Where next?

Information Security Strategy: Transitioning from alignment to integration helps organisations understand what ISF Members are doing to bring about an information security strategy that adds real value to the business. This includes presenting what ‘good practice’ looks like, and highlighting successful techniques already implemented in Member organisations.

Two further factors were identified that will help assure a successful transition towards strategy integration:

1. Don’t forget business as usual: A key enabler to doing this is for the information security function to have the necessary credibility. This involves delivering business initiatives as well as staying on top of the day-to-day responsibilities of the job.

2. Treat integration as a continuum: This is an evolutionary not a revolutionary process. Those who do not have the requisite capabilities, credibility, and foresight to begin transitioning from alignment to integration should start planning now. A failure to do so will put the organisation firmly behind the curve.

The report is supported by an implementation space on the ISF Member website, ISF Live, which contains a facilitated forum for Members to discuss related issues and solutions.

The Information Security Strategy: Transitioning from alignment to integration report is available free of charge to ISF Members, and can be downloaded from the ISF Member website www.isflive.org. Non-Members can purchase the report by contacting Steve Durbin at steve.durbin@securityforum.org

Contact
For more information, please contact:
Steve Durbin, Managing Director
US Tel: +1 (347) 767 6772
UK Tel: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953 800
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

About the ISF
Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

Disclaimer
This document has been published to provide general information only. It is not intended to provide advice of any kind. Neither the Information Security Forum nor the Information Security Forum Limited accept any responsibility for the consequences of any use you make of the information contained in this document.

Reference: ISF 14 06 05 Copyright © 2014 Information Security Forum Limited. All rights reserved. Classification: Public, no restrictions

Information Security Strategy
Transitioning from alignment to integration

The digital landscape offers unparalleled opportunities for every organisation to build a strategy around innovative services and products. As information is fundamental to seizing these opportunities, the door is now wide open for the Chief Information Security Officer (CISO) to play a key role in the definition and execution of the organisation’s business strategy.

In recent years, the CISO in many organisations has focused on aligning the information security function’s strategy to that of the business. However, that is no longer enough: the business’s growing reliance on cyberspace has placed a demand on the CISO to define and execute an information security strategy that goes even further. A transition to integration is now vital for the information security function to deliver what the business needs.

As an organisation’s reliance on information security will only continue to increase, the time has never been better for information security to add the maximum possible value by forging close links with the core business and tying itself tightly into key business processes, strategy in particular. The CISO or equivalent should therefore make use of this unique situation to enhance their contribution by ensuring their function meets or surpasses the strategic expectations of their organisation.

The ISF Report Information Security Strategy: Transitioning from alignment to integration looks forward over the next two to three years, taking the key lessons learned from leading organisations and painting a picture of how the transition to integration may look for the majority of ISF Members.

The Report examines three concepts that form a ‘virtuous circle’, feeding off each other to help drive home an integrated information security strategy:

• Engagement: where the information security function is close to the core business and adequately represented at key decision-making forums;

• Anticipation: able to identify changes to the business and threat landscape that could jeopardise or enhance the chance of business success; and

• Resilience: to recognise that it is impossible to defend against every attack, but that planning and preparation can reduce the potential impact.
Transitioning from alignment to integration – The ISF Approach

The ISF Approach

The ISF’s Approach to an Integrated Information Security Strategy (IISS), shown below, is loosely modelled on Kaplan and Norton’s ‘Closed-Loop Management System’. Each step includes key activities that the CISO should undertake in each stage, supplemented with advice from leading ISF Members on approaches they took on their path towards integration.

#### Step | Key Activities
--- | ---
A. DEFINE | Producing detailed project plans that deliver the strategy ‘on the ground’
A.1 | Understand the business context
A.2 | Understand the information security context
A.3 | Define the information security function’s mission, vision and objectives with the business
A.4 | Prioritise and sequence objectives
A.5 | Define success criteria in line with the accepted governance model
B. EXECUTE | Maintaining concentration on execution as part of the wider business strategy, for which information security plays a key role – but not all key roles
B.1 | Define and execute the Operations Plan
B.2 | Ensure information security activities enable the business
C. MONITOR | Keeping a finger on the pulse of the strategy execution at all times
C.1 | Leverage the stakeholder feedback loop
C.2 | Measure progress against objectives
C.3 | Ensure strategic objectives remain valid and in line with business needs
D. ADJUST | Deciding on the level of analysis required and selecting the appropriate solution
D.1 | Ensure strategic objectives remain valid and in line with business needs
D.2 | Communicate the value

Concepts that underpin an integrated information security strategy

The ISF Approach is supported by an explanation of the attributes associated with an information security strategy that is aligned with the business – as opposed to one that is integrated, as shown below.

