BUILDING THE FOUNDATION FOR SCALE

From Startup Chaos to Enterprise-Ready: Forging Governance & Vendor Trust for a High-Growth Fintech

A Southeast Asian fintech startup with ~50 employees, scaling rapidly into North American markets. The company has a strong product and growing demand from global financial institutions—but no formal security function to support enterprise expectations. Enter STP One.

CASE STUDY

THE ONE STP

WE FORGE CYBERARMORY & PARTNERSHIPS

THE CHALLENGE

The Maturity Gap

The fintech had outgrown informal security practices but wasn't ready to staff a full internal security team. Governance consisted of ad-hoc policies, there was no structured third-party risk oversight, and the team struggled to respond to complex security and vendor risk questionnaires from enterprise prospects.

As a result, deals were slowing—or stalling entirely—during due diligence.

THE ONE STP
WE FORGE CYBERARMORY & PARTNERSHIPS

STPFORGE SOLUTION

STP engaged as fractional security leadership, implementing the STPFORGE framework to establish governance, clarity, and scalable trust, using the NIST Cybersecurity Framework as a tailored foundation aligned to the fintech's assessed risk profile.

Strategic Governance Foundation

We conducted a risk-based assessment focused on the client's actual business model, growth plans, and regulatory exposure—moving beyond generic templates. This resulted in:

- A clear governance and compliance roadmap aligned to PDPA and global standards
- Audit-ready policies designed for real-world adoption, not shelfware
- Defined ownership and oversight through a lightweight security steering structure

THE ONE STP
WE FORGE CYBERARMORY & PARTNERSHIPS

Third-Party Risk Management (TPRM)

To address vendor and supply-chain exposure, STP implemented a continuous TPRM program.

- Vendor tiering based on data sensitivity and operational impact
- Ongoing monitoring to replace static, annual questionnaires
- Embedded risk checks into procurement workflows to assess vendors before contracts were signed

Fig. 1 National Institute of Standards and Technology (NIST) Cybersecurity Framework Diagram

IDENTIFY

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT

- Access Control
- Awareness & Training
- Data Security
- Information Protection Processes & Procedures
- Maintenance

DETECT

- Anomalies & Events
- Ongoing Security Monitoring
- Detection Processes

RESPOND

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recovery Planning
- Communications
- Improvements

THE ONE STP

WE FORGE CYBERARMORY & PARTNERSHIPS

THE RESULTS

Built to Lead & Scale

- **Faster Sales Cycles**
  The sales team now provides a standardized security overview and completed governance package, reducing security review timelines by weeks.

- **Board-Level Visibility**
  Leadership gained a clear, measurable view of security posture and third-party risk—replacing uncertainty with informed decision-making.

- **Enterprise Readiness**
  The company successfully onboarded its first Fortune 500 client, passing a rigorous third-party audit that would not have been achievable six months earlier.

- **Sustainable Scale**
  Security became part of day-to-day operations, enabling growth without adding fragility or overhead.

THE ONE STP
WE FORGE CYBERARMORY & PARTNERSHIPS


The One STP
+1 669 254 8023
+66 08 1824 8911
connect@theonestp.com
theonestp.com
THE ONE STP
WE FORGE CYBERARMORY & PARTNERSHIPS