E COM SECURITY®
SOLUTIONS

SOC 1 | SOC 2 | SOC 3

Compliance Management, Reporting and Certification

Reinforce confidence of your clients through demonstration of effective controls with an objective report that expresses an opinion about the control environment

www.ecomsecurity.org

You can outsource a process, but you can't outsource the risk...

Introduction

Organizations are increasingly outsourcing systems, business processes, and data processing to service providers in an effort to focus on core competencies, reduce costs, and more quickly deploy new application functionality. As a result, user organizations are updating their processes for monitoring their outsourced vendor relationships, and managing the risks associated with outsourcing.

Trusted security partner

E Com Security Solutions and its member firms are trusted by clients in more than 70 countries to manage their information security infrastructure. We have unmatched visibility into the global threat landscape, and the experience of global certified security experts. Our clients include some of the world's largest and most influential organizations.

Be compliant

We give you the ability to build a strong governance structure and manage compliance. You get our experience, systems, and tools to make compliance simple, no matter what industry you are in. And you keep full control of audits and can feel assured that you are ahead of any changes in regulations—before they occur.

Tested methodology

Our methodology is a functional, effective and practically proven concept, built up on a clear specification of our requirements, continual client communication and validation throughout the engagement. A flexible approach together with structured procedures will ensure a seamless course of an audit tailored to your organization's internal processes.

Clearly structured report

Our output is an easy-to-navigate report adjusted to your organization's specifics. We provide a management summary of the key issues in which your client will be interested the most. Naturally, the report is structured by topics so that anything may be searched for and found very fast. All this is provided with respect to the rules and instructions the report has to meet to be generally acknowledged.

Cost savings

Our SOC reports will avoid additional costs in sending the auditors of the user entity to the service organization to perform their procedures and answering customer questionnaires. Our SOC reports ensure that the expectations of third-party vendor relationships are met and maintaining compliance with industry, governmental, & other relevant regulatory requirements.

SOC 1, SOC 2, & SOC 3
A PRIMER

There are three SOC reporting options currently available in the marketplace – SOC 1, 2 and 3. The SOC reporting options each allow management of a service organisation to provide a level of transparency around their internal controls to their customers and/or perspective customers. To best understand the reporting options it's important to consider the intended use and audience in each case.

The table below provides a side-by-side comparison of the SOC reporting options related to several reporting considerations.

Service Organisation Control (SOC) reports most commonly cover the design and effectiveness of controls for a 12-month period of activity with continuous coverage from year to year to meet user requirements from a financial reporting or governance perspective.

Period of time reports covering design and operating effectiveness are generally referred to as "Type 2" reports whereas point in time reports covering design are generally referred to as "Type 1" reports.

	SOC 1	SOC2	SOC 3
Purpose	Report on controls over at service organisation that may be relevant for to user entities' internal controls over financial reporting.	Report on non-financial processing based on one or more of the Trust Service criteria on security, availability, privacy, confidentiality and processing integrity	Report on non-financial processing based on one or more of the Trust Service criteria on security, availability, privacy, confidentiality and processing integrity.
Scope	Services and processes covered in the report are defined by the management of the service organisation.	Consists of 1 or more of Trust Service criteria on security, availability, confidentiality, processing integrity and privacy. For each domain principles and controls are predefined.	Services and processes covered in the report are defined by the management of the service organisation
Content	Auditor's Opinion Management Assertion System Description Examination Results Additional Information	Auditor's Opinion Management Assertion System Description Examination Results Additional Information	Auditor's Opinion Management Assertion
Standards	ISAE3402	ISAE 3000	ISAE 3000
	SSAE16	AT 101	AT 101
Types	Type I & Type II	Type I & Type II	Type I & Type II
Audience	Distribution restricted to the users of the services and their auditors.	Distribution restricted to the users of the services, their auditors and specified parties (e.g. prospects).	Distribution to anyone.

REPORT STRUCTURE

The following table compares the report components of each SOC option. Generally, a SOC 2 report has a similar 'look and feel' of a traditional SOC 1 report. A SOC 3 report provides a high level summary of information due to its unlimited distribution. Each SOC option can be prepared as a point in time assessment of control design (Type I) or assessment of design and operating effectiveness over a period of time (Type II).

