Integrity360
your security in mind

CYBER RISK & ASSURANCE PRACTICE

Integrity360

your **security** in mind

How mature is the security posture of your organisation?

Executive summary

A company-wide cyber security strategy is absolutely essential to combat today's evolving risk landscape.

While systems expertise remains an essential ingredient of preparedness, it is only when cyber security is understood within the organisation's overall business strategy that executive leadership can have confidence that information, the single most important business asset is sufficiently protected against today's threats.

Integrity360 helps organisations mature their security programmes by offering a range of strategic advisory services:

1. Cyber Security Risk Assessment
2. Cyber Security Compliance
3. Cyber Security Governance and Strategy
4. ISMS as a Service
5. ISO 27001 Consulting
6. Third Party Risk Management
7. Cloud Security Assessment
8. Cyber Threat Modelling
9. Resilience Services
10. Data Protection Services

Cyber Security Risk Assessment

Organisations face persistent threats from advanced attackers, a rapidly expanding technology landscape, as well as complicated and evolving regulatory requirements.

Our team of CRA Advisors can provide you with the guidance to develop or enhance your information security program through informed decision-making, optimised information security investments and influencing the strategic vision and direction.

Defining the scope of potential risks helps create unique response plans for each one.

They assist with assessing your current security maturity levels, identify your desired target or future state and develop a prioritised roadmap based on industry standards, leading practices and your business priorities.

OUTCOMES & DELIVERABLES

- Understand your current security maturity with a view of identifying areas of improvement across people, processes and technology, and providing risk-informed, prioritised actions to achieve your target maturity state
- Gain expert advice for planning and improving your existing security program posture
- Make informed decisions for planning cyber security activities, risk management and targeted improvement
- Ensure your information security program is aligned with industry best practices, regulations and compliance mandates
- Establish a strategic risk management program built on a security framework to effectively sustain and improve the programme
- Compare yourself to your peers and receive recommendations to quickly move toward a more mature security program

Cyber Security Compliance

How mature is the security posture of your organisation? How closely does it align with mandated frameworks? Leverage deep security experience and knowledge of industry leading holistic frameworks to gain an end-to-end view of your security programme's current maturity status and inform target outcomes. The most sought after frameworks we work with include:

- Center for Internet Security (CIS)
- Cyber Essentials
- ISO 27001
- NIST
- ISO 27017(Cloud)
- ISO 27701(PIMS)
- SOC 2
- GDPR

