

# ComplianceSuite™

# SALES PLAYBOOK

# Q&A

## For South African ASPs

*A Practical ASP Internal Guide to Selling ComplianceSuite™ All-in-One Bundle*

**Disclaimer:** This is a sales guide exclusively for authorised service providers (ASP) partners. None of the information contained herein is consider professional legal advice. Some of the information is based on South African POPIA and FSCA Joint Standards regulations, search results and information obtained through artificial intelligence. For specific legal advice, consult a compliance/legal expert.

**SMBsecure™**

## 1. Playbook Purpose

This sales playbook equips you to confidently position the **SMBsecure™ ComplianceSuite™ All-in-One** bundle to customers, handle common objections, guide pricing discussions, and close customer engagements consistently.

## 2. Ideal Customer Profile

SMBsecure ComplianceSuite is for organisations that:

- Must **operate at a defined protection standard**.
- Need to be **defensible under regulatory / supplier / client scrutiny**.
- Want **financial protection against cyber incidents**.
- Going for **ISO/IEC27001 certification**.
- Small Medical Practice desiring **ISO/IEC 27701:2025 certification** or **ISO27799 as recommended by the HPCSA**.
- **Cannot afford weak or inconsistent security controls**.

**ASP Tip!** *You're no longer just helping with compliance. You're providing a managed risk standard.*

### Prime Targets:

- Small to Medium Financial Service Providers (FSPs).
- Medical Practices.
- SMBs handling personal or sensitive data, including Legal, Professional Services, etc.
- Customers experiencing increased cybersecurity or JS/POPIA-related audit requests:
  - *Supply-chain questionnaire*
  - *Vendor audit / review*
  - *Instructive communication from regulatory body / association to comply*
- Micro enterprises with **1-3 Computer/Users (max)**, leveraging the low-cost **ComplianceSuite™ for MICRO ENTERPRISES** SKU (See RATE CARD for details).

## 3. Core Value Proposition

**A standardised, advanced cybersecurity and compliance protection solution bundle with built-in financial protection.**

- Fully managed All-in-One cybersecurity solution purpose-built for SMBs
- Supports JS and POPIA-aligned technical safeguards
- Simplifies POPIA and Joint Standard compliance through managed policies, controls, evidence, and audit readiness.
  - Move compliance from documents to **operational reality**.
  - Reduce regulatory risk, audit stress, and internal burden.

## Core Positioning Q&A:

### Q: What is ComplianceSuite?

- ComplianceSuite is our **All-in-One** managed cybersecurity and compliance enablement service designed for non-complex environment. It supports POPIA and regulatory requirements by combining technical controls, governance support, and ongoing reporting for provable “effective” compliance governance and controls.

### Q: Who is it designed for?

- Any non-complex organisation – like yours - that handles personal or sensitive data and must demonstrate compliance without building an enterprise security stack.

## 4. Conversation Framework

Discover -> Educate -> Position Risk -> Present Managed Outcome -> Close

**Open:** Explore client pressure around cybersecurity and compliance.

**Diagnose:** Identify gaps in current data security & compliance posture.

**Position:** Introduce ComplianceSuite as a solid “baseline” for compliance posture.

**Close:** Invite them to do a readiness check or basic compliance gap assessment.

### Your 5 Point Pitch Guidance:

1. Introduce ComplianceSuite as your managed compliance service for SMBs.
2. Explain why compliance has become complex and risky for small organisations.
  - *Compliance complexity, audit pressure, regulatory risk*
3. Position ComplianceSuite as an ongoing managed solution, not documents.
  - *ComplianceSuite as a managed service from you*
4. Reinforce the value of continuous governance and audit readiness.
  - *Ongoing assurance, evidence, governance*
5. Close by proposing a compliance readiness review or *quick check* as the next step.
  - *Conduct Compliance Readiness Review*

Your “Sales Language” **must shift** to:

- Risk transfer
- Insurability
- Regulatory defensibility
- Financial impact protection
- Stakeholder Trust and Confidence

## 5. Customer Pricing Conversation Guide

- Position pricing as a monthly managed governance service, **not a product.**
  - ✓ Affordable monthly compliance operating cost.
- Focus on risk reduction and compliance value, not per-feature cost.
  - ✓ Anchor value to regulatory exposure and audit readiness.
  - ✓ **Sell outcomes:** reduced risk, audit confidence, and executive oversight.
  - ✓ Avoid selling policies as once-off documents.
- Position as ongoing compliance assurance, not a once-off project.
  - ✓ Compare to cost of a breach or regulatory fine. **Give some real examples.**
  - ✓ Emphasise managed service and accountability.

