IRM INFORMATION RISK MANAGEMENT
•ALTRAN GROUP

Think cyber.
Think security.
Think data.

For more information on SYNERGi
or to arrange a demo please contact
hello@irmsecurity.com

SECURE CYBER UNLOCK OPPORTUNITY.

IRM INFORMATION RISK MANAGEMENT
•ALTRAN GROUP

PRODUCT OVERVIEW

SYNERGi: AN INTEGRATED CYBER GRC SOFTWARE PLATFORM.

ALTRAN

TABLE OF CONTENT

SYNERGi®

AN INTEGRATED CYBER GOVERNANCE, RISK & COMPLIANCE SOFTWARE PLATFORM

Overview

SYNERGi is used by organisations to develop, maintain and report compliance against legal and regulatory obligations, as well as supporting a pervasive and continual approach to privacy, cybersecurity and operational risk. Each with its own reporting capabilities, SYNERGi has six dedicated modules:

- Governance Management
- Risk Management
- Compliance Management
- Audit Management
- Vendor Management
- IT Security Management

If you're currently working out of a spreadsheet or another manual process that just isn't scalable anymore, then SYNERGi offers a unique solution to help your organisation uplift its cyber posture.

Request a demo today at hello@irmsecurity.com or by visiting irmsecurity.com

MODULE 1. GOVERNANCE MANAGEMENT

Governance management is fundamental for ensuring that the correct policies, systems and processes are set in place to ensure the organisation's goals, direction, limitations and accountability frameworks are all equally defined.

Challenges

Ineffective governance can compromise management's ability to succeed, whereas effective governance in contrast can greatly assist the organisation.

Many organisations struggle to have a centralised way of managing their policies, processes and objectives; usually relying on spreadsheets to do so. The problem with this is that it becomes very difficult and time-consuming to link risks to your objectives and policies, meaning it becomes almost impossible to do any kind of intricate and thorough analysis.

There is no way to assess that the policies you have created align with any industry standard controls. Without knowing which controls are performing best, you run the risk of not conforming to the standards, which ultimately puts your organisation at higher risk and in a very vulnerable position.

The solution

SYNERGi Governance Management allows you to create Objectives (also known as Corporate Objectives) as well as Policies.

Objectives are statements of intent expressed by the business and typically detail some kind of business outcome. Objectives can be set at any level of the business from strategic Objectives all the way down to individual project Objectives. You can link Risks to your Objectives in order to, for example, plan Remediation Projects which will allow you to achieve your Objectives.

The Policies section of SYNERGi acts as a repository for all your Organisation's Policies and Procedures regarding cybersecurity. When a Policy has been created, you can link Controls from various Standards Libraries to your Policy. Subsequently, you can create Policy Statements and then link them to Controls (therefore linking them to the Policy).

This allows for a gap analysis to be conducted on your Policy and assess how well they align with the Controls in the Standards libraries. This will allow you to review your Policies and determine if they need improving and/or changing.

MODULE 2. RISK MANAGEMENT

As an organisation's cybersecurity matures, the emphasis moves beyond simple tick-box compliance, to understanding actual risks and their potential impact on an organisation's broadest corporate goals.

Challenges

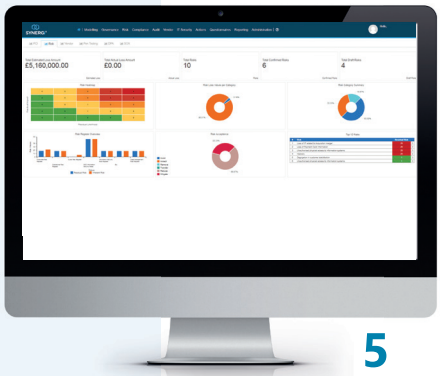
Risks are everywhere within an organisation – from operational risk, legal risk through to technology risk, financial risk and reputational risk. Because of this, many business leaders and board members are increasingly ensuring that risk is an integral part of their business strategy and decision making, and are continually making resources available to mitigate any risk that could cause catastrophic consequences.

