KPMG

ISACA
Netherlands Chapter

Why IT Service Providers of the future adopt SOC2

ISACA NL Square Table

14 October 2020

Ronald Koorn & Stefan Zwinkels

Introduction

Ronald Koorn

Partner
KPMG IT Assurance & Advisory

Stefan Zwinkels

Manager
KPMG IT Assurance & Advisory

Agenda

- **Why SOC2 ?**
- **SOC1 vs. SOC2/3**
- **Trust Services Criteria**
- **Benefits for Service Providers and their clients**
- **SOC2 vs. ISO 27001**
- **Migrating to SOC2**
- **How to review SOC2 reports**
- **Lessons Learned**

Why SOC2?

A SOC 2 report can provide organizations the benefits of detailed examination of operational controls based on defined criteria for Security, Availability, Confidentiality, Processing Integrity and/or Privacy.

Why SOC2

- Robust Framework for Security, Availability, Confidentiality, etc.
- Focus on service commitments to clients
- Ability to attest to Trust Services Categories
- Integration of IT controls with Internal Controls
- Opportunity for strengthening & professionalizing provider-client relations

SOC1 vs. SOC2/3

SOC1

- Classes of Transactions
- Procedures for processing and reporting transactions
- Accounting records of the system
- Handling of significant events and conditions other than transactions
- Report preparation for user
- Other aspects relevant to processing and reporting user transactions

