



GET TO KNOW:

BDO's Cybersecurity & Privacy Services in Cyprus & Beyond

JANUARY 2019



Table of contents

BDO' Cybersecurity&Privacy Management Team	2
Our Value Proposition	3
Cybersecurity Overview	4
Comprehensive Cybersecurity Portfolio Of Services	5
Cybersecurity Services Descriptions	6
Cyber risk assessment	7
Incident response	10
Cybersecurity strategy & mitigation plans	11
Cyber Investigations	12
Cybersecurity solutions	13
Vulnerability assessment and penetration testing (VAPT) services	14
ISO 27001 & 27002	21
Virtual CISO	22
PCI data security standard	23
AICPA SOC for cybersecurity	25
Managed cybersecurity services	27
Cyber risk management "ä holistic approach"	29
About Us	30



BDO' Cybersecurity&Privacy Management Team



Director | Technology Risk Advisory

Christos is the Technology Risk Advisory Director of BDO Cyprus. Christos has 18 years of experience in the areas of Information Technology, Cyber Security Risk Management, data protection and information security governance. He has held a number of positions such as IT architect, IT Consultant and Chief Information Security Officer (CISO). For the past 10 years, Christos was the CISO of one of the largest banks in Cyprus. During this time he was also nominated as the SWIFT national CISO by the Central Bank of Cyprus.

Christos's extensive experience spans out to numerous Information Security Risk management domains such as Security Policies, Compliance, Business Continuity, Networking, Cryptography, ISMS, ISO 27K, Information Security Risk Management Frameworks, Basel III, EU Personal Data Protection Legislation/GDPR, PSD2, NIS, Cloud Security and SWIFT CSPF.

Christos is a qualified PECB ISO/IEC 27001 Lead Implementer and Certified Data Protection Officer (CDPO).

He is a graduate of the University of Surrey holding an MSc in Telecommunications and Software and a BEng in Electrical and Electronics Engineering (Telecommunications), Awarded with a 1st Class Honors).

t: +357 22 495707
m: +357 99 497953
e: ckoutsoupi@bdo.com.cy



Manager | Technology Risk Advisory

Philippos is a Technology Risk Advisory Manager at BDO Cyprus. Philippos has 10 years of experience in the areas of Information Technology, Cyber Security Risk Management, data protection and information security governance. He has held a number of positions working for technology advisory firms and in the financial sector. For the past 5 years, Philippos was a senior information security officer at one of the largest banks in Cyprus. During this time he was also responsible for assessing the bank's SWIFT/Target infrastructure as per the directives of the Central Bank of Cyprus.

Philippos experience spans out to numerous Information Security Risk management domains such as Security Policies, Compliance, Business Continuity, Networking, Cryptography, ISO 27K, Information Security Risk Management Frameworks, Basel III, EU Personal Data Protection Legislation/GDPR, PSD2, NIS, Cloud Security and SWIFT CSPF.

Philippos is a qualified PECB ISO/IEC 27001 Lead Implementer and Certified Data Protection Officer (CDPO).

He is a graduate of the Royal Holloway University of London holding an MSc in Information Security and the University of Warwick BSc (with Honours) in Computer Science.

t: +357 22 495707
e: pdemetriou@bdo.com.cy

Our Value Proposition

BDO's cybersecurity leadership, expertise and holistic approach to managing cyber risk allows organizations to improve their governance, risk management, compliance, and bottom lines by reducing their exposure to and the impact from cyber attacks.



BDO differentiator

- ▶ Our unparalleled cybersecurity leadership, expertise, and global presence combined with a holistic cyber risk management approach and our diverse blend of cyber services.



Impact

- ▶ Optimize information management, governance, risk and compliance in a cost-effective manner.
- ▶ Reduce IT and business operational expenses.
- ▶ Leverage industry best practices, technologies & tools to improve business results.

Cybersecurity Overview

Strategy, services, and solutions to address the unique cyber risks of every organization.

CYBER ATTACKS: INCREASINGLY LIKELY, POTENTIALLY CATASTROPHIC

Information sharing is fundamental to virtually every aspect of business. As a business grows, information sharing grows along with it - with vendors, contractors, partners, and customers. And every one of these digital relationships presents a new set of cyber vulnerabilities.

The need for security and the way in which it is implemented must be balanced, thoughtfully, against the needs of an organization to operate effectively, and to actively pursue its future goals.

While it is impossible to eliminate all risk of a cyber attack, a well-designed program will minimize the negative impact on both short- and long-term business goals.

PROTECTING BUSINESS STARTS WITH UNDERSTANDING BUSINESS

BDO's Cybersecurity team is comprised of professionals from a diverse range of backgrounds, including IT, business operations, government, data privacy consultants, forensic technology, business advisory, and audit services. We are built to provide comprehensive, customized services for each client, focusing on your specific needs, operating model, technical demands, regulatory environment, and industry dynamics.

Everyone at BDO recognizes that a robust information security program is part of an optimal business strategy. Our unique combination of technology and business advisory practitioners place a high priority on mitigating risk, while supporting long-term business growth. We work collaboratively with you to develop and implement programs that are not only effective, but sustainable.