Despite the momentum and increased focus on business risk, many organisations still try to manage risk through manual processes like spreadsheets. This is very surprising, because one small error on a spreadsheet could cause significant damage to a business. Although they increase productivity, they do not scale effectively and were not designed to handle the complex nature of risk management – endless amounts of data, intricate calculations and multiple users that are necessary today to conduct efficient risk management processes.

Many organisations are starting to realise that having a decentralised approach to risk management creates extreme difficulties to manage, as well as virtually impossible to see the bigger picture or identify any trends.

The solution

SYNERGi Risk Management is a cloud-based solution that allows organisations to identify, assess and manage all types of business risk through streamlined processes and a centralised, helicopter view of risk across the enterprise. The solution makes it easy to assess risks consistently, map them to your organisational model, and make informed decisions about a proportionate response.



MODULE 3. COMPLIANCE MANAGEMENT

Organisations must demonstrate ongoing compliance with various protection laws and regulations across many different business sectors. Failure to adhere to these can result in big fines and damage company reputation.

Challenges

Staying compliant with ever-changing standards and a continuously changing regulatory landscape creates interpretation and implementation challenges for organisations. Often compliance management and auditing programmes require a large degree of effort – establishing and implementing the appropriate controls as well as regularly testing and assessing their effectiveness. These processes are often managed by manual processes like spreadsheets and email filing systems, which were not designed to cope with complex compliance and audit tasks. Whilst these tools provide easy distribution and training, they are fundamentally a single-user tool meaning scalability is limited. Capturing and processing input from various documents to form efficient management and audit reports will be time consuming and very costly.

The solution

SYNERGi's Compliance Management module significantly streamlines compliance processes through a specially designed framework and reduces the time and effort needed to keep up with regulations, standards and policies; minimising the risk of non-compliance that could potentially affect your organisation. Our range of Policy and Control libraries help you get the most out of this module.

Some are provided out-of-the-box, such as ISO 27001/2, PCI DSS and NISD, and others can be industry or client specific. These libraries, along with associated control tests and questionnaires, enhance your ability to develop and maintain your compliance obligations. You get insight and control at the click of a button, so you can track your cyber maturity in different parts of the organisation, see how well standards, regulations and policies are applied, and confirm you always have the right controls in place.

MODULE 4. AUDIT MANAGEMENT

Your company most likely uses traditional spreadsheets and documents for audit management; whilst a common process, this method builds up a number of time-consuming tasks.

Challenges

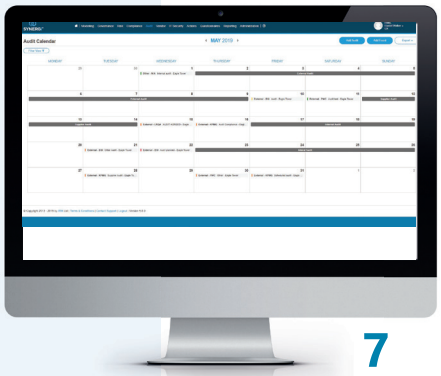
As a key element to risk and compliance, you need to gain control of the complete audit lifecycle, improve team collaboration and generate useful audit reports. Arduous activities like planning an audit calendar, printing checklists or gathering scope item documentation shouldn't be taking up the majority of your time.

It becomes even worse when this complex information is spread across disparate systems, meaning your business is unable to see the bigger picture of its audit management program; hindering its opportunity for continual improvement.

The solution

SYNERGi's Audit Management module is designed to help companies manage their wide range of audit related activities, data and processes in a single, comprehensive framework. The solution provides the flexibility to support all types of audits. Whether you're carrying out internal audits, operational audits, IT audits, supplier audits or quality audits, it doesn't matter because SYNERGi has the functionality to automate many of the necessary tasks for each.

The solution can help you plan, build and schedule appropriate checklists right through to collecting field data and reporting to your board and auditors alike. You'll finally be able to provide them with recommendations and useful insights they've been waiting to see.



MODULE 5. VENDOR MANAGEMENT

With the rise of new legislation and regulation coupled with regular media coverage of breaches occurring from third-party sources, the pressure is increasing like never before on businesses to effectively track and assess their supply chain and their vendor's risk and compliance.