SOC2 / SOC3

Infrastructure

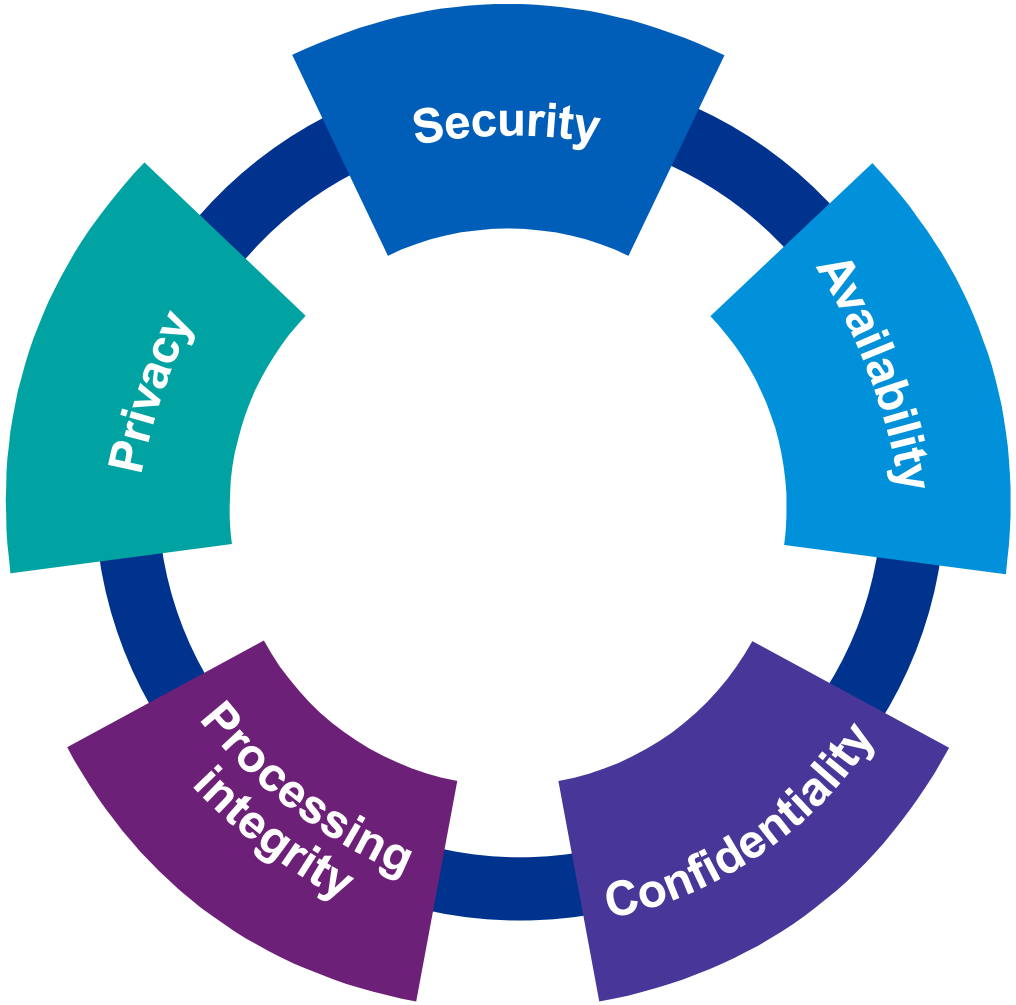
Software

Data

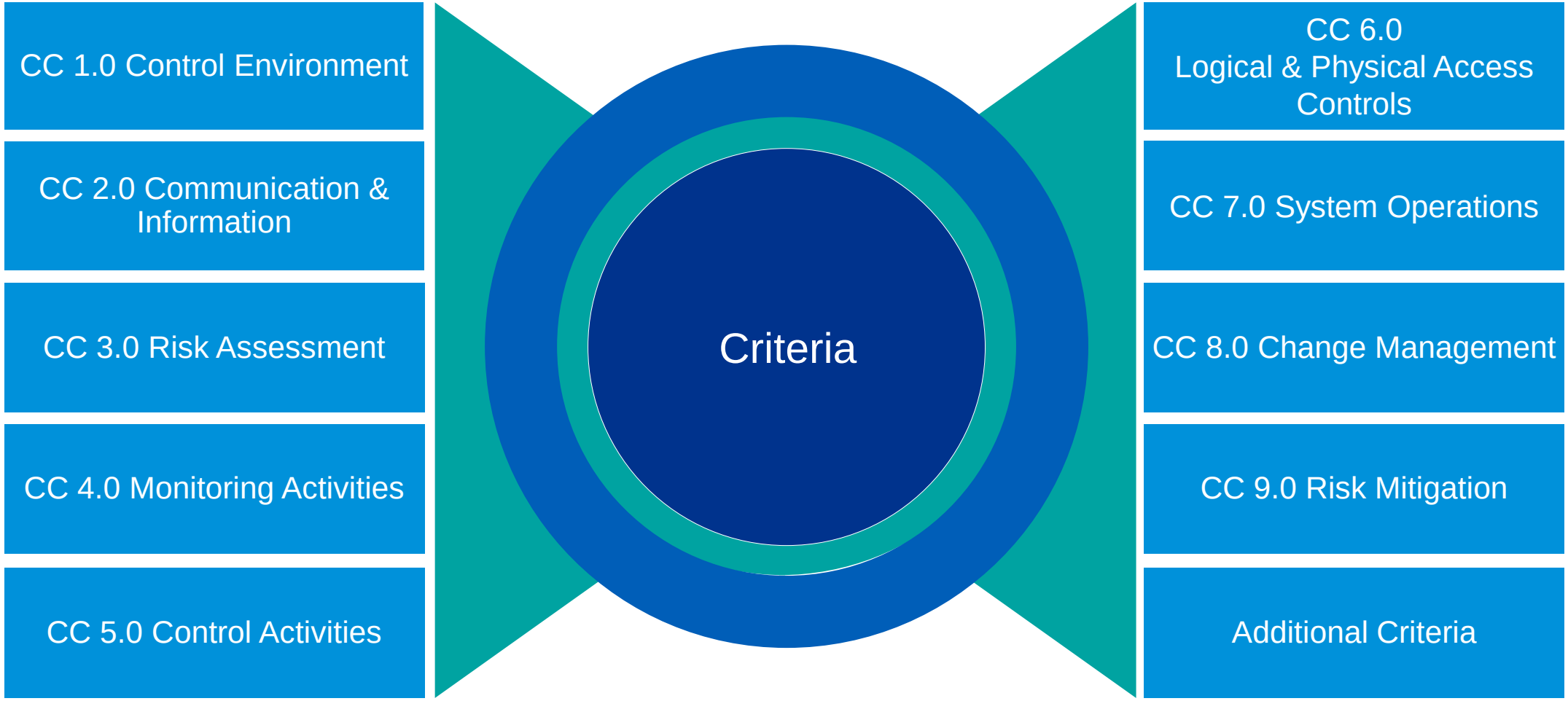
Procedures

People

SOC2 & SOC3 Trust Services Categories



Organization of Trust Services Criteria (TSC)



Benefits for IT Service Providers and their clients

Service Providers

- Building trust
- Integration of control over technology and enterprise risk management
