Actions

Where next?
The Federated Identity and Access Management: Creating a connected world report—available from the ISF website—provides an overview of the challenges and solutions related to implementation of FIAM. It also sets out approaches for developing a FIAM programme and managing new FIAM connections.

The report is supplemented by the Federated Identity and Access Management: Implementation toolkit—available exclusively to ISF Members. The toolkit helps organisations implement the recommendations of the main report. It provides resources to help organisations develop a FIAM programme, manage new FIAM connections, check the security arrangements of service providers, and create and support the business case for FIAM.

The report and toolkit are supported by an implementation space on the ISF Member website. This space provides a facilitated forum for ISF Members to discuss FIAM-related issues and solutions, along with a central pool of additional resources including a checklist tool, webcasts and presentations.

Input for the report was gathered from analysis by an ISF Principal Analyst, discussions at global ISF development workshops, detailed Member expert interviews, vendor interviews, Member case studies and recommendations from related ISF research projects.

About the ISF
Founded in 1989, the Information Security Forum 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 information security and 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 program. 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.

Contacts
For further information contact:
Steve Durbin
UK Tel: +44 (0)20 7213 3745
US Tel: +1 (347) 767 6772
Fax: +44(0)20 7213 4813
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

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 11 FIAM Marketing Copyright © 2011 Information Security Forum Limited. All rights reserved. Classification: Public, no restrictions.

Federated Identity and Access Management

Creating a connected world

Federated Identity and Access Management (FIAM) enables seamless, secure access to multiple external systems—revolutionising the ways organisations interconnect with customers and suppliers.

FIAM allows an organisation to manage employees’ access to multiple external systems centrally, without the need to do so in each external system. Security is increased, costs are reduced, and the user experience improves.

To operate in today’s connected world, organisations need secure access to a variety of systems. Suppliers, customers, shared service centres and strategic partners operate numerous business applications: payroll, inventory and parts management, employee travel, service orders and client relationship management (CRM) to name a few.

As organisations increasingly turn to other parties—including cloud service providers—to deliver an even-greater number of services, FIAM is growing in importance. FIAM can also be useful in organisations that operate a federated organisational structure, or during reorganisations, mergers or acquisitions, when it can provide an alternative to expensive systems integration.

Most organisations will focus on outbound FIAM connections, defined as those where their staff are given access to systems provided by other parties. Organisations that provide outsourced or cloud-based applications can gain competitive advantage by developing inbound connections for their customers.

FIAM introduces significant business risks when not adopted securely, so the Information Security Forum has launched Federated Identity and Access Management: Creating a connected world. This practical, business-focused report provides detailed guidance and good practices for working with business and technical teams to implement FIAM securely and effectively, for both outbound and inbound connections.
Developing a FIAM programme

Core to the recommendations contained in the ISF report is the development of a strategic programme for adopting Federated Identity and Access Management (FIAM) securely and effectively. The approach comprises a series of steps that should be performed at an organisational level, with an embedded process for managing the lifecycle of each FIAM connection, as illustrated here.

A Build a business case for FIAM
To succeed, any FIAM project must have the full backing of the business. This step identifies the activities needed to create a strong business case for FIAM, including examining the benefits and risks, and how to reach a decision on its adoption.

B Determine the scope of the FIAM programme
Organisations need to determine how far-reaching their FIAM programme will be, which will depend on the desired applications and the suitability of existing IT systems. Activities include specifying suitable business applications ensuring target applications will support FIAM and assessing the impact of related business and IT activities.

C Establish a governance framework for FIAM
Establish a governance framework for FIAM that will ensure any decisions are aligned with corporate policies and are in the interest of the business. Steps include appointing a business manager to oversee the programme and creating an approval board.

D Define a set of technical FIAM standards
Organisations need to define a set of security-related technical requirements and standards when establishing FIAM connections. These include unique user identifiers, policy for user attributes, FIAM protocols and certificate policy for federated connections.

E Run a FIAM pilot
In order to prove the benefits of a FIAM solution, identify any security weaknesses and confirm an approach for wider deployment, organisations should run a pilot FIAM project. Activities include selecting a FIAM software supplier and running a pilot FIAM project.