### Pricing Justification Guidance:

How to Frame Price	How to Frame Value Delivery
Risk reduction vs tool cost	Ongoing management
Accountability and managed oversight	Compliance-aligned controls
Regulatory exposure avoidance	Reporting and evidence

**ASP Tip!** ComplianceSuite is your **All-in-One** package (*plus* your own-stack tools) and isn't a pick-and-mix toolset. **It's a managed compliance-ready security standard.**

## 6. Common Customer Objections & Responses - Q&A

**"We already have policies":** Policies alone do not equal compliance.

**"We don't have extra budget":** Non-compliance costs far more. Position as a compliance and governance requirement, not optional IT.

**"We are too small":** Regulations explicitly include small entities.

**"We already have security tools":** This complements and simplifies security governance delivery.

**"We don't want more user overhead":** SMBsecure is streamlined and managed for you.

**"We already have compliance documents":** ComplianceSuite ensures ongoing security governance, tracking, and evidence.

**"We already have antivirus and a firewall":** Antivirus and firewalls are important, but they don't address data encryption, secure email, user risk, or compliance reporting. ComplianceSuite closes those gaps.

*“We are too small to be a target”*: Most cyber incidents target SMBs because controls are weaker. Regulators also don’t exempt small firms from compliance obligations.

*“Compliance feels like paperwork”*: ComplianceSuite focuses on practical controls and evidence, not documents alone.

*“We don’t have much data, for now we just need basic security”*: ComplianceSuite delivers ongoing risk reduction, compliance alignment, reporting, and managed oversight for good governance - not just tools.

## Objection Handling By Type:

### Technical Objections

- We already have security tools > Tools do not equal compliance evidence.
- We have an outsource “IT guy” > Responsibility still sits with the business.

### Compliance Objections

- We passed our last audit > Audits are point-in-time.
- We’re too small > Regulations don’t scale down your obligations.

### Commercial Objections

- It’s too expensive for us > Compared to fines, incidents, remediation.  
*The Cyber Warranty alone can be more value than buying cyber insurance separately.*
- Budgets are tight > This is a monthly business compliance operating spend.

## 7. Proof Points to Reinforce Value

### “Managed Security + Compliance + Financial Protection”

- POPIA-aligned controls.
- Joint Standard readiness.
- Managed evidence and audit support.
- 50+ Controls addressable with ComplianceSuite alone.
- Built-in financial resilience if a breach or cybercrime incident occurs.

### Key Elements included for Governance, Risk & Compliance (GRC):

> POPIA readiness, JS alignment, policy management, risk tracking, financial safety.

## 8. Closing & Next Steps

Position the next step as a readiness review, *quick check*, or compliance gap assessment (If required. If prospect acknowledges gap, go for CLOSE = Add to MSA).

- Free DMARC Compliance check (quick check via smbsecure.co.za)
- Free External Risk Assessment (Scan)
  - Share the Company Questionnaire for Risk and Insurability Scoring
- Provide free copy of the “Best Practices Guide”
- POPI Check on Info Regulator eServices Portal or CIPC BizPortal
  - **This is also an important check to do for their Supply Chain!**

### **Remember!**

- ✓ Align stakeholders: IT (if required), compliance, and management.
- ✓ Confirm success criteria and onboarding steps.