CYBER RISK: UNIQUE TO EVERY ORGANIZATION

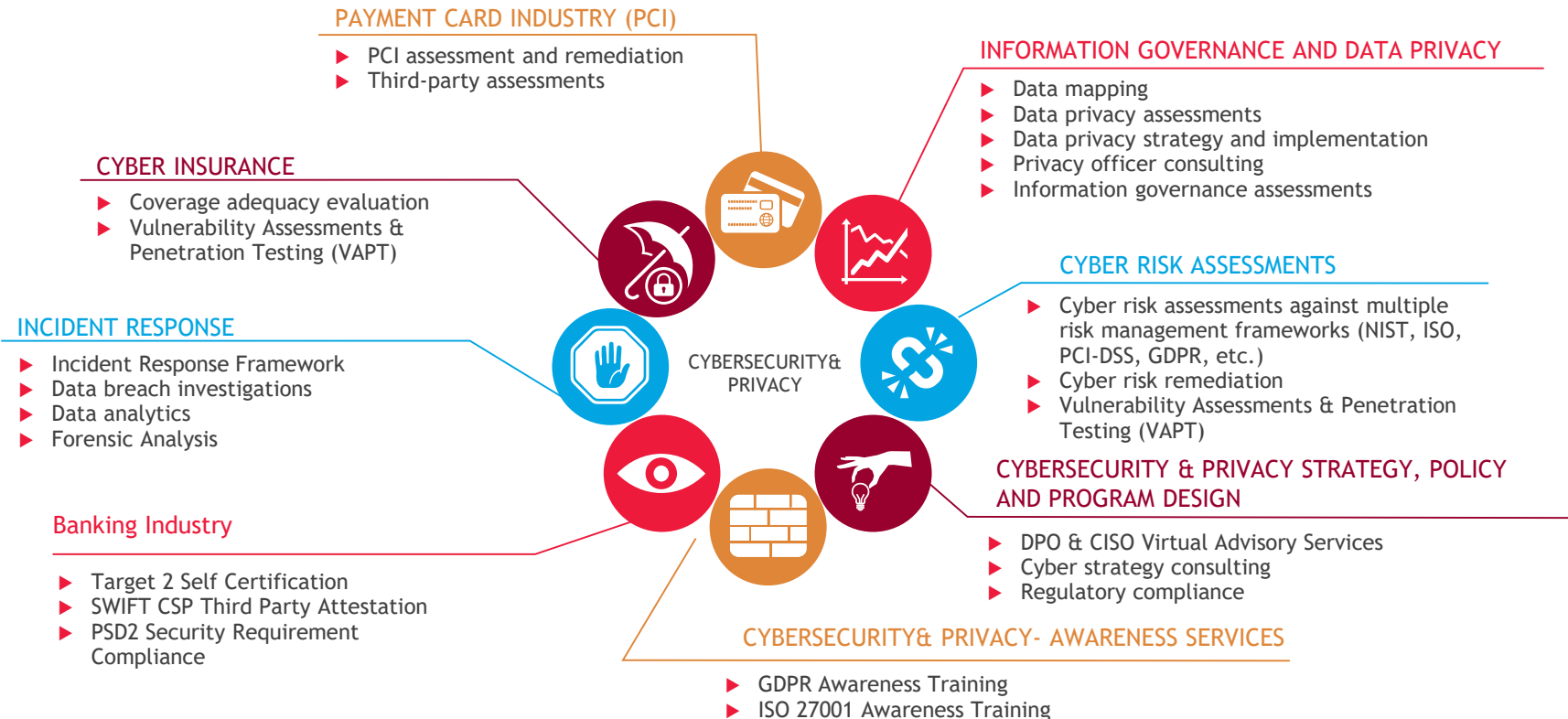
Answering the question, "Is an organization secure?" requires a comprehensive assessment of its operating environment and its specific business needs. Ultimately, implementing a cost-effective Cybersecurity framework includes careful consideration of how you identify, protect, and recover critical assets, as well as detect and respond to security breaches.

Conducting risk assessments, planning incident response, and establishing governance structures - all begin by asking the right questions:

- ▶ What type of critical data does your company generate and use?
- ▶ Who requires access to that data?
- ▶ Where is that data vulnerable to a breach?
- ▶ Do you have an established definition of a security breach?
- ▶ What notification obligations do you have in the event of a breach?
- ▶ What are your current Cybersecurity policies and procedures, and how are they governed and maintained?

Comprehensive Cybersecurity Portfolio Of Services

Our full spectrum of services operates in a continual process of risk remediation and security posture improvement.



Cybersecurity Services Descriptions

CYBER RISK ASSESSMENT & SECURITY TESTING

Assess risks and identify vulnerabilities to digital assets; evaluate potential impact and exposure, prioritizing risks against the costs of protection. Includes assessments, security testing, remediation, and executive-level reporting to guide security investments.

CYBER RISK MANAGEMENT STRATEGY & PROGRAM DESIGN

Design and implement a comprehensive program aligned with an existing enterprise risk management framework. Includes strategy, organizational structure, governance, policies and procedures, training, and both internal and external communications.

DATA PRIVACY & PROTECTION

Establish compliance with evolving global data privacy and protection regulations in alignment with an organization's existing practices. Implement technology and protocols with applicable data privacy policies in accordance with country-specific data protection requirements, leveraging BDO resources in over 150 countries.

SECURITY ARCHITECTURE & TRANSFORMATION

Design and implement a cybersecurity architecture and framework tailored to business needs and the enterprise ecosystem. Encompasses access controls, entitlement, data protection, security monitoring, data privacy, and the selection and implementation of security tools.

INCIDENT RESPONSE PLANNING

Develop and test comprehensive incident response plans to minimize the impact of a data breach. Considers company processes, as well as roles and responsibilities of individuals throughout the organization.

CYBER INSURANCE CLAIM PREPARATION & COVERAGE ADEQUACY EVALUATION

Identify and quantify incurred event response costs for inclusion and submission in an insured entity's claim. Pre-loss services include measuring estimated response costs related to data breach scenarios to assist in evaluating cyber insurance coverage.

BUSINESS CONTINUITY PLANNING & DISASTER RECOVERY

Develop and test company-wide business continuity and disaster recovery plans for critical systems, applications, infrastructure, facilities, people, and business processes.

CYBER INVESTIGATIONS

Rapid response to breach incidents, including identification of cause and implementation of remediation measures for affected areas, as well as expert testimony when needed.

MONITORING, DETECTION, & RESPONSE (MDR) SERVICES

24x7x365 Continuous monitoring and diagnostic services available via BDO's three global Security Operation Centers located in Tel Aviv, Israel.

CYBERSECURITY CUSTOMIZED EDUCATION & TRAINING PROGRAMS

Customized cybersecurity education and training programs for executives to the entire organization. Available on-line, via webinars, and/or classroom training. Instructed by world-class cybersecurity experts.

Cyber risk assessment

THE CLIENT CHALLENGE

Cybersecurity threats are on the rise for organizations of all sizes and in all industries, and regulators, industry associations, and the federal government have begun to take action, issuing attestation guidelines and regulatory mandates surrounding organizational cybersecurity programs.

With concern growing among stakeholders, there's building pressure for companies to prove they have effective controls in place. Businesses must be able to detect and mitigate cyber breaches that have the potential to disrupt business operations, damage their brand, and cause significant financial losses.

Obtaining a comprehensive cyber risk assessment allows an organization to understand the current state of its cyber program, identify potential gaps and risks, and ultimately implement an effective cybersecurity framework. Risk assessments should evaluate:

- ▶ **Application Security.** Are your applications protected from outside threats?
- ▶ **Data Protection.** Do you know where your sensitive data is stored and how it is protected?
- ▶ **Identity and Access Management.** How well do you control who accesses your systems and data?
- ▶ **Infrastructure Management.** How well is your network protected?
- ▶ **Event Management.** Do you know what to do if there is a cyber breach?
- ▶ **Vendor Management.** What are the security practices of third party vendors who have access to your systems and data?
- ▶ **Training.** How aware are your people about their cyber responsibilities?

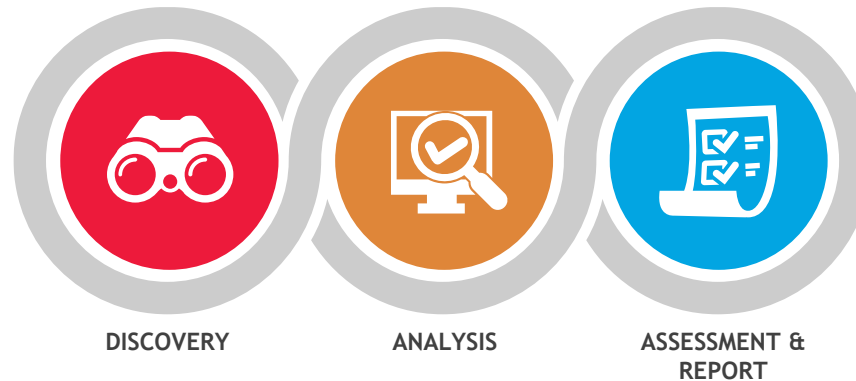


A risk assessment and gap analysis can be used as the basis for an action plan in case of a cyber breach.

