# Moving MoveSynch

A proposal for building tomorrow's security

By: Matin Aliyev (presenter) Lakshmi Priya Kumar Sinduja Mullangi Deyuan Huang Bo Fu Shimei Meng

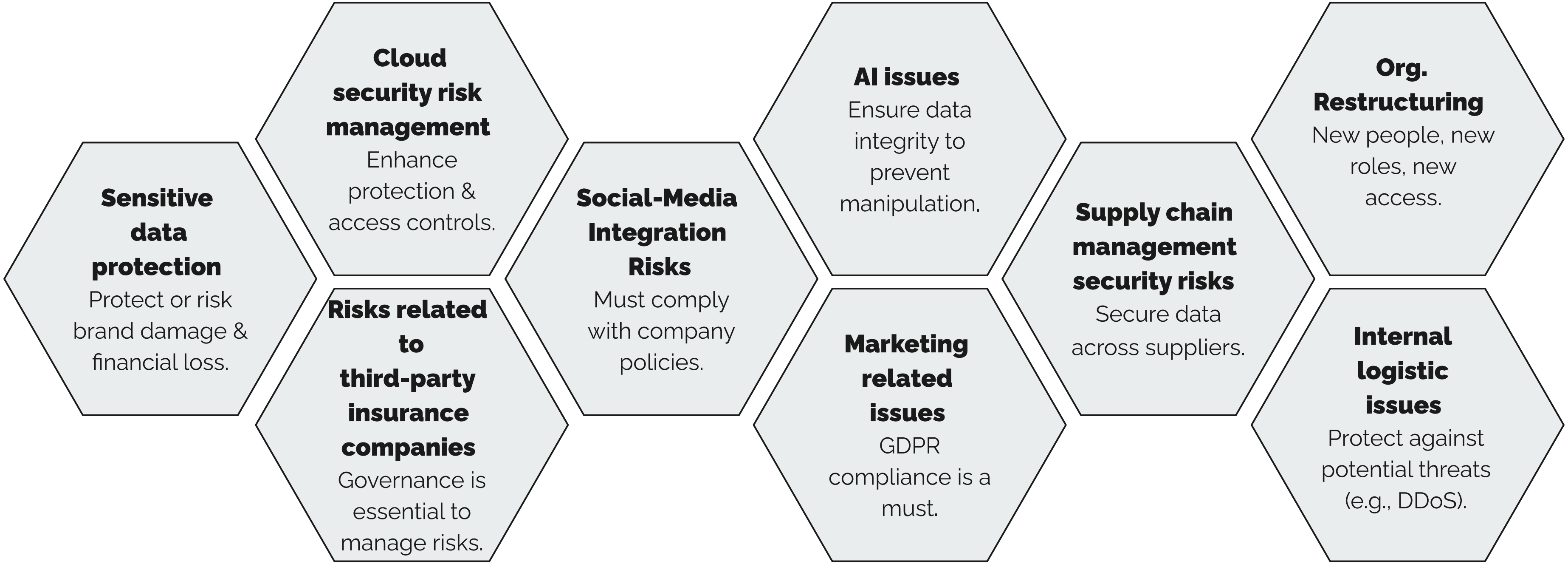
## Our plans

- 🏥 Health technology pioneer
- 🛠️ Expanding with cutting-edge features
- Customizable health plans
- 🌐 Social media integration for engagement
- 🤖 AI for a competitive edge
- 💸 Optimized operations via low-cost supply chains
- 📈 Enhanced marketing strategies

## What we need

- 🔒 **Protect user data** by ensuring confidentiality, integrity, and availability.
- ⚠️ **Effective risk management** at every level.
- 🤝 **Business alignment** driven by leadership support.
- 🏫 Foster a **security-aware culture** organization-wide.
- 🔁 **Continuous monitoring** and learning to adapt

# Areas of Concern



**Sensitive data protection** Protect or risk brand damage & financial loss.

**Cloud security risk management** Enhance protection & access controls.

**Risks related to third-party insurance companies** Governance is essential to manage risks.

**Social-Media Integration Risks** Must comply with company policies.

**AI issues** Ensure data integrity to prevent manipulation.

**Marketing related issues** GDPR compliance is a must.

**Supply chain management security risks** Secure data across suppliers.

**Org. Restructuring** New people, new roles, new access.

**Internal logistic issues** Protect against potential threats (e.g., DDoS).

# The Solution: ISO27001

### PROTECTION MEASURES

Builds resilience to protect sensitive data, especially when involving third parties.

### RISK MANAGEMENT

Identify and address problem areas to comply with regulations and ensure business continuity.

### CERTIFICATION

Enhance our brand reputation and help attract top talent.

### OPERATIONAL EFFICIENCY

Optimize and standardize workflows to minimize risks and reduce costs.

# Road to compliance: Establishing Leadership

Why is it needed?

- ↪ Leaders guide the journey.
- ↪ Convince and align everyone on the need for ISO.

How will it be controlled?

- ↪ Set policies and delegate tasks for clear execution.
- ↪ Create an environment conducive to achieving goals.
- ↪ Establish communication channels for smooth progress.
- ↪ Engage everyone to ensure compliance across the board.