- Bolstering its service portfolio
- Growth in Internal Control maturity
- Harmonization of processes and quality management
- Transparency in provided services

Clients

- Assurance over important criteria, like security and availability
- Vendor risk management
- Insights of control at subservice organizations
- Mandatory baseline

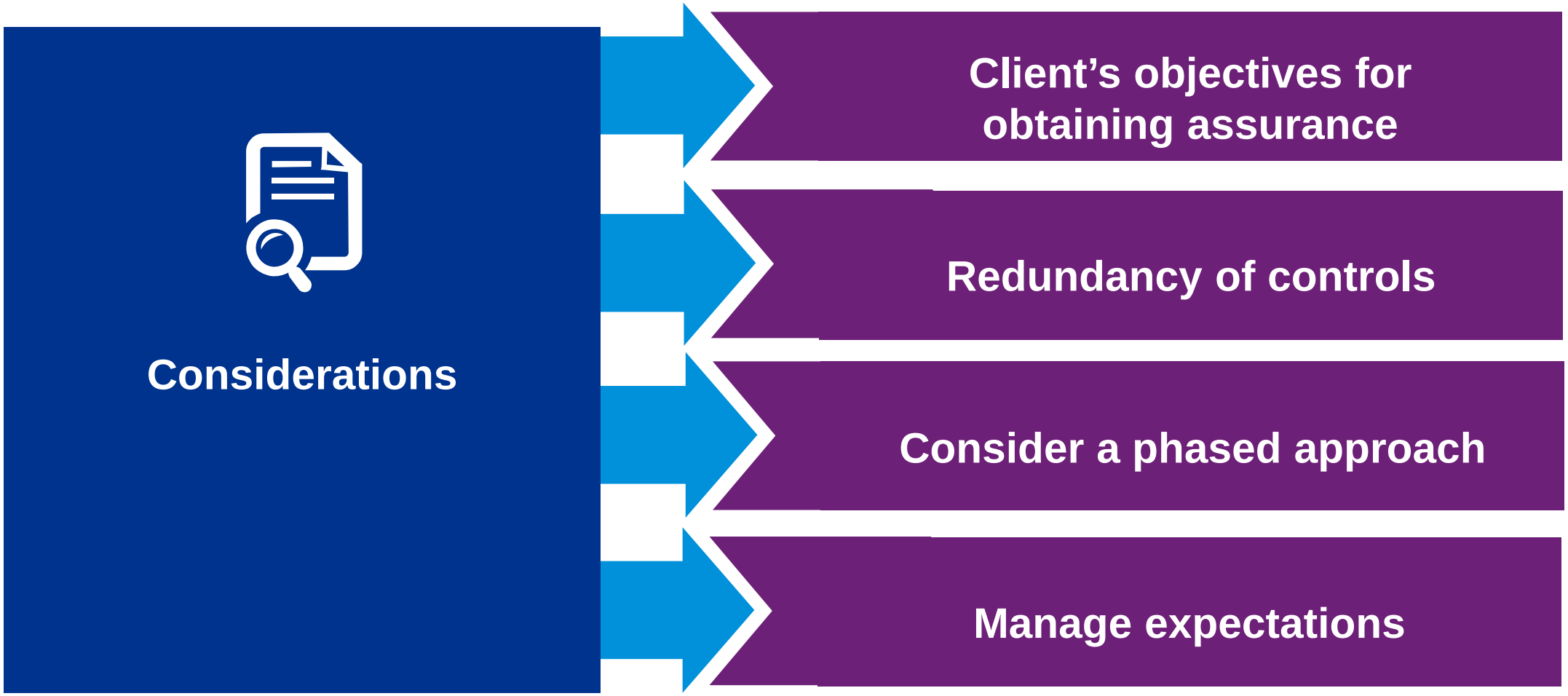
SOC2 assurance vs. ISO 27001 certification