Cyber risk assessment

THE BDO APPROACH

BDO integrates select components of the major cybersecurity frameworks, including ISO27K, NIST and AICPA measuring against regulatory and legal guidance and requirements such as HIPAA, and GDPR, to optimize risk mitigation. This approach results in a comprehensive program and maximizes alignment across the organization.



DISCOVERY

- ▶ Collect relevant policies, standards, procedures, infrastructure/ network diagrams, previous assessments and audit reports.
- ▶ Interviews are conducted to gather valuable information to support the Analysis phase.

ANALYSIS

- ▶ Review collected data and assess it against HIPAA or HITRUST requirements to determine compliance and vulnerabilities.
- ▶ If a vulnerability is found, level of risk is determined and potential threats enumerated. Gaps and vulnerabilities found will be further explored and validated during the Assessment phase.

ASSESSMENT & REPORT

- ▶ Validate the extent to which all vulnerabilities discovered exist and determine the risk rating. Provide a detailed risk report that describes the assessed areas and their strengths and weaknesses.
- ▶ Identified weaknesses are described in detail, including recommendations for remediation measures to achieve compliance with both regulations and standards.

Cyber risk assessment

THE BDO APPROACH: CYBER RISK ASSESSMENT

BDO integrates select components of the major assessment frameworks to optimize risk mitigation unique to organizations, and focuses on maximizing alignment among varying stakeholders, including compliance, legal, IT security, finance, and operations. This provides a comprehensive plan to be utilized in measuring compliance against both the regulations and the widely recognized industry standards.

BDO's cyber risk assessment includes the following approach:



DISCOVERY

Collect relevant policies, standards, procedures, infrastructure/network diagrams, previous assessments and audit reports.

Interviews are conducted to gather valuable information to support the Analysis phase.



ANALYSIS

Review collected data and assess it against ISO 27002 requirements to determine compliance and vulnerabilities. If a vulnerability is found, level of risk is determined and potential threats enumerated. Gaps and vulnerabilities found will be further explored and validated during the Assessment phase.



ASSESSMENT & REPORT

Validate the extent to which all vulnerabilities discovered exist and determine the risk rating. Provide a detailed risk report that describes the assessed areas and their strengths and weaknesses. Identified weaknesses are described in detail, including recommendations for remediation measures to achieve compliance with both regulations and standards.



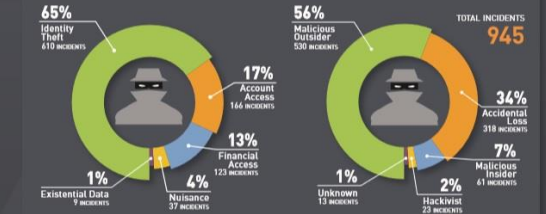
DATA RECORDS COMPROMISED IN FIRST HALF OF 2018

4,553,172,708

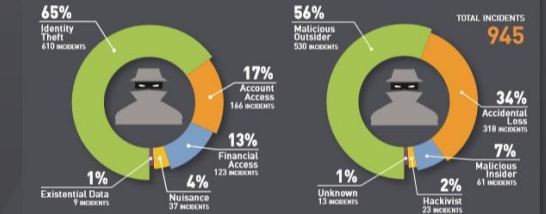
25,155,650 records lost or stolen every day
1,048,152 records every hour
17,469 records every minute
291 records every second

LESS THAN 3% of breaches were "Secure Breaches" where encryption rendered the stolen data useless

Number of Breach Incidents by Type



Number of Breach Incidents by Source



Number of Breach Incidents by Industry



Incident response

BDO's Cybersecurity Incident Response Team responds rapidly to breach incidents by performing digital forensics and cyber investigations to identify the cause and implement remediation measures, as well as provide expert testimony when needed.

Whether the cyber threat is an Advanced Persistent Threat (APT), intrusion or targeted attack, we identify the "who," "what," "when," "where," and "how" of the attacker. Leveraging our forensic investigation and threat intelligence experience and utilizing analytic tools and techniques, we identify compromised systems and impacted individuals, determine breach scope and data loss, and advise on containment and remediation measures.

Our professionals have a diverse range of backgrounds, including experienced cyber investigators, former law enforcement, technology professionals, operations, and data privacy consultants, as well as forensic technology, business advisory, and accounting practitioners.

We are built to provide comprehensive, customized services for each client, focusing on an organization's specific operating model, technical demands, regulatory environment, and industry dynamics.

Our services also include incident response planning to minimize the impact of a future breach. We work with organizations to develop and test comprehensive incident response plans, considering company processes, as well as roles and responsibilities of individuals throughout an organization.



INCIDENT RESPONSE SERVICES:

- ▶ Forensic investigation and root-cause analysis
- ▶ Incident containment
- ▶ Threat intelligence
- ▶ Remediation and recovery
- ▶ Security policy development & rollout
- ▶ First responder training
- ▶ Expert testimony

Cybersecurity strategy & mitigation plans

ADDRESSING DATA SECURITY RISKS AND VULNERABILITIES

Over the last decade, data breaches impacting customer information, financial data, and other types of sensitive and confidential data, have risen to a new level of security risk.

An enterprise ecosystem is comprised of many players, each with a significant role in the processing of a transaction. When a transaction occurs, all players in the value chain are involved.

Along to continuum of the ecosystem are three “states” of data that can be affected during a breach, including static data, internal data transfer and external data transfer. All parties involved may be vulnerable to a breach, and require appropriate protective measures.

IDENTIFYING AND MANAGING SECURITY RISKS

BDO's Information Security Framework, which includes identification, protection, detection, response, and recovery, are implemented to effectively assess an organization's IT applications and infrastructure to mitigate the risk of a data breach.

Our technology specialists perform security risk assessments that align with cybersecurity controls subject to the industry security standards. Using standard scoring methodologies focused on prioritizing investment areas, BDO designs and develops solutions that address all components of the Information Security Framework.

In addition, our team can also assist clients to develop a security strategy, security solutions architecture and framework, security implementation plan, security policies, third party risk analysis procedures, customer engagement models (to curb reputational pitfalls), as well as organizational structures related to information security that establish appropriate levels of system access.



SERVICES:

- ▶ Cybersecurity strategy and program
- ▶ Security risk assessment
- ▶ Information security policies & standards
- ▶ IT risk structure optimization
- ▶ Information security process optimization
- ▶ Identify & access management
- ▶ Entitlement management
- ▶ Data protection & privacy
- ▶ Vendor risk management
- ▶ Customer engagement strategy

Cyber Investigations

DATA BREACH. NOW WHAT?