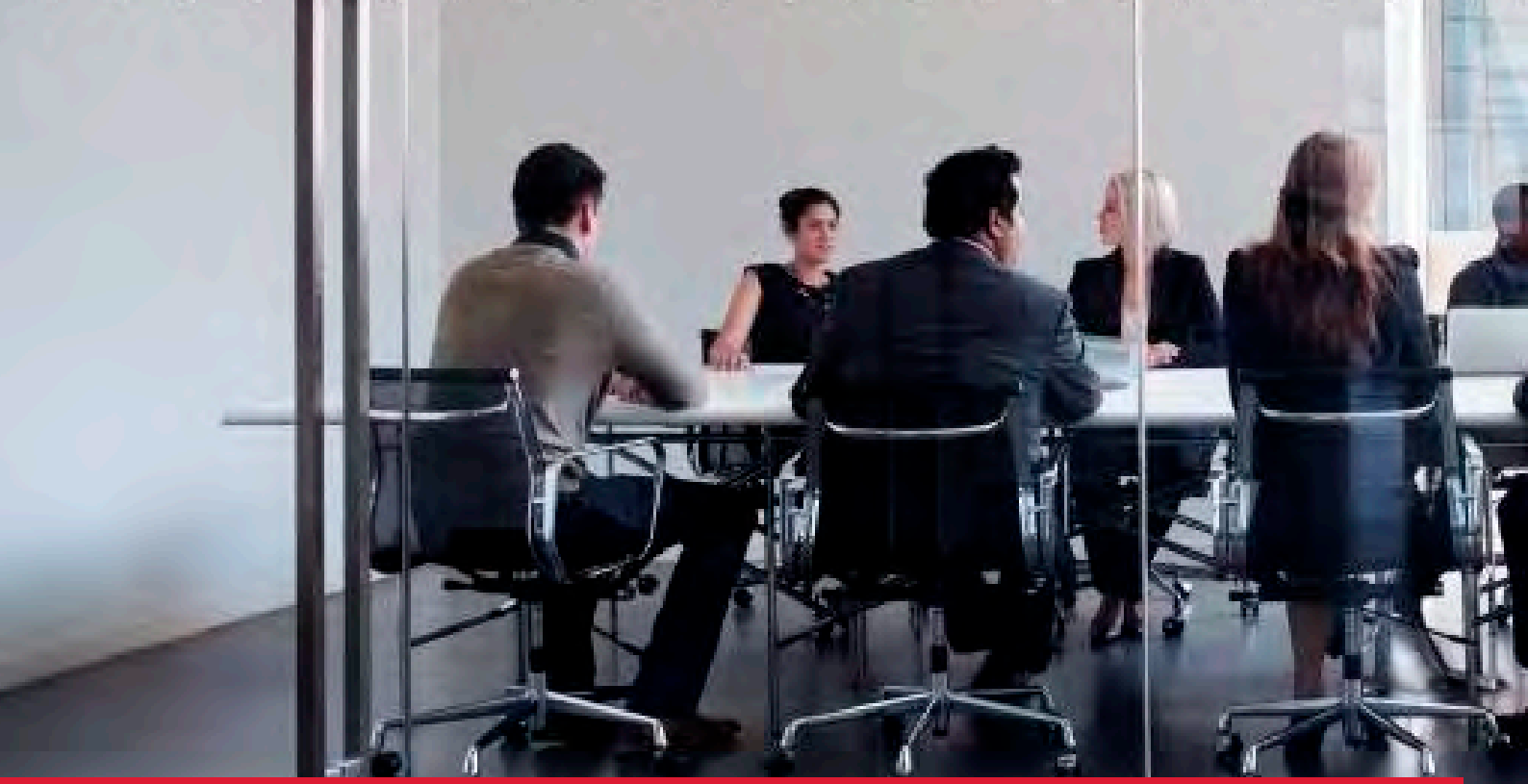
OUTCOMES & DELIVERABLES

Our CRA team offers a variety of different assessment types, based on industry recognised security frameworks to:

- Understand current level of compliance for required standards to facilitate compliance
- Identify critical security control gaps and measure your security controls against industry best practice
- Drive a pragmatic, prioritised approach to implementing regulatory mandated changes, improving your security posture and optimising operational efficiency
- Quantify your cyber security risk and benchmark your performance against industry peers

PROBLEMS OUR CLIENTS FACE

- Regulatory requirements
- Customer requirements
- Unstructured security initiatives
- Existing security vulnerabilities
- Ineffective security policies and procedures
- Stakeholders, investors and clients requiring data security assurances



Cyber Security Governance and Strategy

A company-wide cyber security strategy is absolutely essential to combat today's evolving risk landscape. This means breaking down silos and encouraging the engagement of security experts throughout different business units.
Organisations need to make informed cyber security decisions and stay up to date with complex regulations. Too often, executives lack oversight to take the proper action. By informing decision-making with objective measurements around cyber risk, we help mitigate risk across the enterprise, resulting in better decisions that protect your company's ability to operate.