### **ComplianceSuite Readiness – Customer Quick Probe:**

- ✓ **For any SMB:** Is your Info Officer registered? Do you have POPIA policies documented? Do you have evidence of Technical & Organisational Measures?
- ✓ **Additionally, for FSPs:** Are Joint Standards JS01 / JS02 documented?
- ✓ Are policies translated into actual technical controls?
- ✓ Do you maintain compliance evidence? Is it easily producible (quickly)?
- ✓ What is your current compliance & security governance posture?

### **CLOSE**

= **Subscription Green Light**

= **Agrees to quote**

= **Add to Managed Services Agreement**

## 9. ComplianceSuite Talking Points:

- ✓ Frame compliance as an ongoing managed service.
- ✓ Demonstrate policy, control, and evidence management.
- ✓ Close with onboarding and next steps.
- ✓ For FSPs remain focused on Joint Standards (JS01 & JS02), FAIS oversight, governance and audit readiness.
- ✓ For Healthcare remain focused on POPIA, patient data protection, operational risk and patient data breach prevention.
- ✓ For professional services (Legal, Property, Travel, etc) remain focused on POPIA, client data protection, operational risk and client data breach prevention.

## 10. Tools & Coverage

### What's included with ComplianceSuite?

Download and leverage the [ComplianceSuite Solution Map](#) from the website.

### **“Other” Crucial Components to Add/Include with Your Service Offering: (Not Included with ComplianceSuite)**

- + Backup
- + EDR & MDR
- + Password Manager, VPN
- + Spam Filtering, DNS Filtering, Log Management, Email Archiving
- + Patch & Software Update Management
- + SendGuard DLP (Contact CRS for details)

## ComplianceSuite – Annual Compliance Roadmap

*~ a 12-month compliance lifecycle with your new ComplianceSuite customer*

### **Q1: Baseline controls & policy alignment**

- *Encryption, MFA, basic review of risk assessments*
- *Basic reporting: Start to use Compliance Toolkit & ComplianceEZ®*

### **Q2: Rollout additional controls & training**

- Secure email, Phishing protection, review awareness training reports
- Review Risk Assessment reports and begin implementing remediations
- Consider gaps and additional security layers required
- Compliance reporting: Ramp up use of Compliance Toolkit & ComplianceEZ®
- Schedule QBRs

### **Q3: Evidence & remediation**

- Full rollout of ComplianceSuite
- Ensure other critical controls are in-place
- Governance reporting: Complete 70%+ of Toolkit and ComplianceEZ®
- Run QBR

### **Q4: Audit readiness, governance & reporting**

- Review reports and work towards “managed” compliance
- Complete 90%+ of Toolkit and ComplianceEZ®
- Maintain documentation for evidence support
- Run QBRs

## Accounting Practices

### The Context

You operate in a regulated environment overseen by the SAICA and already take compliance seriously.

### The Real Risk

The challenge is not intent or policy, but being able to demonstrate compliance quickly and confidently.

### The Solution

ComplianceSuite formalises existing practices and makes compliance provable for financial records, audit evidence, client data protection.

## Why Accounting Practices Choose ComplianceSuite

### Designed for Regulated Professionals

Built for practices regulated by the SAICA handling sensitive personal information.

### What It Solves

- ✓ Centralises compliance evidence.
- ✓ Reduces manual and paper-based processes.
- ✓ Provides audit-ready proof on demand.

### Why It Matters

- Supports Responsible Party accountability.
- Reduces regulatory and reputational risk.
- Works alongside existing IT providers.

## Estate Agents Practices

### The Context

You operate in a regulated environment overseen by the PPRA and already take compliance seriously.

### The Real Risk

The challenge is not intent or policy, but being able to demonstrate compliance quickly and confidently.

### The Solution

ComplianceSuite formalises existing practices and makes compliance provable for client identity data, transaction records, POPI accountability.

## Why Estate Agents Practices Choose ComplianceSuite

### Designed for Regulated Professionals

Built for practices regulated by the PPRA handling sensitive personal information.

### What It Solves

- ✓ Centralises compliance evidence.
- ✓ Reduces manual and paper-based processes.
- ✓ Provides audit-ready proof on demand.

### Why It Matters

- Supports Responsible Party accountability.
- Reduces regulatory and reputational risk.
- Works alongside existing IT providers.