Cyberattacks and media attention around data breaches are leaving organizations vulnerable to the risks of data loss or exposure.

BDO's Forensic Technology Services specialists help clients respond to data breach incidents by finding out "who" did "what," "when" and "how." We identify and locate relevant data, preserve it for use and analyze it in our secure on-site forensics lab. We can also recover and reconstruct missing or deleted data.

Without the proper system configuration and management, sensitive data can be leaked or hacked by outside and inside sources. BDO's team of technology specialists work with clients to identify high risk vulnerabilities in their IT infrastructure, and provides professional guidance on how to minimize the risks.

ESTABLISHING INFORMATION GOVERNANCE

Information is often a corporation's most valuable asset. BDO helps clients protect and manage their information by developing proper controls and safeguards across the enterprise.

With backgrounds in investigations, compliance, information management, e-discovery, auditing and technology solution development, BDO provides a strong foundation to help organizations develop a comprehensive governance, risk, and compliance program.

Our professionals draw upon deep industry expertise, working with clients to develop pragmatic and repeatable processes, policies, and solutions.



SERVICES:

- ▶ Identification, preservation & collection
- ▶ Data culling
- ▶ Data processing
- ▶ Review & production
- ▶ Multinational / multilingual reviews
- ▶ Assessments:
 - External host
 - Web application
 - Internal server
 - Wireless security
 - Spear phishing & data exfiltration
 - Physical security & environmental
- ▶ Social engineering & dumpster diving

Cybersecurity solutions

CYBER ATTACKS: INCREASINGLY LIKELY, POTENTIALLY CATASTROPHIC

Organizations are highly vulnerable to the increasing number of attacks from sophisticated cyber criminals. Protecting sensitive information is critical and large amounts of Personally Identifiable Information (PII) are of increasing value surpassing even credit card data in value.

Information sharing is fundamental to virtually every aspect of business. As you focus on engaging others in your mission, information sharing with vendors, contractors, partners, members and the public in general has grown and is essential to your success. And every one of these digital relationships presents a new set of cyber vulnerabilities.

The need for security and the way in which it is implemented must be balanced, thoughtfully, against the needs of an organization to operate effectively, and to actively pursue its mission.

While it is impossible to eliminate all risk of cyber attack, a well-designed program will minimize the negative impact on both short-and long-term business goals.

CYBER RISKS: UNIQUE TO EVERY ORGANIZATION BUT CRITICAL TO NONPROFITS

Answering the question, “Is an organization secure?” requires a comprehensive assessment of its operating environment and its specific business needs.

Ultimately, implementing a cost-effective cybersecurity framework includes careful consideration of how you identify, protect, and recover critical assets, as well as detect and respond to security breaches. Conducting risk assessments, planning incident response, and establishing governance structures - all begin by asking the right questions:

- ▶ How do we protect our donors' and/or members' information?
- ▶ How do we ensure that our agents and vendors do not compromise our systems?
- ▶ Who requires access to which data?
- ▶ Where are the particular points of vulnerability?
- ▶ Do you have an established definition of a security breach?
- ▶ What notification obligations do you have in the event of a breach?
- ▶ What are your current policies and procedures, and how are they governed and maintained?



Implementing a cost-effective cybersecurity framework includes careful consideration of how you identify, protect, and recover critical assets, as well as detect and respond to security breaches.

Vulnerability assessment and penetration testing (VAPT) services

Our security team has built a reputation that focuses on providing advisory services that reduce the cost and complexity of compliance. Clients can greatly benefit from our experience, both before and after the actual assessment or vulnerability scan—from our complimentary pre-engagement scoping consultations to our spot check programs; we add value to your organization.

We offer the following information security services:

- ▶ **Internal and/or external vulnerability assessments** - utilizing the most respected commercial and open source tools available managed and reviewed by information security veterans
- ▶ **Quarterly vulnerability assessments** - performed by a PCI certified approved scanning vendor (ASV)
- ▶ **Annual penetration testing** - internal and external penetration testing from information security experts
- ▶ **Information security training** - customized training for security topics ranging from secure coding to performing self-testing
- ▶ **Security assessments and risk assessments** - fundamental assessments of the entire organization from an IT security or overall IT risk perspective
- ▶ **Remediation assistance & evaluation services** - compensating control guidance and security solution reviews
- ▶ **PCI annual compliance validation and reporting** - in accordance with the PCI-DSS standard for organizations of any size (levels 1 through 4)
- ▶ **NERC critical infrastructure protection (CIP)** - readiness and assessments against the latest approved standards provided by the North American Electric Reliability Corporation
- ▶ **Forensic investigations** - forensic gathering, evaluation and testimony for information security investigations
- ▶ **Strategic planning** - short-term and long-term visioning for security compliance or the organization's security blueprint
- ▶ **ISO 27001** - Readiness Assessment against the standards established by the International Standards Organization
- ▶ **Threat profiling** - identify the threats which an organization is subject to by evaluating the company as a target, their business and technical footprint, and types of operations
- ▶ **Red Teaming and Blue Teaming** - going beyond standard penetration testing, Red Teaming (offensive strategies using real-world attack scenarios) and Blue Teaming (defensive strategies) help organizations significantly improve their security position

Vulnerability assessment and penetration testing (VAPT) services

- ▶ **Vulnerability Scanning and Penetration Testing Toolsets.** Our senior security team utilizes the most recognized and awarded commercial toolsets available in addition to the most well-respected open source security tools to perform our testing. The right tools - in the right hands.
- ▶ **Veteran Security Team.** The security team is experienced and each member has years of information security expertise, including offensive and defensive security skills. They are also educators, trainers and speakers within the information security field and are highly active in the security community.
- ▶ **Proper Preparation.** We will take the time to understand the client environment and the boundaries, extensions and relationships of your network. We do not simply ask for a list of IP addresses to test. We look for ways to help reduce the scope of the environment that needs testing.
- ▶ **Two-Way Communication.** We consider the answering of your periodic vulnerability, security or compliance questions to be an important part of our service. We keep an open line of communication with your company.
- ▶ **Proper Debrief.** We do not just 'hand-off' the final report, we ask to properly debrief you on the results so that you understand the vulnerabilities and the risks we've discovered. We share our knowledge and expertise with our client, so that personnel and environmental improvements can be made at the organization.
- ▶ **Vulnerability Management.** We do not try to perform vulnerability assessments as a one-time project. We want to be a part of your vulnerability management program. Not only do we want to assist you in maintaining your quarterly vulnerability compliance requirements, but we also want to help you manage your vulnerabilities. We look beyond the compliance requirements and provide metrics to determine the effectiveness of your patch management process and the posture of your organization's overall security program.
- ▶ **Penetration Testing.** The Penetration testing is the next logical step, and sometimes can be the first step, to vulnerability scanning. Often, an organization might deem the identified systems as non-critical or of little value; however, the penetration testing may reveal that by exploiting a non-critical (or low-value) system, an attacker can pivot from the exploited system into other systems that are important to the organization.



