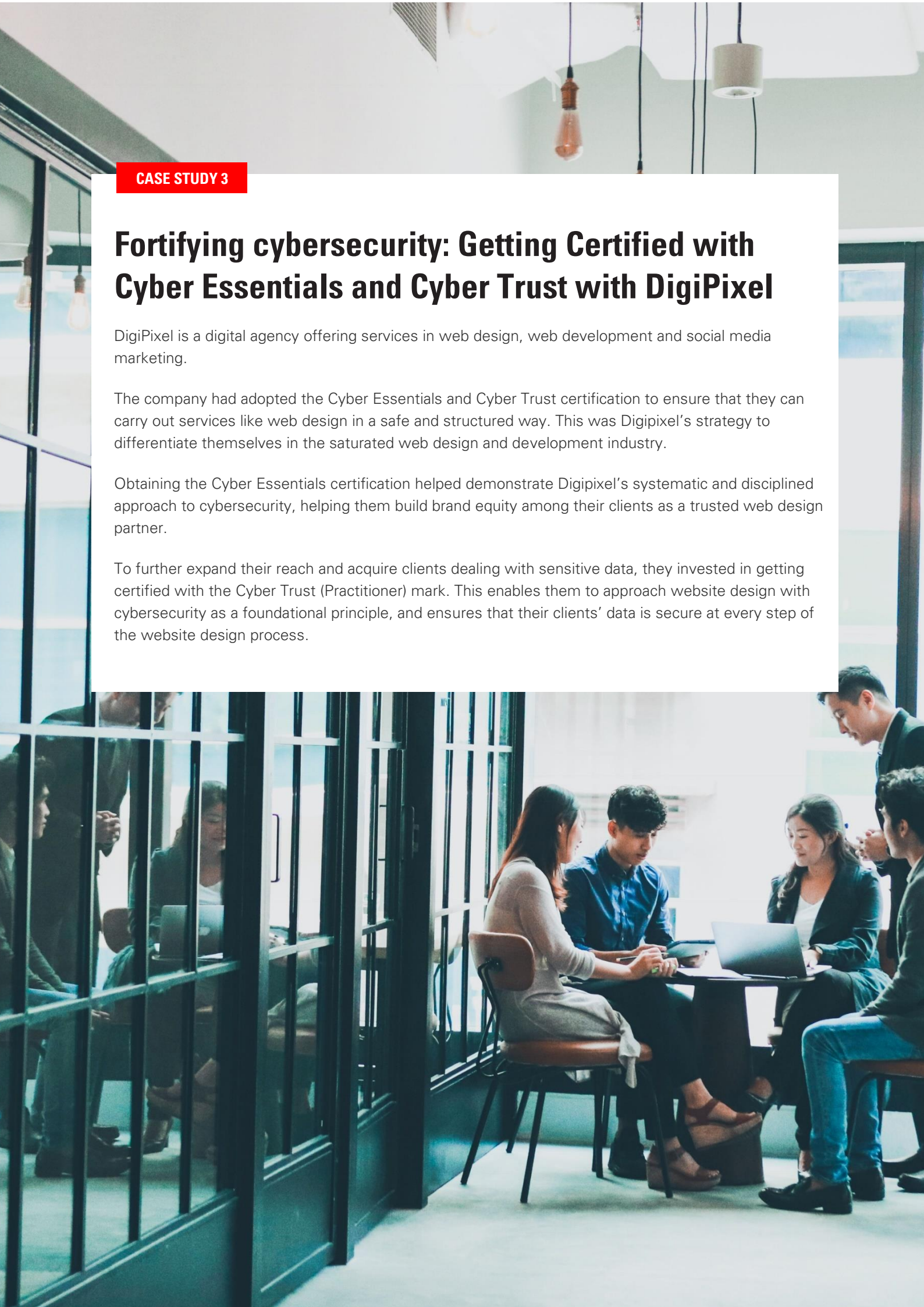
Global Expansion: Adopting Universal S&C with I-Sprint Innovations

I-Sprint Innovations specialises in customisable Identity Access Management (IAM) services for financial institutions. Known to be a trusted company in the cybersecurity industry, they have successfully expanded their operations globally, operating in Southeast Asia and across the Asia-Pacific region.

In their experience, most of their clients require them to comply with international standards like ISO27001. However, discerning overseas clients have increasingly sophisticated data processing and privacy needs, and have additional requirements for certification like the APEC CBPR and PRP. Proactive adoption of advanced standards and conformance can help SMEs stay a few steps ahead of clients' needs in a fast-changing global digital economy.

"Certifications are universal. No matter where you go in the region, you must focus on the right standards for the industry that you're in. For us, it's banking."

Dutch Ng | CEO | I-Sprint Innovations



CASE STUDY 3

Fortifying cybersecurity: Getting Certified with Cyber Essentials and Cyber Trust with DigiPixel

DigiPixel is a digital agency offering services in web design, web development and social media marketing.

The company had adopted the Cyber Essentials and Cyber Trust certification to ensure that they can carry out services like web design in a safe and structured way. This was Digipixel's strategy to differentiate themselves in the saturated web design and development industry.

Obtaining the Cyber Essentials certification helped demonstrate Digipixel's systematic and disciplined approach to cybersecurity, helping them build brand equity among their clients as a trusted web design partner.

To further expand their reach and acquire clients dealing with sensitive data, they invested in getting certified with the Cyber Trust (Practitioner) mark. This enables them to approach website design with cybersecurity as a foundational principle, and ensures that their clients' data is secure at every step of the website design process.

Connect with us today:

www.enterprisesg.gov.sg

GrowingEnterprises SG