## Financial Services Practices

### The Context

**You operate in a regulated environment overseen by the FSCA & PA and already take compliance seriously.**

### The Real Risk

The challenge is not intent or policy, but being able to demonstrate compliance quickly and confidently.

### The Solution

ComplianceSuite formalises existing practices and makes compliance provable for client financial data, financial advice records, governance, Joint Standards & POPIA accountability, FAIS oversight, and audit readiness.

## Why Financial Services Practices Choose ComplianceSuite

### Designed for Regulated Professionals

Built for practices regulated by the FSCA & PA handling sensitive personal information.

### What It Solves

- ✓ Centralises compliance evidence.
- ✓ Reduces manual and paper-based processes.
- ✓ Provides audit-ready proof on demand.

### Why It Matters

- Supports Responsible Party accountability.
- Reduces regulatory and reputational risk.
- Works alongside existing IT providers.

## Medical Practices & Doctors

### The Context

**You operate in a regulated environment overseen by the HPCSA and already take compliance seriously.**

### The Real Risk

The challenge is not intent or policy, but being able to demonstrate compliance quickly and confidently.

### The Solution

ComplianceSuite formalises existing practices and makes compliance provable for patient records, confidentiality, access control and accountability, breach prevention and operational risks.

## Why Medical Practices & Doctors Choose ComplianceSuite

### Designed for Regulated Professionals

Built for practices regulated by the HPCSA handling sensitive personal information.

### What It Solves

- ✓ Centralises compliance evidence.
- ✓ Reduces manual and paper-based processes.
- ✓ Provides audit-ready proof on demand.

### Why It Matters

- Supports Responsible Party accountability.
- Reduces regulatory and reputational risk.
- Works alongside existing IT providers.

**ComplianceSuite does not replace what you are doing today — it formalises it, secures it, and makes governance easy to demonstrate when required.**

## Legal Practices & Attorneys

### The Context

You operate in a regulated environment overseen by the Legal Practice Council and already take compliance seriously.

### The Real Risk

The challenge is not intent or policy, but being able to demonstrate compliance quickly and confidently.

### The Solution

ComplianceSuite formalises existing practices and makes compliance provable for client confidentiality, conveyancing records, Responsible Party accountability.

## Why Legal Practices & Attorneys Choose ComplianceSuite

### Designed for Regulated Professionals

Built for practices regulated by the Legal Practice Council handling sensitive personal information.

### What It Solves

- ✓ Centralises compliance evidence.
- ✓ Reduces manual and paper-based processes.
- ✓ Provides audit-ready proof on demand.

### Why It Matters

- Supports Responsible Party accountability.
- Reduces regulatory and reputational risk.
- Works alongside existing IT providers.

## Pitching and Selling to “Micro” Conveyancing Attorneys

Many small conveyancing practices in South Africa are actually Micro enterprises i.e. 1-3 computers users. This presents a massive opportunity to sell **ComplianceSuite for Micro Enterprises** as a low-cost solution for compliance and security governance.

The **Legal Practitioners Indemnity Insurance Fund (LPIIF)** has reported that since 2016, it has **rejected** over **210 cybercrime-related claims** worth approximately **R150 million** because **the firms failed to follow basic security protocols**.

**The LPIIF Master Policy generally excludes cybercrime-related theft. Firms must obtain standalone cyber liability insurance to cover data breaches and fraudulent transfers.**

**Note: ComplianceSuite Cyber Warranty only provides 1<sup>st</sup> party protection (our customer)**

## Overcoming The “Cost” Barrier

**Show real examples why investing in ComplianceSuite is far more cost-effective compared to the COSTS of dealing with a breach and/or fighting cyber-crime cases.**

Cybercrime targeting conveyancing attorneys in South Africa has surged, primarily through **Business Email Compromise (BEC)**, where fraudsters intercept communications to divert property sale proceeds.