Our primary goals are to identify, risk-rank, and provide solutions to internal and/or external information security risks.

PCI - assessment, testing & other security requirements

Our security team has built a reputation that focuses on providing advisory services that reduce the cost and complexity of compliance. Clients can greatly benefit from our expertise both before and after the actual assessment or vulnerability scan — from our complimentary pre-engagement scoping consultations to our spot check programs; we add value to your organization.

At BDO, we offer the following information security services:

- ▶ **Internal and/or external vulnerability assessments** - utilizing the most respected commercial and open source tools available managed and reviewed by information security veterans
- ▶ **Quarterly vulnerability assessments** - performed by a PCI certified approved scanning vendor (ASV)
- ▶ **Annual penetration testing** - internal and external penetration testing from information security experts
- ▶ **Information security training** - customized training for security topics ranging from secure coding to performing self-testing
- ▶ **Security assessments and risk assessments** - fundamental assessments of the entire organization from an IT security or overall IT risk perspective
- ▶ **Remediation assistance & evaluation services** - compensating control guidance and security solution reviews
- ▶ **PCI annual compliance validation and reporting** - in accordance with the PCI DSS standard for organizations of any size (levels 1 through 4)
- ▶ **Incident Response** - develop a plan of response and communications in answer to a security event



As industry leaders in the fields of information technology risk and information security, the skilled professionals at BDO understand the complexity and importance of vulnerability scanning and penetration testing as they provide valuable insight into an organization's security posture.

PCI - scanning & penetrations testing

The primary goals of our vulnerability assessment and penetration testing services are to identify, risk-rank and provide solutions to internal and/or external information security risks. We provide solutions to your security needs by offering the following:

VULNERABILITY SCANNING AND PENETRATION TESTING TOOLSETS

Our senior security team utilizes the most recognized and awarded commercial toolsets available in addition to the most well-respected open source security tools to perform our testing. The right tools – in the right hands.

VETERAN SECURITY TEAM

The security team is experienced and each member has years of information security expertise, including offensive and defensive security skills. They are also educators, trainers and speakers within the information security field and are highly active in the security community.

PROPER PREPARATION

We will take the time to understand the client environment and the boundaries, extensions and relationships of your network. We do not simply ask for a list of IP addresses to test. We look for ways to help reduce the scope of the environment that needs testing.

TWO-WAY COMMUNICATION

We consider the answering of your periodic vulnerability, security or compliance questions to be an important part of our service. We keep an open line of communication with your company.

PROPER DEBRIEF

We do not just ‘hand-off’ the final report, we ask to properly debrief you on the results so that you understand the vulnerabilities and the risks we’ve discovered. We share our knowledge and expertise with our client, so that personnel and environmental improvements can be made at the organization.

VULNERABILITY MANAGEMENT

We do not try to perform vulnerability assessments as a one-time project. We want to be a part of your vulnerability management program. Not only do we want to assist you in maintaining your quarterly vulnerability compliance requirements, but we also want to help you manage your vulnerabilities. We look beyond the compliance requirements and provide metrics to determine the effectiveness of your patch management process and the posture of your organization’s overall security program.

PENETRATION TESTING

The penetration testing is the next logical step, and sometimes can be the first step, to vulnerability scanning. Often, an organization might deem the identified systems as non-critical or of little value; however, the penetration testing may reveal that by exploiting a non-critical (or low-value) system, an attacker can pivot from the exploited system into other systems that are important to the organization.

APPROVED SCANNING VENDOR VULNERABILITY SCANNING SERVICES

BDO understands the complexity and importance of vulnerability scanning as it relates to PCI requirements as well as the security posture of an organization. We do not perform the scans merely to check off that they have been performed; rather, we strive to deliver useable and understandable recommendations.

Approved scanning vendor vulnerability scanning services

Clients can greatly benefit from our expertise both before and after the actual PCI assessment or Approved Scanning Vendor (ASV) vulnerability scan.

SOLUTIONS FOR YOUR PCI/ASV NEEDS

Our PCI and ASV team has built a reputation that focuses on providing advisory services that reduce the cost and complexity of PCI compliance. Clients can greatly benefit from our expertise both before and after the actual PCI assessment or ASV vulnerability scan — from our complimentary pre-engagement scoping consultations to our spot check programs; we add value to your organization.

We offer the following PCI/ASV compliance services:

- ▶ **Annual Compliance Validation & Reporting** - in accordance with the PCI- DSS standard for organizations of any size (levels 1 through 4)
- ▶ **Quarterly Vulnerability Assessments** - performed by a PCI certified ASV
- ▶ **Annual Penetration Testing** - internal and external penetration testing from information security experts
- ▶ **PCI Program Management to Merchants & Service Providers for Complex Partner & Parent/Child Organizations** — facilitation of the overall PCI program for your organization
- ▶ **Readiness Assessment** - pre-engagement scoping, hot spots and Q&A sessions
- ▶ **Remediation Assistance & Evaluation Services** - compensating control guidance and solution reviews, security infrastructure selection and implementation, policy and procedure development
- ▶ **Scope Reduction Services** - minimizing the scope of PCI compliance in your environment
- ▶ **Spot Check Programs** - maintenance and spot checking of your PCI activities
- ▶ **Strategic Planning** - short-term and long-term visioning for PCI compliance
- ▶ **PCI Compliance Optimization and Training** - organizational efficiency and optimization assistance to reduce the PCI impact

ISO/IEC 27001 Security Standard, “the facts”

- ▶ International standard that defines the requirements for an Information Security Management System (ISMS)
- ▶ ISMS is a risk management framework that ensures processes are in place for the identification, classification and mitigation of risks
- ▶ All components of the ISMS are mandatory
- ▶ The standard also includes 14 DOMAINS 35 CONTROL OBJECTIVES AND 114 DETAIL CONTROLS
- ▶ An organization must formally declare which controls are applicable to them
- ▶ The controls that are not applicable must also be justified based on the outputs from the ISMS
- ▶ The ISMS and the controls defined in the Statement of Applicability define the scope of certification
- ▶ Consider the reasons for certification and then carefully define the scope
- ▶ Organization wide involvement (Senior management commitment, HR processes, physical security, training and awareness, compliance with legal and regulatory obligations, third party management are all assessed)
- ▶ Accountability for ISMS outside of IT (depending on scope) - IT controls are a big part of managing Information security risk but not the only consideration
- ▶ Training and awareness is key
- ▶ Focus on risk management - compliance should be a by-product
- ▶ Do not look for short cuts - you need to be able to manage this when the consultants are long gone
- ▶ Expect to embed the ISMS over 3-5 years - it will continually improve but needs the resources to do this

ISO 27001 certification process

BDO will identify and investigate vulnerabilities that pose a risk to the organization's information technology infrastructure and environment. The assessment will consider both the security and adequacy of its technologies.