# Road to compliance: Risk Assessment & Management

### Why is it needed?

- Overall process of risk identification, risk analysis and risk evaluation
- Culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects
- Drives informed decisions, efficiency, and reputation!

### How will it be controlled?

- Establish context
- Identity risks
- Analysis risks
- Evaluate risks
- Treat risks

# Road to compliance: Operations Planning & Security

Why is it needed?

- ↪ Minimize the impact of changes.

How will it be controlled?

- ↪ Establish process guidelines.
- ↪ Provide documented information.
- ↪ Approve, document and control changes.
- ↪ Monitor resources and predict their usage.
- ↪ Review unintended changes and take action if necessary.
- ↪ Control interactions with external organizations.
- ↪ Conduct regular information security risk assessment.

# Road to compliance: Organisational Structure

Why is it needed?

- ↪ Maintain information security during company expansion.

How will it be controlled?

- ↪ Define and assign roles, responsibilities, and authorities.
- ↪ Be clear about expectations.
- ↪ Ensure that all personnel comply with information security policies and procedures.
- ↪ Implement access control.

# Road to compliance: Regulatory Compliance

Why is it needed?

- Organization’s adherence to laws, regulations, guidelines, and specifications relevant to its business processes
- Avoiding illegality and penalties
- Building trust and improve user satisfaction
- Enhancing data security

How will it be controlled?

- Build consent management
- Build data review mechanism
- Build data breach Response Plan
- Enhance employee training and awareness
- Enhance third-party management

# Road to compliance: Human Resource Security

Why is it needed?

- ↪ Reduce human-caused information security risks.

How will it be controlled?

- ↪ Ensure that personnel fit their roles.
- ↪ Ensure understanding of policy, responsibilities & consequences of non-compliance.
- ↪ Ensure personnel have the necessary competencies.
- ↪ Safety training.
- ↪ Document the above processes.

# Road to compliance: Communication Management

Why is it needed?

- ↪ Processes and protocols to ensure effective communication regarding information security within an organization
- ↪ Strategy that will be used to mitigate possible key issues
- ↪ Supervise our security management system
- ↪ Drives operational efficiency, trust and transparency!

How will it be controlled?

- ↪ Internal communication
  - ○ Security Awareness Training
  - ○ Regular updates and audit
- ↪ External communication
  - ○ Customer notifications
  - ○ Third-Party Communication

# Road to compliance: Documentation

Why is it needed?

- The documentation is an important source of information required to record appropriate policies
- Strategy that will be used to mitigate possible key issues
- To supervise the security management system of MoveSynch

How will it be controlled?

- Access Control
- Documentation Storage
- Loss Prevention

# Program logistics: Cost Estimation

| Cost Component | Estimated Cost (AUD) | Notes |
|---|---|---|
| 1. Consultation and Initial Audit | $50,000 | Hire professional external auditors to evaluate gaps and risks. |
| 2. Implementation (Tools/Tech) | $150,000 | Firewalls, encryption, SIEM, cloud security. |
| 3. Employee Training | $30,000 | Yearly security awareness and targeted training. |
| 4. Software Licensing | $100,000 | Endpoint security, DLP, and vulnerability scanning. |
| 5. Compliance Audits | $40,000/year | Ongoing audits for ISO 27001 and GDPR. |
| 6. Personnel Costs | $250,000/year | IT auditors, security analysts, and CISOs. |
| 7. Insurance Premiums | $20,000/year | Covering for cyber liability. |
| **Total** | **$640,000** | **Annual cost may vary by implementation.** |

# Program logistics: Scheduling

**PHASE 1**
Initial Planning and Consultation (Month 1-2)

- ○ Risk Assessment and Gap Analysis
- ○ Strategy Development

**PHASE 2**
Implementation of Security Controls (Month 3-6)

- ○ Technical Controls
- ○ Employee Training
- ○ Policy Development

**PHASE 3**
Compliance and Auditing (Month 6-8)

- ○ Internal Audit
- ○ External Certification

**PHASE 4**
Monitoring and Continuous Improvement (Month 9-12)

- ○ Monitoring Systems
- ○ Security Reviews
- ○ Ongoing Training

# Program logistics: Monitoring

Why is it needed?

- To keep track of the performance of the ISMS
- To detect risks and vulnerabilities

How will it be controlled?

- Internal Audit Programme
- Key Performance Indicators
  - Incident Response Time/ Frequency
  - Risk Management
  - Business Process Assurance
  - Continuous Improvement

# References

Down, B. (2019). Breaking down ISO 27001 certification costs. @NordLayer.

https://nordlayer.com/learn/iso/iso-27001-cost/

International Organization for Standardization. (2023). ISO/IEC 27001:2023 Information security, cybersecurity and privacy protection — Information security management systems — Requirements . Retrieved from British Standards Online Via The University of Sydney Library.

Martinez, J. (2024). How Much Does ISO 27001 Certification Cost in 2024? Strongdm.com; StrongDM, Inc.

https://www.strongdm.com/blog/iso-27001-certification-cost

# Thank you!