## Specific examples of law firms involved in high-profile cybercrime cases include:

- **ENS (Edward Nathan Sonnenbergs Inc.):** In a landmark case, a property purchaser, Judith Hawarden, paid **R5.5 million** into a fraudulent account after an email from an ENS conveyancing secretary was intercepted and altered by hackers. While the High Court initially found ENS negligent for using insecure email, the [Supreme Court of Appeal \(SCA\)](#) overturned this in 2024, finding that the firm could not be held liable for the purchaser's failure to verify banking details.
- **Van der Spuy & De Jongh Inc.:** This Pretoria-based firm was found negligent by the High Court after paying **R1.7 million** of a client's funds into a fake account. Hackers had hijacked the client's email and sent "new bank details" to the firm, which the attorneys followed without verification.
- **Gavin Hartog:** A Johannesburg conveyancer was held liable for **R1.4 million** after fraudsters intercepted emails between him and the property sellers. The court rejected his argument that there was a "tacit term" requiring the clients to ensure their own email security, ruling that the attorney had a mandate to ensure the money reached the correct parties.

## Why This Matters?

- Demonstrates that legal costs outstrip the costs for implementing ComplianceSuite.
- Provides validated examples of negligence and non-compliance cases.
- Proof that conveyancing firms are real target for cybercrimes, especially BEC.
- LPIIF (generally) do not cover any cyber incidents. Firms need separate cover.

## ComplianceSuite Specific Measures to Help Reduce BEC:

- 1) Secure PDF Email Encryption for sensitive correspondence
- 2) Computer access control, MFA and Automated Risk Response
- 3) Ongoing Awareness Training and SCAM Insights
- 4) FREE **Check4Phish** service
- 5) M365 / Google Workspace account security monitoring
- 6) Browser Passwords review and improvement
- 7) Dark Web exposed data monitoring
- 8) Managed DMARC & domain typosquatting monitoring
- 9) Managed MTA-STS (enforced use of TLS encryption)
- 10) Cyber Warranty for the customer's own protection i.e. data breach related expenses and up to R250K reimbursement of funds for BEC (to them only NOT for 3<sup>rd</sup> parties)

## LAW SOCIETY OF SOUTH AFRICA REFERENCE:

Guide your customer to stay compliant with the **Protection of Personal Information Act (POPIA)** and mitigate Business Email Compromise (BEC) risks. The Law Society of South Africa (LSSA) and the [Information Regulator](#) recommend the following multi-layered protocols:

### 1. Administrative & Legal Requirements (POPIA)

- **Information Officer (IO):** Formally appoint and register an Information Officer with the Information Regulator. **Legally, a firm cannot process PI without doing this.**
- **Data Mapping:** Conduct a comprehensive audit to identify what personal information you collect, where it is stored, and who has access.
- **Impact Assessments:** Perform regular **Personal Information Impact Assessments** to identify security vulnerabilities in your data processing workflows.
- **Breach Response:** Develop a formal **Incident Response Plan** that includes mandatory timelines for notifying the Regulator and affected clients in the event of a breach.

### 2. Technical Security Safeguards

- **Multi-Factor Authentication (MFA):** Enforce MFA on all firm systems, particularly email and banking portals, to prevent "silent monitoring" by hackers.
- **Encryption:** **Use email encryption for sensitive information and ensure all company devices (laptops, mobile phones, USB sticks) are encrypted.**
- **Secure Infrastructure:** Use **Virtual Private Networks (VPNs)** for remote work and avoid free web-based email accounts (like Gmail or Yahoo) for professional communication.
- **Automatic Updates:** Enable automatic daily patching for operating systems and antivirus software to close known security gaps.

### 3. Conveyancing-Specific Payment Protocols

- **Encrypt Correspondence:** Ensure correspondence to clients which contain any payment information is encryption using a password to prevent unauthorised access.
- **Telephonic Verification:** Never process a payment or change banking details based on an email alone. Always verify details via a **trusted phone number** (not the one in the suspicious email).
- **Public Beneficiary Status:** Register your firm's trust account as a [Public Beneficiary](#) with major banks so clients don't have to manually enter account details.
- **Standard Advisory Wording:** Include [LSSA-recommended warnings](#) at the beginning of all client communications stating that the firm will **never** change bank details via email.

