Integrated Risk Management (IRM) Checklist

By taking an IRM approach to risk organizations can reach higher levels of program maturity and deliver real value in the form of stronger performance, increased resilience, better assurance and more efficient compliance.

Getting Started

Selecting the right IRM solution for your business can be a challenge, so Acuity has developed a high-level checklist based on its deep industry expertise to help you get started on your risk management journey. Note that not everything may be applicable to your unique situation. For more specific discussions around your organization's needs, please email: **info@cybersec.solutions.**

Assessing IRM

Before you can start evaluating solutions, you need to define the business outcomes needed for success.

Good business outcomes from IRM:

- Resilience to loss events
- Risk informed decision making
- Effective & efficient use of resources
- Integrated approach across multiple disciplines
- Optimized spending
- Continuous optimization
- Justified and comprehensible investment
- Confidence building for stakeholders

IRM Checklist

Key capabilities for IRM:

○ Business-focussed (delivering value to business leaders as opposed to just technical, compliance, audit teams)

○ Risk-based (needed to deliver value to senior leaders / the board but with seamless and efficient demonstration of compliance as a by-product of managing risk well)

○ Holistic, addressing the entire business, supply chain, partner ecosystem / all type of risks (as opposed to modular / siloed)

○ Always-on, data-driven, close to real-time (as opposed to slow, process driven, point in time)

○ Agile to react quickly to changes in business, regulation, emerging risks

○ Underpinned by an expertly engineered platform and data model created and delivered by experts specifically to deliver all of the above (as opposed to customizable document management and workflow typical of traditional GRC solutions)

Functional requirements for IRM:

Centralize

○ Support for integrated control frameworks to allow common controls to be measured once and then reported through the lens of multiple frameworks

○ Ability to model the Enterprise to support all parts of the organisation, supply chains etc. Ability to model business processes and assets in relation to the Enterprise model

○ Recording, tracking and reporting on a variety of different entities, including Incidents, Incident response plans, Non-conformities, Audit findings, Issues, Business Objectives etc.

○ Integrated action management to raise and track actions for risks, controls, assets and entities

○ Easy visibility of all relevant data on a single page, e.g. for a risk, see all linked controls, entities, actions and documents, then pivot to all risks linked to each control

○ Export of data to business intelligence and other third-party applications

○ Multiple integrated applications within the same system, e.g. cyber risk management, enterprise/operational risk management, compliance management, privacy management, vendor risk management, business continuity management

Automate

○ User configurable workflow and alerting

○ Easy configurability, including assessment schemes, colour thresholds, configurable fields for all risks, controls, assets entities and actions

○ Import of data from vulnerability scanning, threat intelligence, ticketing and other third-party applications

Quantify

○ Quantitative, qualitative or mixed-mode risk assessments

○ Aggregation of risk to understand exposure across parts of the business and overall

○ Comparison of risk exposure against tolerance across parts of the business and overall

○ Modelling the effect of control improvements or new controls on risk exposure and ROI

Report

○ Configurable and drillable home pages providing summary data and easy navigation to data of interest

○ Measuring and reporting on compliance with regulations, standards and other frameworks

○ Identification of control improvements which will give the greatest reduction in risk

○ Pre-configured graphical reports

○ User definable custom reports, extracting from all available fields in the database

Non-functional requirements for IRM:

- ◯ Rapid deployment
- ◯ Easy configuration
- ◯ Allow upload of legacy data
- ◯ Training manuals and documentation
- ◯ Unlimited scalability
- ◯ Intuitive to use with easy navigation
- ◯ SaaS or On-premise

Acuity Risk Management helps businesses worldwide effectively manage, prioritize and report on their risks to inform strategic decision-making and build long-term resilience.

Its powerful STREAM platform provides rapid time to value to reassure stakeholders that risks are under control and compliance is maintained with increasingly complex standards and regulations. With STREAM, Acuity eliminates the guesswork around risk to support strategic decision-making, prioritization of resources and justification of expenditure to maximize ROI. With customers worldwide, Acuity has proven success supporting customers in highly regulated and targeted industries such as finance, IT, telecommunications, healthcare, defense and government.

CYBERSEC SOLUTIONS

Email: info@cybersec.solutions
Web: https://cybersec.solutions
Tel: 01494 936696