Aspects	SOC2 assurance (based on 3000A)	ISO 27001 certificate
Specific target audience (closed user group)	☑	☒
Standard set of criteria	☑	☑
Client- / sector- / IT-specific criteria	☑	☒
Test of (Security) Management System (PDCA cycle)	☒	☑
Test of Design ('Documentation audit')	☑	☑
Test of Operational Effectiveness ('Implementation audit')	☑	☒
Standard reporting (certificate)	☑	☑
Reporting of exceptions	☑	☒

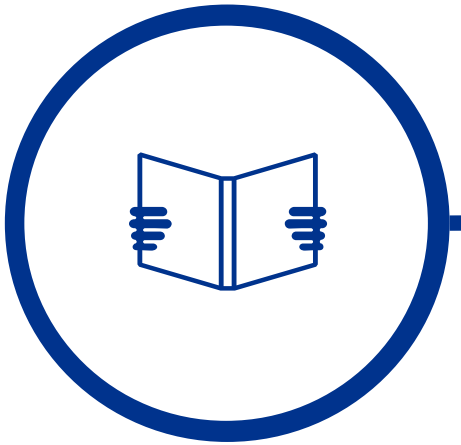
Decision making SOC1 and SOC2/3

How do you identify the SOC report that is right for you?		
1 Will the report be used by your customers and their auditors to plan and perform an audit or integrated audit of your customer's financial statements?	Yes	SOC 1 Report
2 Will the report be used by your customers as part of their compliance with the Sarbanes-Oxley Act or similar law or regulation?	Yes	SOC 1 Report
3 Will the report be used by your customers or stakeholders to gain confidence and place trust in a service organization's systems?	Yes	SOC 2 or 3 Report
4 Do you need to make the report generally available or seal?	Yes	SOC 3 Report
5 Do your customers have the need for and ability to understand the details of the processing and controls at a service organization, the tests performed by the service auditor and results of those tests?	Yes	SOC 2 Report
	No	SOC 3 Report

Migrating to SOC2



How to review SOC2 reports



- Audit period
- Scope (incl. subservice orgs)
- Qualifications
- Relevance of noted exceptions
- System description
- Complementary User Entity Controls
- Substantial changes during the audit period
- Management response

Lessons learned

- Consider needs of the client / audience – now and in the future
- Extent of maturity of internal control of service organization
- First perform readiness assessment
- Scoping is key (service commitments & third parties)
- Scaling & phasing
- Consider extent of client experience with assurance
- Consider lead time
- Definition of control activity
- Strong 2nd line very beneficial
- (GRC) tooling is helpful
- SOC2 is more than a report

What questions do you have?

Contact us:

Ronald Koorn
Partner
T: 06 – 2292 8127
E: koorn.ronald@kpmg.nl

Stefan Zwinkels
Manager
T: 06 – 2139 3070
E: wwinkels.stefan@kpmg.nl

Visit KPMG IT Assurance & Advisory

useful links:

SOC1/2/3 introduction:
https://www.compact.nl/articles/nieuwe-ontwikkelingen-it-gerelateerde-service-organisation-control-rapportages/

SOC suite:
https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html

Assurance vs. certification:
https://www.compact.nl/articles/it-assurance-versus-it-certificering/