| When the information security strategy is... | Aligned | Integrated |
--- | --- | ---
Posture | Passive: reacts to developments, Takes direction from senior management and business units; works in a silo, Bolts on information security to existing projects | Active: anticipates and helps shape the future of the organisation, Collaborates with senior management and business units, Builds projects securely |
Direction | Derives its objectives from the business strategy | Is part of the process and therefore informs and is ‘bought in’ |
Representation | Liaises with business leaders to gain an understanding of how it can help, At best, on the fringes of the business’s governance model | Is represented when the business strategy is defined, Embedded within the business’s governance model |

The Report also outlines the typical behavioral change that a CISO is likely to exhibit along the journey towards integration, summarised below.

| Concept | Change | Starting the transition | During the transition | Closing in on integration |
--- | --- | --- | --- | ---
Engagement | Regular feedback from the business | Most feedback comes from self-assessments; possibly backed with limited feedback from the business | Feedback becomes more regular and formal as a closer working relationship is established with senior management | Feedback comes through a continual process as the CISO and information security attain trusted advisor status |
Anticipation | Timing of the production of the information security strategy | Information security strategy is produced after the business strategy is complete | Elements of the information security strategy are prepared as the business strategy develops | The information security strategy is produced in parallel with the business strategy |
Resilience | Delivery of individual projects | Information security input, advice and guidance is sought after projects have passed through their start-up phase | Liaison with business representatives helps ensure information security becomes involved in the start-up process | Information security involvement is sought out from the outset of each relevant project |
About the ISF

Founded in 1996, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

Disclaimer

This document has been published to provide general information only. It is not intended to provide advice of any kind. Neither the Information Security Forum nor the Information Security Forum Limited accept any responsibility for the consequences of any use you make of the information contained in this document.

Where next?

The Information Security Strategy: Transitioning from alignment to integration helps organisations understand what ISF Members are doing to bring about an information security strategy that adds real value to the business. This includes presenting what ‘good practice’ looks like, and highlighting successful techniques already implemented in Member organisations.

Two further factors were identified that will help assure a successful transition towards strategy integration:

1. Don’t forget business as usual: A key enabler to doing this is for the information security function to have the necessary credibility. This involves delivering business initiatives as well as staying on top of the day-to-day responsibilities of the job.

2. Treat integration as a continuum: This is an evolutionary not a revolutionary process. Those who do not have the requisite capabilities, credibility, and foresight to begin transitioning from alignment to integration should start planning now. A failure to do so will put the organisation firmly behind the curve.

The report is supported by an implementation space on the ISF Member website, ISF Live, which contains a facilitated forum for Members to discuss related issues and solutions.

The Information Security Strategy: Transitioning from alignment to integration report is available free of charge to ISF Members, and can be downloaded from the ISF Member website www.isflive.org. Non-Members can purchase the report by contacting Steve Durbin at steve.durbin@securityforum.org

Information Security Strategy

Transitioning from alignment to integration

The digital landscape offers unparalleled opportunities for every organisation to build a strategy around innovative services and products. As information is fundamental to seizing these opportunities, the door is now wide open for the Chief Information Security Officer (CISO) to play a key role in the definition and execution of the organisation’s business strategy.

In recent years, the CISO in many organisations has focused on aligning the information security function’s strategy to that of the business. However, that is no longer enough: the business’s growing reliance on cyberspace has placed a demand on the CISO to define and execute an information security strategy that goes even further. A transition to integration is now vital for the information security function to deliver what the business needs.

As an organisation’s reliance on information security will only continue to increase, the time has never been better for information security to add the maximum possible value by forging close links with the core business and tying itself tightly into key business processes, strategy in particular. The CISO or equivalent should therefore make use of this unique situation to enhance their contribution by ensuring their function meets or surpasses the strategic expectations of their organisation.

The ISF Report Information Security Strategy: Transitioning from alignment to integration looks forward over the next two to three years, taking the key lessons learned from leading organisations and painting a picture of how the transition to integration may look for the majority of ISF Members.

The Report examines three concepts that form a ‘virtuous circle’, feeding off each other to help drive home an integrated information security strategy:

• Engagement: where the information security function is close to the core business and adequately represented at key decision-making forums;

• Anticipation: able to identify changes to the business and threat landscape that could jeopardise or enhance the chance of business success; and

• Resilience: to recognise that it is impossible to defend against every attack, but that planning and preparation can reduce the potential impact.

Contact

For more information, please contact:
Steve Durbin, Managing Director
US Tel: +1 (347) 767 6772
UK Tel: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953 800
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

Reference: ISF 14 06 05 Copyright © 2014 Information Security Forum Limited. All rights reserved. Classification: Public, no restrictions