F Integrate FIAM into existing IAM systems and general IT processes
Organisations need to ensure that they identify dependencies and put controls in place to ensure the confidentiality, integrity and availability of the FIAM solution. Identify the activities needed to ensure FIAM is integrated into the corporate IT infrastructure such as extending existing IAM systems and including FIAM components in standard IT processes.

G Define approach for managing relationships with FIAM partners
Organisations need to define policies for identifying, assessing and mitigating the security risks involved in setting up each new FIAM connection. They include creating a standard approach for assessing security arrangements at service providers and identity providers, and defining legal and regulatory requirements in contracts.

H Create a process for managing FIAM connections
Organisations should define a standardised approach for managing FIAM connections, ensuring security issues are adequately addressed, and based on activities that need to be performed at different stages of the FIAM connection lifecycle. These are illustrated below.
Actions

About the ISF

Founded in 1989, the Information Security Forum 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 information security and 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 program. 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.

Contacts

For further information contact:
Steve Durbin
UK Tel: +44 (0)20 7213 1745
US Tel: +1 (347) 767 6732
Fax: +44(0)20 7213 4813
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

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 11 FIA M Marketing Copyright © 2011 Information Security Forum Limited. All rights reserved. Classification: Public, no restrictions

Where next?

The Federated Identity and Access Management: Creating a connected world report – available from the ISF website – provides an overview of the challenges and solutions related to implementation of FIAM. It also sets out approaches for developing a FIAM programme and managing new FIAM connections.

The report is supplemented by the Federated Identity and Access Management: Implementation toolkit – available exclusively to ISF Members. The toolkit helps organisations implement the recommendations of the main report. It provides resources to help organisations develop a FIAM programme, manage new FIAM connections, check the security arrangements of service providers, and create and support the business case for FIAM.

The report and toolkit are supported by an implementation space on the ISF Member website. This provides a facilitated forum for ISF Members to discuss FIAM-related issues and solutions, along with a central pool of additional resources including a checklist tool, webcast and presentations.

Input for the report was gathered from analysis by an ISF Principal Analyst, discussions at global ISF development workshops, detailed Member expert interviews, vendor interviews, Member case studies and recommendations from related ISF research projects.

Federated Identity and Access Management

Creating a connected world

Federated Identity and Access Management (FIAM) enables seamless, secure access to multiple external systems—revolutionising the way organisations interconnect with customers and suppliers.

FIAM allows an organisation to manage employees’ access to multiple external systems centrally, without the need to do so in each external system. Security is increased, costs are reduced, and the user experience improves.

To operate in today’s connected world, organisations need secure access to a variety of systems. Suppliers, customers, shared service centres and strategic partners operate numerous business applications: payroll, inventory and parts management, employee travel, service orders and client relationship management (CRM) to name a few.

Most organisations will focus on outbound FIAM connections, defined as those where their staff are given access to systems provided by other parties. Organisations that provide outsourced or cloud-based applications can gain competitive advantage by developing inbound connections for their customers.

As organisations increasingly turn to other parties—including cloud service providers—to deliver an ever-growing number of services, FIAM is growing in importance. FIAM can also be useful in organisations that operate a federated organisational structure, or during reorganisations, mergers or acquisitions, when it can provide an alternative to expensive systems integration.

To operate in today’s connected world, organisations need secure access to a variety of systems. Suppliers, customers, shared service centres and strategic partners operate numerous business applications: payroll, inventory and parts management, employee travel, service orders and client relationship management (CRM) to name a few.

Most organisations will focus on outbound FIAM connections, defined as those where their staff are given access to systems provided by other parties. Organisations that provide outsourced or cloud-based applications can gain competitive advantage by developing inbound connections for their customers.

FIAM introduces significant business risks when not adopted securely, so the Information Security Forum has launched Federated Identity and Access Management: Creating a connected world. This practical, business-focused report provides detailed guidance and good practices for working with business and technical teams to implement FIAM securely and effectively, for both outbound and inbound connections.