The certification process is a continuous one which calls for the active involvement of the organization. This process is made up of four phases. The various phases together form one PDCA (Plan - Do - Check - Act) cycle.

We believe in forming a team with our clients so that we have both the necessary relationships within the company to properly use our expertise, and to provide security and assessment services in a way that provides the results required while minimizing the impact on the organisation's IT infrastructure and business operations.

ISO 27001 is international standard that defines the requirements for an Information Security Management System (ISMS), a risk management framework that ensures processes are in place for the identification, classification and mitigation of risks.

All components of the ISMS are mandatory. The standard also includes a list of controls across from which an organization must formally declare the ones applicable to them. Those controls that are not applicable must also be justified based on the outputs from the ISMS. The ISMS and the controls defined in the Statement of Applicability define the scope of certification.

There are some steps along the way to certification that need to be done in a certain order otherwise the right information won't be available in later stages.

The approach shown effectively steps through the standard provided a top management decision is provided.



BDO performs risk assessment based on recognized standards ISO31000/27005.

This process follows the following steps:

1. Identifying the risk area (context) by charting the critical processes and operational resources;
2. Risk assessment by means of a business impact analysis and threat analysis;
3. Risk management plan;
4. Risk acceptance;
5. Risk communication;
6. Continuous improvement;

ISO 27001 & 27002

- ▶ ISO27001 formally specifies how to establish an Information Security Management System (ISMS).
- ▶ The adoption of an ISMS is a strategic decision.
- ▶ The design and implementation of an organization's ISMS is influenced by its business and security objectives, its security risks and control requirements, the processes employed and the size and structure of the organization: a simple situation requires a simple ISMS.
- ▶ The ISMS will evolve systematically in response to changing risks.
- ▶ Compliance with ISO27001 can be formally assessed and certified. A certified ISMS builds confidence in the organization's approach to information security management among stakeholders.
- ▶ ISO27002 is a "Code of Practice" recommending a large number of information security controls.
- ▶ Control objectives throughout the standard are generic, high-level statements of business requirements for securing or protecting information assets.
- ▶ The numerous information security controls recommended by the standard are meant to be implemented in the context of an ISMS, in order to address risks and satisfy applicable control objectives systematically.
- ▶ Compliance with ISO27002 implies that the organization has adopted a comprehensive, good practice approach to securing information.



Virtual CISO

[“A virtual CISO \(vCISO\) can bring both strategic and operational leadership on security to companies that can't afford a full-time person in the role”](#)

Not all organizations have the resources to onboard a full time Chief Information Security Officer (CISO), but still, cyber security and cyber security risk management are critical factors of resiliency. The cost-effective “vCISO” can be the most realistic approach for managing all the risks such organizations undertake.

Our security team can just be the right solution for such cases. Utilizing our expertise and leadership in Cyber Security can help you identify and mitigate vulnerabilities, establish security best practices, and implement the right technology to protect your business operations. Our vCISO entails years of security experience that can be made available either on-premise or virtually depending on your specific requirements. You have the benefit of our global network of security experts and practitioners that can define a comprehensive strategy, establish a clear technology roadmap and implement a strong security program to protect your business operations.

vCISOs are estimated to cost between 30 percent and 40 percent of a full-time CISO and are available on-demand. The benefits go well beyond cost. Virtual CISOs require no training and can engage instantly. In this model, it's purely about results, and vCISOs will provide reasonable KPIs and reporting.

They could help pull together security policies, guidelines and standards. That could entail anything from coming to grips with compliance, to staying on top of vendor risk assessment. They could also help recruit, set security strategies, procure solutions, remediate incidents, and put foundations in place for ISO 27001 compliance. They might also assist coaching newly established CISOs, or even managing the board relationship until a full time capable CISO can be onboarded.

vCISOs are the best fit for supplementing the existing management team or simply as an interim solution.



CYBER RISK: UNIQUE TO EVERY ORGANIZATION

Answering the question, “Is an organization secure?” requires a comprehensive assessment of its operating environment and its specific business needs. Ultimately, implementing a cost-effective Cybersecurity framework includes careful consideration of how you identify, protect, and recover critical assets, as well as detect and respond to security breaches.

Conducting risk assessments, planning incident response, and establishing governance structures - all begin by asking the right questions:

What type of critical data does your company generate and use?

Who requires access to that data?

Where is that data vulnerable to a breach?

Do you have an established definition of a security breach?

What notification obligations do you have in the event of a breach?

What are your current Cybersecurity policies and procedures, and how are they governed and maintained?

PCI data security standard

BUSINESS COSTS

If card holder data that you process, store or transmit is compromised you could face increased business costs from:

- ▶ Fines from your acquiring bank
- ▶ Increased processing fees
- ▶ Removal of your ability to accept payment cards
- ▶ Legal costs and settlements
- ▶ Loss of customer confidence in your organization

“HOW DO I COMPLY?”

Complying with the PCI DSS can appear to be a daunting task, however it does not need to be. Our Qualified Security Assessors (QSA) can help guide you to understanding your risks and achieving PCI DSS compliance in a manageable and cost-effective way.

To ease the process of validating compliance, Self-Assessment Questionnaires (SAQ) have been developed by the PCI Security Standards Council. The SAQ required will depend on the types of transactions supported and whether cardholder data is stored. If an organization meets certain criteria (for example over six million Visa or MasterCard transactions in a year), a Report on Compliance (ROC) must be completed by an external QSA, such as BDO, or a certified and independent Internal Security Assessor (ISA) to validate compliance.



All organizations that store, process or transmit payment card details must comply with the payment card industry data security standard.

PCI data security standard

OUR APPROACH

BDO has been accredited by the PCI Security Standards Council as a Qualified Security Assessor (QSA). Through working closely with you and understanding your business, we can help you reach and maintain compliance in an efficient and effective way.

Our four phase model provides structure to the compliance process without employing a one-size-fits-all approach. We tailor our approach to your needs. The requirement to be compliant does not end when the forms have been signed. Compliance must be maintained 24 hours a day, 365 days a year. BDO provides on-going support and advice to help you maintain compliance.