OUTCOMES & DELIVERABLES

In order to reduce your exposure, optimise your security controls investments, and protect your organisation, you must be well-versed in and leverage best practices. Integrity360 helps companies develop an execution strategy with short-term and long-term objectives. This empowers your management to implement an appropriate framework that meets business needs while remaining compliant. It additionally helps organisations to:

- Align security with business objectives
- Aid in effective implementation and operation of security processes and technologies
- Maximise return on security investment
- Create a unified security plan
- Unify security with business and IT stakeholders on an enterprise-wide security strategy
- Allow for proper budgeting of security investments with a defendable prioritisation model for implementation of security initiatives

PROBLEMS OUR CLIENTS FACE

- Absence of a company-wide cyber security strategy
- Unclear picture of threat landscape
- Risk based decision making lacking
- Lack of oversight and future roadmap
- Need for cyber risk reduction
- Lack of security optimisation
- Investment rationalisation


SMO
Roadmap activity
NIST Domain
Strategy initiative
Responsible department
2020
2021
2022
Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4
1 Establish a formal information security organisation structure. Identify Security Governance
2 Implement governance structures, forums and update position descriptions for key roles with security responsibilities, based on a RACI matrix. Identify
3 Establish policies and standards based on the ISMS framework aligned to NIST Identify
4 Establish metrics and reporting capabilities to continuously measuring the effectiveness, efficiency and capacity of information security frameworks and resources against business needs. Identify
5 Categorisation of assets to understand the assets most critical to the business. Identify Asset Management
6 Implement a consolidated platform for asset management for identifying, tracking and protecting of assets (i.e. hardware and software assets) throughout all stages of their lifecycle. Identify

ISMS as a Service

Our CRA team provides strategic services to assist you with the creation, planning, and execution of your information security programme, so you have clearly defined and enforceable policies and can measure your cyber risk. Integrity360's virtual CISO (vCISO) and Virtual Information Security Officer (vISO) are dedicated security specialists who work closely with you to gain a clear understanding of your business operations and how to best manage security risks together. Throughout the entire engagement which will run through our vCISO/vISO model, they provide expertise and make recommendations and assist in controlling the pace and assertiveness of your information security program. This partnership ensures that our efforts align with your organisation's business goals and objectives.

OUTCOMES & DELIVERABLES

Our ISMS as a Service helps to:

- Provide security leadership and direction through a virtual CISO advisory
- Define security objectives
- Develop and execute Security strategy and roadmap in line with an international security frameworks
- Define, develop and enforce IT security policies, standards, procedures and controls
- Manage the overall security risk of the enterprise
- Govern Security awareness
- Establish centralised set of security metrics that will be reported periodically.
- Conduct progress review and analysis

PROBLEMS OUR CLIENTS FACE

- Lack of resources/staff for security governance
- Limited cyber performance metrics
- Lack of security awareness
- No experience in driving strategic security
- Security and privacy integration needed
- Lack of security structure

ISO 27001 Consulting

ISO 27001 is the globally recognised international standard for information security management. The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

