The International RegTech Association

Inspiring Innovation, Collaboration and Excellence in RegTech

IRTA PRINCIPLES FOR REGTECH FIRMS

October 2018

IRTA
International RegTech Association

Opening Remarks

Ben Richmond,
IRTA Chief Executive

Collaboration will undoubtedly play a significant role in the adoption of Regulatory Technology (RegTech) across global markets. A key initiative for the International RegTech Association (IRTA) is to facilitate connections between all stakeholders and to advance market development of RegTech. In support of this goal, the IRTA's Innovation Working Group has developed **IRTA Principles for RegTech Firms**, a new set of accessible open standards that help developers to create and deliver high-quality RegTech solutions, foster innovation and build trust with stakeholders from regulated financial institutions, as well as the wider regulator community.

Why now? The financial crisis accentuated the global reach of the financial services sector, as well as the fragility of such an extensive interconnected network that lacks transparency. If open standards had existed in 2007, the degree of risk within financial services would have been more visible, and regulatory requirements could have been translated and applied digitally. Since then, the weight of regulation has focused on reducing costs and leveraging technology to deal with regulatory requirements more flexibly. Open standards make technological innovation possible and are the key to fostering compliance in financial services.

What's next? Please take some time to review the IRTA Principles for RegTech Firms**, watch the launch webinar** and **provide your feedback** through this **Call for Input survey** by **January 14, 2019**. All relevant and appropriate input will be incorporated into the standards, and the final document will be launched in March 2019. IRTA Members will receive an advance pre-view on February 11, 2018.

Ben Richmond is an expert in information governance and regulatory change management, and Founder and CEO of CUBE

Regards,

Ben

Principal authors

Diana Paredes

Executive Board Member & Vice Chair, Innovation Working Group, IRTA

Diana Paredes has many years experience in investment banking, covering all asset classes at Barclays and Merrill Lynch, across sales, trading and structuring.

Diana is also co-founder and CEO at Suade, a RegTech provider that enables financial institutions to understand and deliver their regulatory requirements.

Dr. Daniel Gozman

Senior Lecturer, University of Sydney Business School & Honorary Fellow, Henley Business School (UK)

Daniel Gozman received his PhD from the London School of Economics. His work focuses on the intersection between policy, emergent technology and innovation. Daniel has published within respected peer reviewed scholarly journals and has presented his work at international conferences aimed at practitioners and academics. Daniel has acted as an advisor to major law firms, analyst groups and tech firms. Prior to academia, Daniel worked for a global management consultancy and a big four accounting firm.

Jane Walshe

Executive Board Member, IRTA

Jane Walshe is a Chartered Fellow of the CISI, and a financial services regulatory barrister who previously worked in the FCA's Enforcement Division, and also as a consultant at Simmons & Simmons. She is the Editor, with Norton Rose, of 'Individual Conduct in Financial Services Firms' - a practitioner guide published by Sweet & Maxwell. Jane is also co-founder and CEO of Enforcd, a RegTech start up that is on the Bank of England's FinTech Accelerator.

IRTA Principles for RegTech Firms

Core Principles Overview

Governance and Control

a) **Legal status**

Firms operate with a recognized legal status and have a legal personality separate from that of the individual founders and/or managers. They may be a public or private limited company, a form of partnership or other corporate body, established in any jurisdiction.

b) **Suitability of Management**

The senior managers of the firm are fit and proper individuals. There are three elements to the fit and proper principle:

- Competence and capability
- Financial soundness
- Integrity

a) **Appropriate Resources**

Firms have appropriate financial and non-financial resources with appropriate skills and competences, relative to the nature, scale and complexity of their business. They are able to meet the needs and expectations of their clients from a resource perspective.

Cybersecurity and Stability of Technology

Firms deploy high standards of security around their technological solutions, which are built to be stable and secure.

Outsourcing

RegTech firms providing outsourced services to regulated clients will ensure that they adhere to all relevant outsourcing rules and obligations, which apply in the jurisdiction in which their service is provided.

Risk Management

The RegTech firm has a documented risk management framework and appropriate risk governance in place, which enables the organization to identify, analyze and manage key risks of the firm.

Collaboration and Innovation

Firms are active in their pursuit of innovation in the interests of their clients and of the RegTech community at large.

Firms willingly collaborate with peers, clients, regulators and other relevant parties, with the intention of both creating and improving regulatory technology applications and solutions.

IRTA Principles for RegTech Firms

Guidance Notes

Governance and Control

Legal status

Firms operating with a legal status separate from that of their founders as individuals evidence that they are professional enterprises that are bound by aspects of company law, which may protect both the firm and those with whom they do business.

Cybersecurity and Stability of Technology

The applicable ISO standards include:

27005 – IT security techniques

ISO/IEC 27005:2011 provides guidelines for information security risk management.

It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005:2011. ISO/IEC 27005:2011 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

.

15289 – Systems and software engineering

Content of life-cycle information items (documentation)

ISO/IEC/IEEE 15289:2017 specifies the purpose and content of all identified systems and software life-cycle and service management information items (documentation). The information item contents are defined according to generic document types, as presented in Clause 7, and the specific purpose of the document (Clause 10).