Our four phase model provides structure to the compliance process without employing a one-size-fits-all approach:

PHASE 1: IDENTIFY YOUR COMPLIANCE REQUIREMENTS

- ▶ Work with you to establish where payment card data enters your organization, how it is processed, where it is stored and the associated risks
- ▶ Ascertain which SAQ is appropriate for your environment, or whether you will need a ROC
- ▶ Determine, and where possible reduce, the networks and systems in scope for PCI DSS

PHASE 2: REVIEW CURRENT PRACTICE AGAINST YOUR COMPLIANCE REQUIREMENTS

- ▶ Perform a gap analysis against the standard or appropriate SAQ
- ▶ Identify where you meet the standard, and where current processes and implementations do not
- ▶ Work with you to establish a roadmap to compliance and identify any compensating controls
- ▶ Confirm compliance program with your bank where necessary

PHASE 3: WORK TOWARDS COMPLIANCE

- ▶ Provide guidance in following the roadmap to compliance
- ▶ Provide assistance on changes to business processes and documentation
- ▶ Participate in project meetings to provide ongoing advice on the implementation of PCI DSS compliant solutions

PHASE 4: REPORTING AND ONGOING COMPLIANCE

- ▶ Review against the standard or SAQ to ensure that all areas meet compliance
- ▶ Assist with the completion of the Attestation of Compliance and complete a ROC as necessary
- ▶ Work with you to develop a process to ensure ongoing compliance

AICPA SOC for cybersecurity

Not that long ago, cybersecurity was deemed the responsibility of those in the IT department.

Today, however, C-suite executives and boards of directors are becoming increasingly involved in their organizations' cyber risk management—realizing cybersecurity is not just an IT issue, it's an enterprise-wide risk that must be identified, assessed, and managed in order to mitigate the risk of business interruption, reputational damage, and significant financial losses.

With cyber threats on the rise for companies of all sizes in all industries, the American Institute of CPAs (AICPA)—with help from BDO—developed the System and Organization Controls (SOC) for Cybersecurity framework, which provides a standard method for reporting enterprise-wide cyber risk management and helps organizations communicate the effectiveness of their cyber programs to key stakeholders. The framework establishes a set of benchmarks, known as description criteria, that organizations can use as guiding principles to define their cybersecurity objectives and design a corresponding cyber risk management program to meet those objectives.

Early adoption of the AICPA's cyber risk management reporting framework provides companies with a competitive advantage in retaining and attracting clients, enabling them to demonstrate the effectiveness of their cyber risk management programs, and ability to safeguard sensitive client information in advance of a breach.

A McKinsey Global Survey indicated that over half of executives interviewed believe that cybersecurity is a strategic risk for their companies. Yet only 5 percent of companies' report "mature" or "robust" cybersecurity risk management maturity capabilities.

As with any compliance challenge, knowing who to turn for help is mission critical. At BDO, we're committed to helping our clients with all their risk mitigation demands—and especially with a cybersecurity risk management program. BDO will:

- ▶ Work with you and your team to help you develop and implement cybersecurity controls appropriate for your organization
- ▶ Help you benchmark the current cyber state of your organization with this framework
- ▶ Provide assurance with an annual audit of your company's cybersecurity risk management program



According to the managing partners of more than 70 of BDO's 400+ Alliance CPA firms,

71%

believe their firm has at least a medium level of exposure to cyber threats.

However ...

40%

have not conducted a cyber risk assessment in the past 18 months.

42%

have no written cyber policy in place.

46%

have not inventoried their firm's sensitive data.

AICPA SOC for cybersecurity

BDO SERVICES



Readiness Assessment and Gap Analysis

In preparation for a SOC for Cybersecurity attestation, conducting a readiness assessment is key to understanding an organization's level of preparedness to preemptively address any issues that could result in a qualified opinion from an auditor. BDO's team of highly-skilled advisors helps clients identify gaps and strengthen their cyber risk management programs by:

- ▶ Utilizing AICPA criteria and guidance to identify and remediate deficiencies in controls.
- ▶ Conducting a readiness assessment to benchmark the current state of an organization's cyber program against the SOC for Cybersecurity framework, identifying gaps and key risk areas, and recommending remediation strategies that align with the SOC attestation standards.



Independent Cyber Risk Examination

BDO conducts cybersecurity risk management examinations and provides clients with attestation services in accordance with AICPA standards including an opinion on an organization's description of its efforts and the effectiveness of its controls. By aligning with the rigors of SOC attestation, an independent cyber risk examination:

- ▶ Serves as an independent third-party assessment of the design and operating effectiveness of an organization's internal controls.
- ▶ Combines cyber-savvy with the accounting industry knowledge of the audit process, and expands assessment beyond financial impact to enterprise-level risk management.
- ▶ Provides a higher level of assurance to management and boards, or interested outside parties, and can be used to inform the purchase of cyber liability coverage under various types of insurance policies.

No approach can prevent a cybersecurity threat or breach. BDO can, however, assist you and your board by adding substantial credibility to assertions made by management about your cybersecurity risk management program. As the saying goes, "That which is measured, improves." Consequently, in addition to enhancing the credibility of the information provided, a periodic, independent examination of the effectiveness of those controls can often improve the diligence with which an entity performs those controls. If you don't have a game plan—we're ready to help. If you do, we would be happy to review it with you.

Managed cybersecurity services

Monitoring, detection, and response

Any firm with zero tolerance to loss of confidential data should adopt a prepared and proactive posture to countering espionage and data theft with a dynamic concept of cyber defense which incorporates “real time” capability.

The role of monitoring and detection is central to any advanced cyber defense concept, and establishing resilience requires the ability to detect, react, defend, and recover from a targeted cyber intrusion or attack with a minimal impact to the organization.

BDO SOLUTIONS

BDO can provide and manage a full range of security operations functions on a remote basis from our Cybersecurity Operations Center, whether you just need security operations center (SOC) services, or security information and event management (SIEM) services

as well. Our services can be tailored to your environment, nature of operations, and the specific cyber risks that you face, and our onboarding process will identify how best to achieve your objectives and related advisory services to quickly realign your processes to integrate the new capabilities.

We can adapt our processes, outputs, and solutions to suit almost any requirement including specific staffing, threat intelligence, and technology demands. Our services can evolve as you do, with additional modules.

EMAIL & NETWORK ATTACK DETECTION & MONITORING

- ▶ Event collection
- ▶ Event preservation
- ▶ Correlation-based alerting
- ▶ Standard security devices collection
 - Active Directory
 - Firewall
 - Antivirus
 - Proxy
- VPN
- Critical servers
- ▶ Selected KPI's per device
- ▶ Technical intelligence
- ▶ Dashboard per device
- ▶ Portal access for forensics
- ▶ Expert analyst services

SOC AS A SERVICE

- ▶ Alert analysis and response
- ▶ 24x7 service
- ▶ Expert analyst services
- ▶ Responder on call (SLA)
- ▶ Hunting services
- ▶ Case reporting
- ▶ Cyber resilience advisory

SIEM AND SOC AS A SERVICE

- ▶ Includes both SIEM and SOC
- ▶ 24x7 service
- ▶ Alerts workflows creation
- ▶ Expert analyst services
- ▶ Operator services
- ▶ Responder services (SLA)
- ▶ Threat hunting services
- ▶ Continuous content creation (rules, reports alerts)
- ▶ Additional security device collection

Managed cybersecurity services

Monitoring, detection, and response (cont.)

CYBER EVENT AND INFORMATION MANAGEMENT

SIEM projects are costly, complex, and—in most cases—not very effective. BDO helps clients simplify these projects by deploying best-in-class technologies with verified use cases for monitoring, using the latest technologies for correlation and analytics.