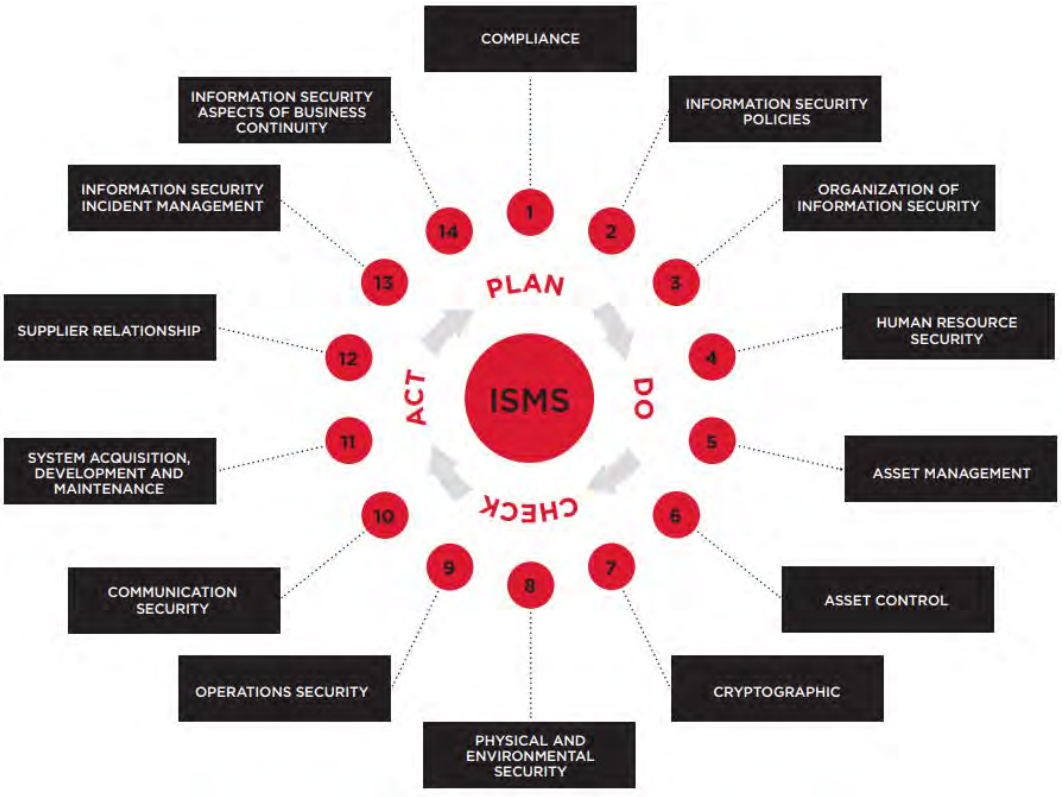
More and more organisations are realising the benefits of achieving compliance with a security standard. This is sometimes driven by client requirements and sometimes driven by the desire for competitive advantage. Too often IT managers feel that it is a huge undertaking and that they will be buried in bureaucracy and documentation and so fail to even begin the process. Integrity360 has helped many organisations achieve certification and can assist from developing the roadmap to certification, mentoring your team along the way, to developing the framework and implementing the controls. Our involvement can be tailored to fit your requirements.

OUTCOMES & DELIVERABLES

- ISO 27001 GAP Assessment: We assess the current state of your ISO 27001 Compliance using the ISO 27001 Standard
- ISO 27001 Risk Assessment: We perform the ISMS Risk Assessment using a suitable framework for your organisation.
- ISO 27001 Policies & Procedures: Our ISO 27001 Consultants develop the required Information Security policies and procedures tailored to your organisation's needs.
- ISMS Security Awareness: We provide security awareness training for employees to embed a solid security culture.
- Technology Implementations: We advise on remediation of technology gaps and implementation of technical controls within the Standard
- ISMS Internal Audits: We carry out Internal audits to help you identify deviations from the defined ISMS policies and procedures.
- ISO 27001 Certification Audit: We provide hand-holding support during the ISO 27001 certification audit leading to ISO 27001 Certification.

PROBLEMS OUR CLIENTS FACE

- Lack of resources/staff for security governance
- Limited cyber performance metrics
- Lack of security awareness
- No experience in driving strategic security
- Security and privacy integration needed
- Lack of security structure



Third Party Risk Management

Organisations looking to make real improvements must gain operational command of the security posture and risk of their third parties. Integrity360's Third Party Risk Management service manages all aspects of monitoring, allowing you to focus on strategic tasks with the confidence that your vendor population is being properly managed and vendor maturity is improving over time. Our team provides expert industry advice to help you manage your security reputation and accelerate your third-party risk management programme.

OUTCOMES & DELIVERABLES

- Increase understanding of business risk and identification of risk mitigating factors
- Identify list of Third Parties across Business Functions
- Classify the Third Parties based on their Risk Profile
- Identify Risk to which your organisation is exposed based on the service(s) provided by the third party
- Utilise common industry methodology to identify the compliance requirements and assess current level of compliance

PROBLEMS OUR CLIENTS FACE

- No common guidelines for managing third party risk
- Risk of reputational damage should an event occur at your third-party
- Incomplete population of vendors with sensitive data
- Increased focus on securing customer personally identifiable information (PII)
- Inconsistent risk assessment and review practices across organisation
- Various compliance requirements not being monitored effectively
- Third-party failure to maintain continuation of business as usual (BAU) for your organisation
- Risk of doing business in a specific country including legal/regulatory, geo-political and social-economic considerations
- Financial loss due to third-party failure or non-performance
- Third-party failure to comply with a required regulation