New legislation & challenges of using manual processes

Those responsible for this task within their enterprise are quickly realising that spreadsheet-based methods are no longer viable for managing the complexity of their vendor risk and compliance programmes, and they are now seeking a more intuitive and cost-effective solution.

Many organisations tend to manage their supply chain risk internally through manual processes; distributing, tracking and reporting on their numerous vendors through large amounts of spreadsheet questionnaires and filing them in their email inboxes.

Hiring people to do this means they are spending more time on arduous tasks when they could be utilising their time on the more skilled areas of implementing risk based programmes. Some organisations outsource these tasks to other countries, but this option poses many risks associated with questionable governance standards.

The solution

SYNERGi Vendor Management enables organisations to fully automate their vendor and risk assessment processes, giving your compliance teams a complete overview of supplier risk so that they can focus their effort where it is needed most.

The platform can help you to easily capture existing third-party data and gain a complete picture of your vendor landscape straight out-of-the-box – helping you to easily track your vendors and ensure they stay compliant with ever-changing security standards.

MODULE 6. IT SECURITY MANAGEMENT

Unfortunately, in today's digital climate, incidents impacting business systems and sensitive data are considered almost inevitable. Having a timely, efficient and effective response plan is vital. How you react and respond is essential and an ineffective response can cause a lot of damage to a business.

Managing incidents with manual processes in today's climate

When a breach occurs within an organisation, you need to respond fast, know your roles and responsibilities and the activities, controls and processes that should be in place to do so. But what happens when you are managing this via spreadsheets and email?

Well, the entire process slows down, creates inefficiency and uncertainty amongst departments, lack of communication as well as difficulties in reporting on the status of various incidents. This could lead to disruption and reputational damage.

The solution

SYNERGi IT Security Management combines the power of live threat intelligence feeds with automated incident response processes.

Through APIs, the solution easily integrates with your existing SIEM, endpoint solutions, helpdesk and threat intelligence solutions, so you get one global view of potential attacks. By mapping the relationships your data assets have with processes, people, technology and corporate objectives, SYNERGi instantly identifies what has been affected, what incidents are related and what is at risk.

You get the means to prioritise actions, identify additional investment and report upwards.

PENETRATION TESTING PORTAL

Regular tests

Most organisations conduct regular penetration tests as it's the perfect way to audit the general security posture of a website, infrastructure or indeed the whole organisation.

Managing and actioning results

But far too often the remedial activities ascertained from these tests are not acted upon or are not visible enough, and so the same vulnerabilities occur time and time again. Managing and actioning the findings of a penetration test is the most critical activity yet companies struggle to keep track of remediation activities often relying on a combination of SharePoint, email and spreadsheets to action fixes, illustrate need and to obtain acknowledgement that remedial work has been completed. But this is a disjointed approach and one that lacks an auditable process which, in today's accountable age, is critical.

Without a coherent approach that allows a simple overview for senior management, there is little to no degree of assurance available that your organisations assets are protected. Without overview and accountability, the responsibility for fixing issues raised by your pen test results can be lost.

This is why we have developed the Penetration Testing Portal in SYNERGi.

93%

The clear majority (93%) of testers say that after a penetration test, the client would most commonly not fix some or all of the vulnerabilities identified by the testers or investigators.

7%

Only 7% remediate all vulnerabilities and then re-test to see if they plugged the gaps.

64%

The majority (64%) of penetration testers questioned admitted that the biggest frustration of their job was knowing that people don't fix the things that have been demonstrated to be broken.