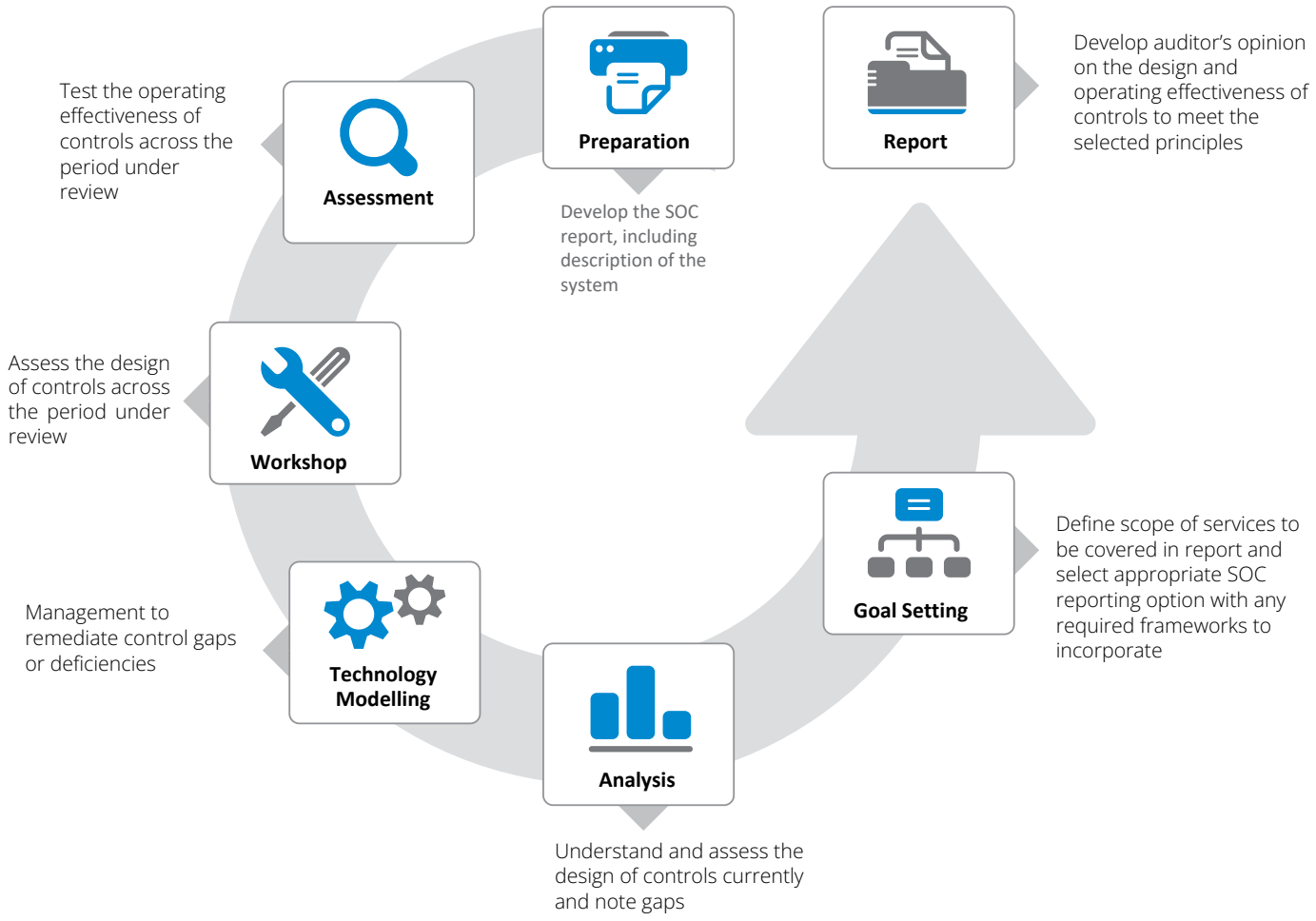
Report components	SOC 1	SOC 2	SOC 3
Auditor's opinion	✓	✓	✓
Management's assertion	✓	✓	✓
Description of the system (including controls)	✓	✓	✓
Control objectives	✓		
Principles and criteria		✓	✓
Auditor's tests of controls	✓	✓	
Auditor's results of testing	✓	✓	
Other information provided by service provider	✓	✓	
Period of coverage	-------- **Type I:** Point in time -------- ----- **Type II:** Minimum of six months -----		