Cloud Security Assessment

As organisations continue to migrate legacy applications and infrastructure into the cloud, they are faced with new challenges and processes like never before. If your organisation already has a cloud footprint, our assessment provides a quantified snapshot of your current state to give you a clear roadmap for improvement and optimisation. During a Cloud Security Assessment, we evaluate your cloud security posture based on industry best practices. We have developed a unique cloud security framework covering critical risk and security controls based on the Cloud Security Alliance, CIS controls and our own operational experiences to help you create and ensure a secure cloud environment.

OUTCOMES & DELIVERABLES

- Provide an in-depth view of your cloud security programme weaknesses and strengths
- Inform more effective cloud operations, architecture and strategy built on prioritised guidance
- Develop a mature cloud security architecture aligned to business objectives and risk profile
- Understand threats to your specific cloud environment architecture
- Prioritise the right security enhancements to your cloud environment
- Deliver prioritised recommendations to help you better avoid attacks and survive incidents with enhanced security practices for your cloud workloads
- Identify areas of improvement and advance your cloud security

PROBLEMS OUR CLIENTS FACE

- Lack of understand of how to use and how not to use cloud resources. This misunderstanding weakens security controls in place and leads to a loss of data
- Increases complexity of protecting data in the cloud, increasing the risk of compromise
- Data leakage and lack of encryption
- Insufficient understanding of roles and responsibilities as a CSP and Cloud user
- Awareness of the need for additional security precautions due to open and shared processing environments that exist in the cloud

Cyber Threat Modelling

Threat Modelling is a next-generation cyber security defence that allows an organisation to understand their level of threat exposure. Threat Modelling consists of a series of workshops to identify high-risk threat vectors facing your organisation, map out detective and preventive defences in place to mitigate those threats, and perform gap analysis to prioritise remediation activities. Questions answered during this engagement include:

- What information is likely to be targeted?
- Who is likely to attack?
- Why will they attack and what are their objectives?
- How will the attack occur?
- How can the threat likelihood and impact be minimised?
- What's my level of threat exposure?

OUTCOMES & DELIVERABLES

- Provide a frame upon which threat intelligence can be established
- Enable better control of threats which are increasing in number and sophistication, and identify motivation of threat actors that can damage your key assets/crown jewels
- Establish a contextual baseline based on geography and industry for understanding the actors
- Enable understanding of more advanced cyber-attacks whereby preventive controls are no longer seen as an effective defence
- Map threats on cyber kill chain to demonstrate the attack process
- Calculate your cyber incident preparedness index/threat score using a sustainable threat modelling approach
- Assess the overall effectiveness of your current cyber defence/tools and benchmark with industry peers
- Assist in identifying threat mitigation measures for major threats in your organisation's context
- Assist in building your overall cyber security strategy and provide direction to drive cyber defence programs focusing on identification, detection and response throughout the lifecycle of an attack

PROBLEMS OUR CLIENTS FACE

- Lack of understanding of who is likely to attack your orgnaisation, how and why the attack could occur
- Minimal understanding of the likelihood and impact of an attack
- Limited awareness of threat exposure

Resilience Services

Resilient organisations must focus on three main areas when it comes to cyber resilience—1. being hard to hit, 2. being ready for the attack when it comes, 3. being able to recover quickly. Cyber threats, both internal and external, are increasing faster than an organisation's ability to implement improvements to its information security program. Further, organisations may not be ready to respond effectively in the event of a major breach. Integrity360 helps the client in establishing effective capabilities for managing emergencies, incidents and crises. It includes development of necessary strategies, plans and procedures for managing continuity of business and IT landscape.