Source: 2018 Black report from Nuix

PENETRATION TESTING PORTAL - FEATURES & BENEFITS

Features

- Central repository for all penetration tests including key project data
- Dynamic activity dashboard for searching and filtering key vulnerabilities
- Questionnaire builder that provides out-of-the-box and custom Cloud, App, IOT, Red Teaming, Infrastructure, Mobile scoping templates
- Calendar for scheduling and viewing key milestones such as start dates and availability
- Powerful reporting engine providing out of the box reports, security metrics and risk heat maps
- Task management for tracking High, Medium and Low fixes
- Exception management for tracking exceptions and waivers through to closure
- Import connectors compatible of supporting all major CHECK and CREST reporting formats

Benefits

- Manage critical findings as soon as they are reported
- Schedule penetration testers who have the skill, knowledge and experience of your technology stack
- Increase accuracy of scope and align to businesses risk appetite and budget
- Track how many issues have been found in each penetration test
- Report SLA targets for High, Medium and Low severity findings
- Track risk exceptions and waivers through to closure
- Prioritise retest activity
- Report against OWASP Top 10 vulnerabilities
- Identify the last time a penetration test was conducted against key
- Report next test date and or flag key systems and applications that haven't been tested
- Reduce costs and gain better governance across all pen tests
- Share results with other delivery and development teams who are working with similar applications and infrastructure

SYNERGi'S ADMINSTRATION FEATURES

Customisation

Any business that is migrating away from manual processes will expect an application such as SYNERGi to support the unique characteristics of their industry, processes and day-to-day business practices. Common software packages work to a point, however, the final tailoring provides each business with a seemingly custom solution to deliver its unique business benefit.

This tailoring is often time-consuming, as it comes with an army of expensive consultants, and more often than not, over-customisation leaves the application untenable. SYNERGi supports this common challenge by providing users with the functionality to highly configure their instance of SYNERGi to meet their use cases.

The Administration features in SYNERGi contain various sections that allow you to configure the platform, as well as control who uses it and what they see.

The core features of the Administration function include:

- Custom workflows
- Business rules
- Custom questionnaires
- Role-based access
- Taxonomies
- Response mapping
- SSO (Single Sign On)
- Next generation role-based access
- Audit logs

INTEGRATION FEATURES

Why do you need integration?

Over the years, we've witnessed organisations take on endless solutions and technologies to assist and enable the risk management process. Unfortunately, this disparate approach to technologies creates an inconsistent and confused conclusion on risk.

Trying to retro-fit their cyber risk and compliance to various technologies makes you reactive. SYNERGi allows you to adopt a proactive approach to cybersecurity as it seamlessly integrates cross-departmental and enterprise data systems.

SYNERGi allows you to capture all the information on your key data and information, integrating endpoint technologies and plug-ins; providing you with greater visibility to govern risk.

Available integrations

- Vulnerability Assessment - Nessus
- CMDB Integration - for Asset Discovery and ingestion
- SIEM Integration - ArcSight, to enable dynamic view of risk overlaid over assets and business
- VAPT Integration - automated compliance view against application controls and policies
- Integration with Enterprise Risk Management Solutions - to escalate the risk to an enterprise risk register

Others

- Sharepoint
- API and Connectors - report writing
- Click
- Qualys
- Power BI

IMPLEMENTATION

"IRM provided on-site consultancy, which certainly made life easier and left us feeling confident." Ned Finn, HEAD OF IT SECURITY, GAME

Expert support

IRM's in-house professional services team is responsible for supporting customers with implementing SYNERGi into their organisation.

'QuickPath' consulting engagements are designed to perform advanced implementation, configuration and training. Each project scope is designed to meet the specific parameters established by the client team, allowing management to determine the level of investment in line with the deliverables desired.

Our approach to SYNERGi implementation:

- Discover & Assess
- Design & Implement
- Configure & Model
- Integrate & Expand

With the right training during and after the implementation process, your organisation's key employees will be able to use SYNERGi to break down internal barriers to provide a single, centralised, view of information security across the business.

Proof of concept

Before making an investment in a GRC platform, we believe it's important to experience the software in full. That's why we offer a free trial lasting up to 2 weeks. It will give you hands-on experience to test your use cases, demonstrate report generation to decision-makers and give you a head-start on implementation if you decide to procure SYNERGi.