ISO/IEC/IEEE 15289:2017 assumes an organization is performing life-cycle processes, or practicing service management, using one or more of the following:

ISO/IEC/IEEE 15289:2017 provides a mapping of processes from the above standards to a set of information items. It provides a consistent approach to meeting the information and documentation requirements of systems and software engineering and IT service management.

ISO/IEC/IEEE 15289:2017 does not establish a service management system.

27001 - Information technology

Security techniques -- Information security management systems -- Requirements

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

Guidance Notes

27002 – Information technology

Security techniques – Code of practice for information security controls

ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

It is designed to be used by organizations that intend to:

- select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001
- implement commonly accepted information security controls
- develop their own information security management guidelines

Outsourcing

Note that two outsourcing scenarios need to be considered:

- The RegTech firm provides a service/software to a client
- The RegTech firm is supported by sub-contracted parties

Considerations include:

Due Diligence

The RegTech firm will provide timely information to the regulated client in order to enable the latter to fulfil due diligence requirements on the RegTech firm.

Agreement

The RegTech firm must sign a legally binding document with the client and must comply with all requirements as outlined in that outsourcing agreement. The agreement must be renewed before expiry.

Monitoring and Management

The RegTech firm can be monitored and managed by the regulated client. The firm must maintain frequent contact with the client as well as provide reports for performance monitoring as required by the client.

Subcontracting

The RegTech firm is responsible for the quality and performance of services provided by sub-contracted parties (4th, 5th etc. party outsourcing) to the RegTech firm. Furthermore, the RegTech firm must ensure that all sub-contracted parties comply with requirements as outlined in the agreement with the client and applicable regulations in respective jurisdiction.

Business Continuity Management and Disaster Recovery

The RegTech firm has a disaster recovery plan and systems in place to enable mitigation of risk in circumstances where the RegTech firm is unable to fulfil it’s contractual obligations. Appropriate plans must be tested and evidenced at least on an annual basis. Recovery times must conform with times stipulated in the agreement.

Data

The RegTech firm confirms that data ownership, control and storage conforms to the requirements of the client at all times and is documented in the agreement. Furthermore, information privacy, confidentiality and security is ensured by appropriate measures complying with applicable regulations and client requirements.

IRTA Principles for RegTech Firms

Guidance Notes

Insurance

The RegTech firm must have an indemnity insurance covering any liabilities or potential claims from the client. The insurance must cover also services provided by sub-contracted parties.

Auditing

The RegTech firm confirms that it will provide regulators, designated external auditors and the regulated client with the right to audit the RegTech. This includes regulators/external auditors in the jurisdiction of the client, the country of registration of the RegTech firm and the jurisdiction the service is provided from. The RegTech firm must grant access to premises as well as data requested by listed parties. Furthermore, the RegTech firm confirms that audits and visits by regulators and external auditors are not disclosed.

Termination

Where a contract is terminated in accordance with terms agreed a managed exit process will be followed including the provision of data recovery/safe disposal to the regulated client.

Geography

Additional requirements may apply for individual jurisdictions. The RegTech firm ensures that these requirements are complied with as well.

KEY DATES

October 2, 2018

Draft IRTA Principles for RegTech Firms launch

Watch the webinar recording

Provide feedback

January 14, 2019

Deadline for providing feedback via our online survey

February 11, 2019

IRTA member-only pre-view of final IRTA Principles for RegTech Firms

March 2019

Final IRTA Principles for RegTech Firms launched to the open market

Want to join the IRTA? Visit our website

www.regtechassociation.org/membership

2018-2019 Membership Available Now!

IRTA Membership

Anyone with an enthusiasm for RegTech can join the IRTA. Choose the membership package that best suits your profile.

- Individual (e.g. researchers, academics, innovators, auditors)
- Academic institution
- RegTech solution provider
- FinTech company
- Government agency
- Technology solution provider
- Consultancy/services provider
- Regulated financial institution

Interested in IRTA membership? Visit

www.regtechassociation.org/membership

Why join the IRTA?

Example benefits* include:

- Be part of the international RegTech community
- Global and local seminars, workshops and meetups
- Special discounts on events, research, training
- Access to special offers from partners
- Discussion forum
- Access to webinar series
- Access to RegTech knowledgebase
- Access, utilize and contribute to RegTech innovation and research materials
- Participate in special interest think tanks
- Discover ways to improve regulatory compliance practices and competitive advantage
- Contribute to the development of RegTech standards
- Advisory briefings
- Member logo
- Market exposure (contribute to blogs, vlogs, podcasts)

…and more

*Benefits vary, according to membership package selected

@WeAreRegtech

Follow us

The International RegTech Association
info@RegTechassociation.org
regtechassociation.org

IRTA International RegTech Association

About the IRTA

The International RegTech Association (IRTA) is a united community of individuals and organizations, with a shared vision to innovate, advance, and influence the future of Regulatory Technology (RegTech).

Through consultation and collaboration, the IRTA plays a central role in shaping the future of the Financial Services industry. A non-profit Association, the IRTA brings together the people, tools and policies that are required to thrive in today's rapidly evolving RegTech landscape.

www.regtechassociation.org

Follow us

Twitter @WeAreRegtech

LinkedIn company/regtechassociation/

IRTA
International RegTech Association