- **Test Deposits:** For high-value transfers, perform a small test deposit first and confirm receipt before sending the full amount.

#### 4. Human Factor & Training

- **Continuous Awareness:** Staff training is not a once-off event; regular workshops on identifying **phishing** and **spoofing** are essential to maintain a "culture of security".
- **Device Management:** Prohibit staff from plugging unverified personal devices or memory sticks into the firm's network. Having locks (access controls) on devices.

Provide the below as **free guidance** to your prospects and once on-boarded, setup a firm-wide email signature for users to include these recommended disclaimers. **To align with the Law Society of South Africa (LSSA) guidelines, your firm should place this warning at the top of emails and include it in your initial mandate/engagement letter.**

##### 1. Email Footer/Header Disclaimer

"**URGENT SECURITY WARNING:** Please be advised that [Firm Name] will **never** send an email or any other electronic communication notifying you of a change in our banking details. Our banking details will remain as provided in our initial signed mandate. Should you receive any communication suggesting a change in banking details, please **do not** make any payment and contact us immediately via a trusted telephone number to verify the authenticity of the message."

##### 2. Mandate/Letter of Engagement Clause

"The parties acknowledge the prevalence of **Business Email Compromise (BEC)**. [Firm Name] shall not be held liable for any loss arising from funds being paid into a fraudulent bank account as a result of intercepted or spoofed emails. The client is specifically instructed to **telephonically verify** our trust account details with the handling attorney before making any electronic transfer, especially if those details appear to have changed."

##### 3. POPIA-Specific Disclaimer

"This email and any attachments are confidential and intended solely for the addressee. The processing of personal information contained herein is subject to our [Privacy Policy](URL to your firm's website), in compliance with the **Protection of Personal Information Act (POPIA)**. If you are not the intended recipient, any disclosure, copying, or distribution is prohibited and may be unlawful."

**ASP Tip To Attorneys:** Following the *ENS v Hawarden* ruling, it is vital to ensure your **engagement letter** explicitly states that the client bears the risk of verifying bank details. Here is a template for your use:

## Client Awareness Letter: Protection Against Cybercrime

**Subject: URGENT: Mandatory Security Procedures for Your Property Transaction**

Dear **[Client Name]**,

As we proceed with your property transaction, we must bring to your attention the significant increase in **Business Email Compromise (BEC)** targeting conveyancing firms in South Africa.

Cybercriminals often intercept emails and substitute legitimate banking details with their own. To protect your funds and ensure compliance with our security protocols, please strictly adhere to the following:

### 1. No Change in Banking Details

Please be advised that **[Firm Name]** will **never** notify you of a change in our banking details via email, WhatsApp, or SMS. Any communication suggesting such a change should be treated as fraudulent.

### 2. Mandatory Telephonic Verification

Before making **any** electronic transfer to our trust account, you are required to call our offices at **[Insert Landline Number]** to verbally verify the account number with the attorney or paralegal handling your matter.

**Warning:** Do not use any telephone numbers provided in a suspicious email, as these may also be fraudulent.

### 3. Verification of Identity (FICA & POPIA)

In accordance with the **Financial Intelligence Centre Act (FICA)** and the **Protection of Personal Information Act (POPIA)**, we will only process your personal information for the purposes of this transaction. We have implemented reasonable technical measures to secure our systems, but we urge you to ensure your own email account is secured with **Multi-Factor Authentication (MFA)**.

### 4. Public Beneficiary Status

For your added safety, **[Firm Name]** is registered as a **Public Beneficiary** with [Bank Names, e.g., Standard Bank/FNB]. We recommend selecting us from your bank's pre-loaded beneficiary list rather than manually entering our details.

### Acknowledgment of Risk

By proceeding with this transaction, you acknowledge that you have been warned of the risks of cybercrime. Failure to follow the verification steps above may result in the loss of funds for which the firm cannot be held liable.

Yours sincerely,

**[Attorney Name/Firm Partner]**

**[Firm Name]**