VALUE TO THE BUSINESS

Financial benefits

- Reduce the risk of heavy fines
- Internal resources are better put to use
- Maintaining compliance standards will help win more customers and increase revenue
- Avoid fines from non-compliance from a vendor or weak supply chain link
- Reduce internal headcount and significantly reduce cost per third-party/ vendor assessment

Operational benefits

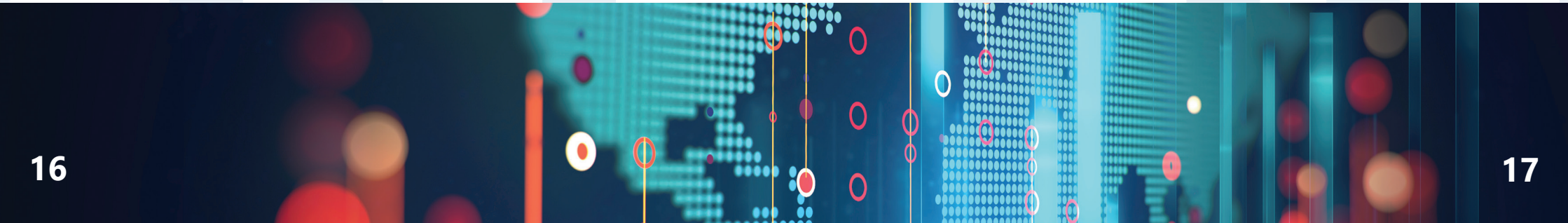
- Track the effectiveness of controls across specific business units
- Quickly identify & address non-conformances
- Unify control standards and reduce audit fatigue
- Assign roles and responsibilities
- Link requirements across departments/units
- Upload and edit policies, standards and requirements
- Allows Information Security personnel to concentrate on security not admin

Automation benefits

- Pre-defined questionnaire templates readily available
- Easily send, receive, evaluate and create remediation actions
- Track upcoming, in-progress, completed and overdue assessments in real time
- Avoid wasting time following up via phone or email
- Ability to re-validate & re-issue previous questionnaire responses and evidence
- Reduce audit fatigue
- Risks can be automatically raised in the third-party risk register
- Meet GDPR, PCI and ISO obligations for managing third-party risk

Strategic benefits

- Helicopter view of risk and compliance stats
- Interactive and colourful dashboards for board reporting
- Instil confidence with complete visibility
- Clear view of the whole organisation – enabling you to spot patterns in minor or isolated events



OUR CUSTOMERS & USE CASES

The range of modules available in SYNERGi means the platform can support various use cases in your organisation

Use cases supported by SYNERGi include:

- PCI DSS
- Supply chain and third-party risk management
- ISO frameworks
- NIST
- NISD
- Compliance
- GDPR/DPA
- BSI
- SOX/financial controls
- Audit management
- NCSC frameworks
- Policy management
- Risk Register

Our customers include:

amey

Rank Group

Legal & General

Travelex worldwide money

vodafone

Carphone Warehouse

Taking advantage of the integration functionality and sophisticated reporting capabilities, SYNERGi can support use cases ranging from managing IT policies to ensuring the compliance of your third parties

CASE STUDY
LEADING GLOBAL TELECOMS PROVIDER

The context

Multiple platforms and technologies were used to record cyber and information security risks, with no integrated solution providing a "single source of truth". Multiple frameworks and standards were being managed in time/resource-consuming spreadsheets alongside eleven incident, vulnerability, asset and technology solutions. Few processes and little ownership of risk and responsibility for remediation were in place. The supply chain landscape was also unclear.

The challenge

To find a GRC platform that could support multiple compliance frameworks, including ISO 27001 and GDPR. Despite good organisational structure, controls were not fully documented or embedded into daily practice. To define pen testing remediation actions, as well as fully mapping the third-party landscape, detailing each party's compliance.

The solution

- Implementation of the SYNERGi GRC platform providing:
  - Out-of-the-box management for compliance visibility across standards
  - Visibility of its technology and information/data assets
  - A consistent language and methodology for governing risk
  - Confidence that the data sources are both accurate and being managed
  - Ability to quantitatively measure its cybersecurity posture through notification of emerging threats
- SYNERGi's Penetration Testing Portal was adopted allowing the organisation to manage and communicate penetration testing activities, remediation and scheduling.
- Having identified hundreds of third-party connections via a third-party risk assessment, the data was then mapped to SYNERGi's Vendor Management module, with the Questionnaire functionality used to obtain their compliance status.