Our advanced services allow the custom collection of both traditional and home-grown applications, creating custom SIEM content, automation capabilities, and procedures. This offers:

- ▶ Flexible architecture
- ▶ Connecting to custom log sources
- ▶ Easy access to data collected
- ▶ Compliance reporting
- ▶ Accessible forensics
- ▶ Advanced analytics
- ▶ Advanced use cases
- ▶ Correlation for noise reduction
- ▶ False positive continuous reduction

SOC STAFF

Trained cyber professionals are hard to recruit and even harder to retain. BDO offers a dedicated, shared, or hybrid team to monitor, manage, assist, identify, and/or resolve cyber incidents. Clients may use existing personnel or dedicated recruits for their SOC operations. We offer:

- ▶ Flexible team models
- ▶ Incident monitoring
- ▶ Incident management
- ▶ Incident investigation
- ▶ Incident documentation
- ▶ Continuous process improvement

CUSTOM CYBERSECURITY TOOL DEVELOPMENT

Often, technology tools are deployed by expert integrators and, over time, lose their efficiency and relevance due to architectural, behavioral, or procedural changes.

The BDO Cybersecurity Center can deploy and monitor various security solutions for detection and response, deception, investigation, and forensics, as well as automated solutions related to detection and response. This provides:

- ▶ Reduced daily responsibilities for client team
- ▶ Dedicated monitoring
- ▶ Expert subject matter teams for specific solutions
- ▶ Reporting to SIEM platform for advanced correlations
- ▶ 24x7 monitoring capabilities

Cyber risk management

A holistic approach

It's all about managing risk.

What is commonly referred to as Cybersecurity is an evolution of Information Security in the context of an organization's risk management program. Cybersecurity needs to be managed consistently with other risk disciplines. Negative events are inevitable—that's why it's important to have controls in place to minimize the impact of those events, processes to quickly recognize they have occurred and a plan to manage their impact and recover.

A HOLISTIC VIEW

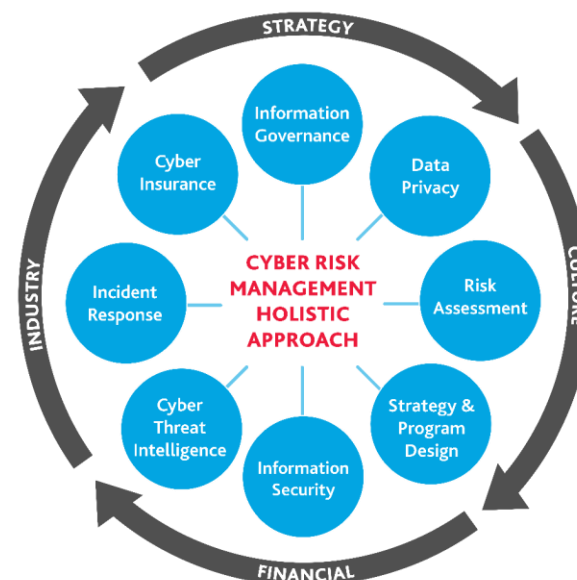
Core to any cybersecurity program is confidentiality, integrity, and availability, cyber risk management also encompasses principles to defend your reputation, finances, and at times life threatening situations. Therefore, in addition to core information security principles covering data protection, access control and entitlement, security monitoring, etc., other aspects of a cyber risk management program are as critically important.

In order to manage risk, you need to assess your risk. This assessment, combined with your organization's appetite for risk, will define your strategy and dictate the design of your risk management program. Once your program is defined you begin to get into the operational aspects of Cyber Risk Management.

Information Security also includes the processes and tools you utilize to protect against cyber attacks and to detect if you have been attacked. Cyber Threat intelligence keeps you abreast of the ever changing cyber environment and provides a basis for adjusting your protection and detection techniques.

As important as protection and detection are to the process which will be utilized when a cyber incident actually occurs, having a robust incident response plan for both pre- and post-event is key to minimizing the impact of an event

Finally, Cyber Insurance helps to manage the financial impact of a cyber event.



IT'S BUSINESS, NOT JUST TECHNOLOGY

When an organization narrowly focuses on cybersecurity it oftentimes mistakenly considers it to be a technology responsibility. Cyber Risk Management is a business responsibility. A holistic approach addresses how your cyber strategy needs to align with your business strategy. A holistic approach recognizes that people, and thus culture, is an important element. It also recognizes that your industry is a driver of your threats. Finally, a holistic approach understands that managing risk has a cost and must be funded.

ABOUT US

BDO's global reach

BDO GLOBAL STATISTICS 2018



WHY OUR CLIENTS CHOOSE US

Exceptional client service, without exception

It's our people, the knowledge they bring to engagements, their commitment to quality service, and the candid relationships they develop with clients that has made BDO the distinctive choice for professional accounting services for more than 100 years.

We can help our clients achieve extraordinary results through sound business and financial advice with our depth of services and the resources of our strong international reach.



Depth of
experience



Technical
knowledge



Open,
communicative
culture



Active
engagement
leaders



Exceptional
client service

BDO's Cybersecurity, Information Technology, & Forensics Services



Management & Technology Advisory

TECHNOLOGY OPERATIONS

- ▶ IT strategy & transformation
- ▶ Technology planning & transformation
- ▶ IT operations & financial management
- ▶ Digital transformation & strategy
- ▶ Technology roadmap & implementation

IT BUSINESS ENABLEMENT

- ▶ Software selection
- ▶ Strategy & Assessment
- ▶ Implementation Management

BUSINESS PERFORMANCE IMPROVEMENT

- ▶ Back office transformation
- ▶ Business process improvement
- ▶ Mergers & Acquisitions
- ▶ Post-merger integration
- ▶ Profit Enhancement Solutions (80/20 Roadmap)



Governance, Risk & Compliance

- ▶ Information governance and data privacy
- ▶ Cyber and information governance risk assessments
- ▶ Strategy, policy, and program design
- ▶ Information security - managed services
- ▶ Cyber threat intelligence and incident response
- ▶ Payment card industry (PCI), HI-Trust, HIPPA, AICPA, ISO, and other compliance




Forensic Technology

- ▶ Global E-discovery
- ▶ Digital forensics
- ▶ Expert witness testimony
- ▶ Data analytics and visualization (BDO Leverage)
- ▶ Artificial intelligence
- ▶ Project management



Data Analytics

- ▶ Data analytics and visualization
- ▶ Artificial intelligence/Machine Learning
- ▶ Software robotics and automation
- ▶ Business Intelligence
- ▶ Predictive Analytics & Modeling
- ▶ Robotic Process Automation



This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact BDO Ltd to discuss these matters in the context of your particular circumstances. BDO Ltd, its partners, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO Ltd, a Cyprus limited liability company, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name of the BDO network and for each of the BDO Member Firms.

Copyright © 2019 BDO Ltd. All rights reserved.

www.bdo.com.cy