OUTCOMES & DELIVERABLES

- Conduct a Business Impact Analysis (BIA) and Risk Assessment
- Perform business continuity and disaster recovery planning
- Implement a structured and consistent framework for central coordination, tracking, response and monitoring of all cyber security-related breaches
- Provide response capabilities during the incident lifecycle to minimise and/or eliminate the effects of cyber security breaches
- Provide executive level briefings that enable management to make timely and informed decisions about cyber security breaches
- Increase disaster preparedness & reduce down-time in the event of a business disruption
- Increase understanding of business risk and identification of risk mitigating factors
- Minimise network/IT/process downtime and reduce exposure (financial & operational)
- Increase level of preparedness to manage a disaster and improve disaster readiness
- Improve the response to an incident or potential incident and minimise service downtime thereby ensuring customer satisfaction and maintenance of brand image
- Development/Deployment of comprehensive business continuity/disaster recovery framework such as ISO 22301

PROBLEMS OUR CLIENTS FACE

- Need to analyse and mitigate increasingly complex threats
- Awareness of risk and impact associated with the disruption of critical business processes
- Need to continuously improve the readiness/resilience of the organisation's IT processes and infrastructure to any crisis or disaster
- Need to improve and maintain the continuity of the people, processes and technology within the organisation
- No defined IR process including documented response plan, cross-functional roles and responsibilities (e.g., legal, HR, public relations)
- Inconsistent incident handling across the enterprise
- Lack of procedures and training to allow first-responder to take action
- Lack of table-top exercises to validate a plan and ensure response team comprehension
- Lack of external communications plan including to external entities such as vendors, customers and the general public

Data Protection Services

Organisations are privy to large amount of personal information, for employees, its customers and in some cases, for third parties. With the shift in regulatory requirements and as technology innovation continues to accelerate, organisations need to work together with privacy professionals to innovate new approaches that entrench privacy as a standard rather than an anomaly.

Applying strong data protection consists of data discovery, assessing risk, identifying solution platforms, defining objectives and workflows, and much more. Integrity360 can help you discover critical data security issues that can result in significant business impacts and help reduce long-term data security related risks that include strategic, compliance and financial implications.

We can help provide you with full visibility and control of your data across on-premise and cloud-based architecture. We also provide you with a set of actionable recommendations to further improve your visibility across all data sources.

Every business has data protection obligations to meet - and they must prove they're meeting them.

OUTCOMES & DELIVERABLES

- Identification of your privacy posture by performing a comprehensive data privacy risk/ impact assessment exercise
- Visibility of your personal information
- Repository of applicable geographical, industry and function specific privacy requirements
- Adherence to privacy legislation requirements like GDPR
- Establishment of an on-going compliance monitoring, enforcement, and reporting practice
- Embedding of privacy into your organisation's culture

PROBLEMS OUR CLIENTS FACE

- Meeting multiple regulatory or client specific requirements
- Lack of data classification
- Emerging and evolving regulatory landscapes and the need to be compliant
- Geographical spread of information changing multiple hands
- Increasing complexity of operations and dependency on third parties
- Failure to managing data privacy due to high attrition rate and poor awareness among employees and management
- Lack of breach notification / communication process

Next Steps

Integrity360's Cyber Risk and Assurance team provides a wide range of services to help enterprises reinvent their risk posture and transform their cyber security strategy from chaotic to organised. By aligning with a framework and building a comprehensive roadmap, businesses can protect their sensitive data and highly valuable assets from hackers.

From initial engagement to technological implementation, Integrity360 has consultants at every point in the journey who specialise in defending businesses from the most challenging threats they face daily.

Contact an Integrity360 advisor today by emailing info@integrity360.com or visit integrity360.com for more information.

Integrity360
your **security** in mind

HEAD OFFICE
3rd Floor, Block D, The Concourse,
Beacon Court, Sandyford, Dublin 18.
+353 (0)1 293 4027

LONDON OFFICE
90 Long Acre,
Covent Garden, London, WC2E 9RZ
+44 20 3397 3414

NEW YORK OFFICE
260 Madison Avenue, 8th Floor
Manhattan, 10016
+1-212-461-3286

www.integrity360.com
info@integrity360.com

Integrity360

your **security** in mind