TSC PRINCIPLES & CRITERIA

Today, companies of all sizes routinely rely upon an ecosystem of outsource service providers (OSPs) to carry out a wide array of functions, many of them mission-critical. Our SOC 2 reports focus on the controls that are relevant to the following Trust Services Criteria (TSC) as established by the American Institute of Certified Public Accountants (AICPA) and build confidence in service delivery processes and controls through the attestation of an independent certified public accountant.

Principles	
Security	The system is protected against unauthorised access (both logical and physical access), use or modification.
Availability	The system is available for operation and use as committed or agreed. The availability principle refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements.
Processing integrity	System processing is complete, valid, accurate, timely, and authorised.
Confidentiality	Information designated as confidential is protected as committed or agreed.
Privacy	Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice and with criteria set forth in the GAPP issued by AICA and CICA (this are expected to be modified in summer 2016).

Pragmatic Framework for SOC Compliance Management and Certification

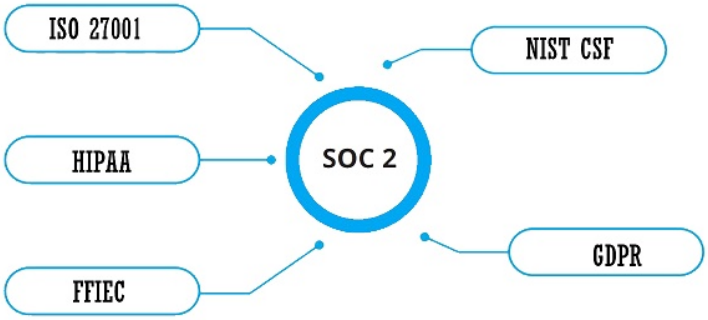


EXTEND SOC 2 REPORTING

Providing assurance with regard to the TSC may be sufficient for some service organization customers, but others may require greater coverage. In particular, those within industries such as health care and financial services have additional industry-specific regulations and requirements. This is why the SOC 2 concept was created. It is an extensible framework that allows service auditors to incorporate various industry standards into an SOC 2 report. Our SOC 2 reports are highly flexible tools that can incorporate multiple frameworks and industry standards into third-party assurance reporting. This flexibility can create substantial efficiencies for service organization customers, including reducing the amount of resources required for third-party oversight.

Because SOC 2 reports are based on a common control framework and address various industry standards, organizations generally do not have to spend as much time and effort conducting performance reviews at their service organizations. Organizations, as well as their service organizations, are also less likely to be exposed to compliance violations that can result in various forms of liability, including fines. For these reasons, some organizations have begun to stipulate their preference for using integrated frameworks as a means of obtaining third-party assurance by writing it into their service organization contracts. Through customers can benefit greatly from SOC 2 reports, the advantages for service organizations are even more significant. Consider that these businesses often must respond annually to hundreds of individual audit requests, customer questionnaires, and requests for proposals. Many of these inquiries ask the same questions and demand assurance on overlapping controls.

Throw regulatory and industry-specific requirements into the mix, and things get even more complicated and onerous. Our SOC 2 examinations can dramatically reduce this burden. By providing a standardized format for meeting a broad range of regulatory and industry control requirements, SOC 2 reports help to eliminate the need for redundant activities and one-off responses. Through a single examination based on the AICPA TSC and one or more integrated frameworks, they allow service organizations to demonstrate to their customers and other stakeholders that effective internal controls are in place. Our SOC 2 reports can also be tailored to meet the ever-growing list of security questionnaires by mapping to suitable and available criteria that can help provide customers with trust and confidence that they are achieving the concepts in the questionnaire.



Incorporate multiple frameworks into SOC 2 Audit and Reporting

Framework	
International Organization for Standardization (ISO) 27001	ISO 27001 is the international standard for securing information assets from threats and provides requirements for broader information security management. A Managed service provider has data centers and clients around the world. It continues to get security questionnaires and requests for understanding how it manages security. Rather than addressing each questionnaire individually, the service provider chooses to compile a SOC 2 mapped with ISO 27001 to demonstrate its information security controls.
National Institute of Standards and Technology (NIST)	The NIST framework focuses on improving cybersecurity for critical infrastructure. A company that maintains governmental contracts for its service offerings has contractual obligations to demonstrate how it meets the latest revision of NIST.
General Data Protection Regulation (GDPR)	GDPR represents a watershed moment in the recognition of personal rights to privacy and identity. Regardless of whether GDPR applies to an organization, it provides an opportunity for all organizations to engage in introspection of their current data collection, processing and storage practices.
The Health Insurance Portability and Accountability Act (HIPAA)	(HIPAA) established standards for the privacy and protection of individually identifiable electronic health information as well as administrative simplification standards. The rules are applicable to health plans, health care clearinghouses, and certain health care providers to safegaurd and demonstrate compliance.

SUCCESS STORIES

E Com Security Solutions provide trust and confidence that information and technology enabled business assets are safeguarded by appropriate controls and in compliance with regulations.

Financial institutions

We assisted some of the leading financial institutions based in U.S, Europe and Asia with the development of their GRC framework and assisted the organizations to comply with regulations including PCI DSS, GDPR, FFIEC and SOC 1 and SOC 2.

European Financial institutions

We executed a large Security Assessments for a leading bank in Europe, for a project comprising of the following components: Vulnerability Assessment, Penetration Testing, Security Infrastructure Study and helped them to comply and certify with industry standards including GDPR, SOC 1, SOC 2 and ISO 27001.

International temporary and contract staffing organisation

For the world leader in human resource solutions, we had helped them to comply and certify with industry standards of SOC 1, SOC 2, and FedRAMP.

e-Commerce companies

We had assessed the company's network infrastructure and their websites that provide services to their customers globally and provided assurance on their security controls and measures in compliance with regulations of PCI DSS, HIPAA, GDPR and SOC 2.

Financial technology solutions

We had assisted the US Government approved Payment Applications, and integration providers throughout its Payment Card Industry Standard, SOC 1, SOC 2 and ISO 27001 compliance programme. The project comprised of a quarterly Vulnerability Assessment of the entire external infrastructure and a thorough yearly assessment targeting both technical, managerial and security management aspects.

Global HRMS firms

For the Human Resource Management companies like, we deployed an internal Vulnerability Management service and annual compliance management exercises and to comply and certify with industry standards including GDPR, SOC 1, SOC 2 and ISO 27001..

Multinational cloud provider

For world leader in cloud analytics organization, we had deployed a Vulnerability Management service across multiple sites in several countries and helped them to comply and certify with industry standards including GDPR, SOC 2 and ISO 27001.

UK Based Telecom operator

We undertook a compliance assessment that encompassed the core infrastructure including servers and network equipment. The findings were analysed and consolidated into an action plan with clear and prioritised steps to remediation. It was further integrated with security event monitoring software and devices.

Contact us

Read more on our website: www.ecomsecurity.org

DavidKeller
Service Excellence
United States
Tel: +1 480 530 6007
david.k@ecomsecurity.org

DarioDrago
Account Director
Basel, Europe
Tel: +44 20 3807 4445
dario.d@ecomsecurity.org

Shane Tonkin
Account Director
Melobourne, Australia

shane.t@ecomsecurity.org

LucaLiGreci
Partner
London, United Kingdom
Tel: +44 20 3807 4445
luca.g@ecomsecurity.org

Ernest Teo
Principal
Singapore

ernest.t@ecomsecurity.org

NadetBudnik
Senior Manager
Johannesburg, South Africa

nadet.b@ecomsecurity.org

YuvrajSingh
Senior Consultant
Hyderabad, India
Tel: +91 040 4854 6642
yuvraj.singh@ecomsecurity.org

E COM SECURITY® SOLUTIONS

About E Com Security Solutions
E Com Security Solutions provide Compliance advisory, consulting, Audit & Assurance, Application Security, Infrastructure security and advisory services through the cloud, managed security services and software that help clients protect their most important assets from evolving cyber threats. As the global professional services and consulting network, E Com Security Solutions, brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges.

E Com Security Solutions serves through a globally connected network of member firms bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges.