

Mattig-Suter und Partner Schwyz Treuhand- und Revisionsgesellschaft



GGI World Conference, Practice Group
Auditing, Reporting and Compliance

**Claudia Mattig: Risk-based Audit
Planning for SME's based on IT
Process Maturity**

Vienna, October 20, 2017



Mitglied von EXPERTsuisse



SWISS
EXCELLENCE
FORUM

GGI
INDEPENDENT MEMBER

Outline

1. Introduction – Audit Planning in General
2. Our Audit Approach
3. The Process in Detail
4. The Next Steps

Introduction - Audit Planning in General

Auditors are required to perform a systematic risk assessment as part of their strategic planning of individual audits.

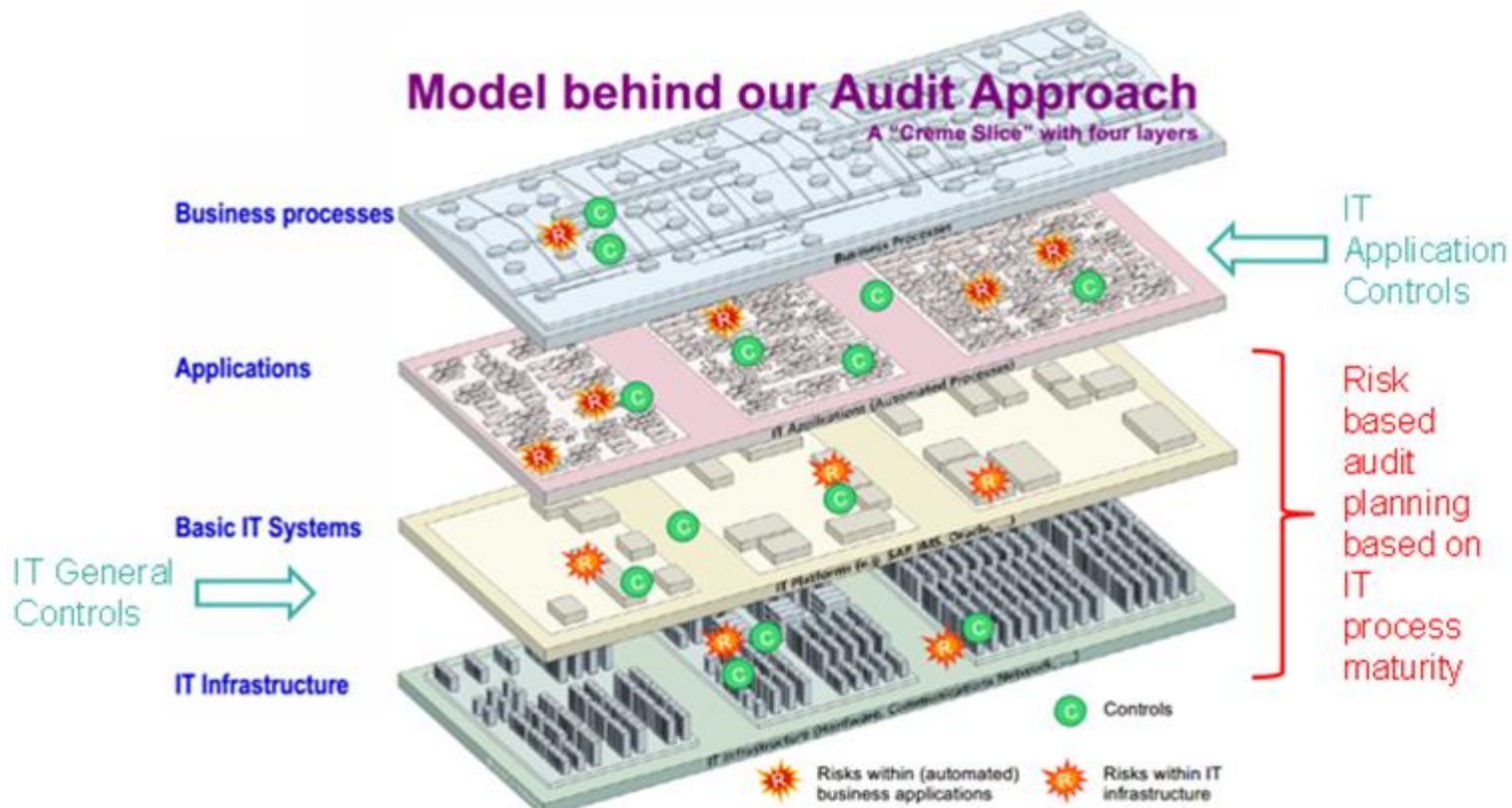
In addition to issues such as business environment, legal requirements, materiality of financial accounts or accounting standards **the maturity of the information processing (IT) environment** also has a direct influence on the reliability of the internal control system.

→ Efficient approach to identify IT risks by means of an assessment of the maturity of relevant IT-processes

Outline

1. Introduction – Audit Planning in General
2. Our Audit Approach
3. The Process in Detail
4. The Next Steps

Our Audit Approach – The Model



Our Audit Approach – The Process

Approach using three phases

- Phase 1:
IT dependency assessment
- Phase 2:
IT Maturity assessment
- Phase 3:
Performing specific IT audits



Part of
Approach



Not part of
our approach

Outline

1. Introduction – Audit Planning in General
2. Our Audit Approach
3. The Process in Detail
4. The Next Steps

The Process in Detail – Phase 1

IT dependency assessment

- When should we plan with the assessment?
 - During the strategic audit planning.
- What is the goal of the assessment?
 - Identifying the significance of IT within the company.

The Process in Detail – Phase 1

IT dependency assessment

Business Strategy and IT

- Degree of innovation while using IT.
- Dependence on the availability of IT.

Internal Organization and Control

- Internal control system / risk management.
- Segregation of duties.
- Delegation of duties and know-how in financial accounting.
- Awareness regarding information security.

IT Applications

- Software for financial accounting.
- Degree of innovation of value flows in financial accounting.
- Program errors in core application.

IT Operations

- Operational security of IT resources.
- Delegation of duties within the IT department.
- Dependency on external staff.

Time factor / Date of last audit

- Timeframe since last independent assessment of IT.

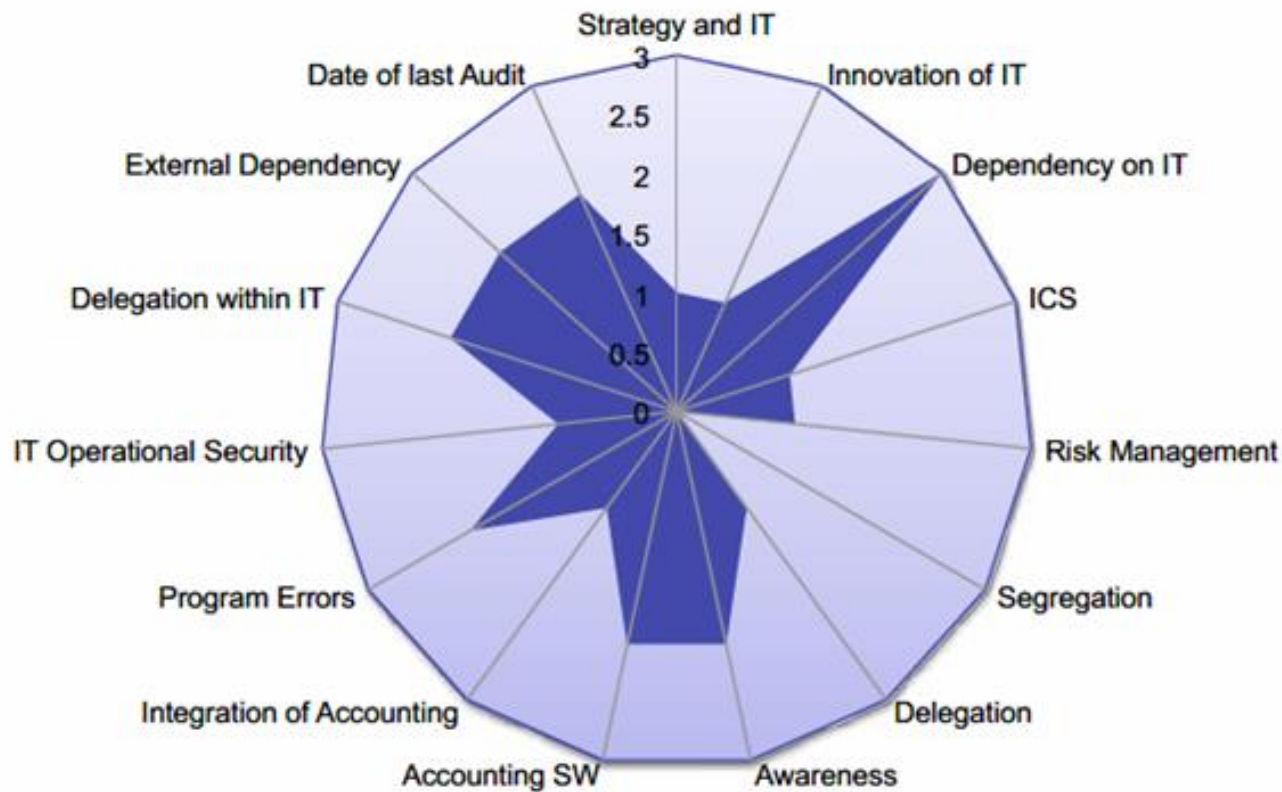
The Process in Detail – Phase 1

General risk assessment questionnaire

Criteria	Step 1	Step 2	Step 3	Step 4
Business strategy and the use of IT		Yellow		
Innovation using IT	Red			
Dependence on availability of information		Yellow		
Risk management			Green	
Internal Control System (ICS)				Green
Awareness for security of information		Yellow		
Functional separation				Green
Substitutes and applicable know-how Financial Accounting				Green
Financial Accounting software			Green	
Changes within core functions	Red			
Integration of the value flow in financial accounting	Red			
Programming errors in core functions			Green	
Operational liability IT		Yellow		
Substitutes in the IT department				Green
Dependency on third-party employees (including outsourcing partners)		Yellow		
Date of the last independent assessment of the IT	Red			

The Process in Detail – Phase 1

General risk assessment



The Process in Detail – Phase 1

Conclusion

- It permits the rapid assessment of the IT dependency of the entity audited.
- It indirectly indicates how mature the IT should be.
- It gives a clear indication whether phase 2 should be performed.

The Process in Detail - Phase 2

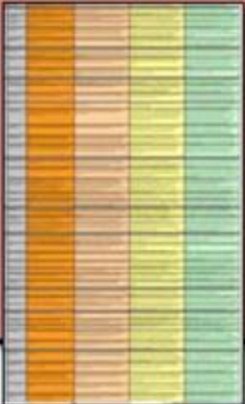
IT maturity assessment

20 Topics / 91 Controls

- IT related documentation (4)
- Organization of IT (7)
- IT governance (6)
- IT risk management (3)
- Compliance (2)
- IT project management (6)
- Software development (7)
- Application testing (5)
- Financial accounting (3)
- direct application controls (4)
- supporting application controls(5)
- End-user policies (3)
- End-user training (3)
- Access control (5)
- IT security (6)
- Physical security (3)
- IT operations (7)
- Problem management (3)
- Backup (5)
- Outsourcing (4)

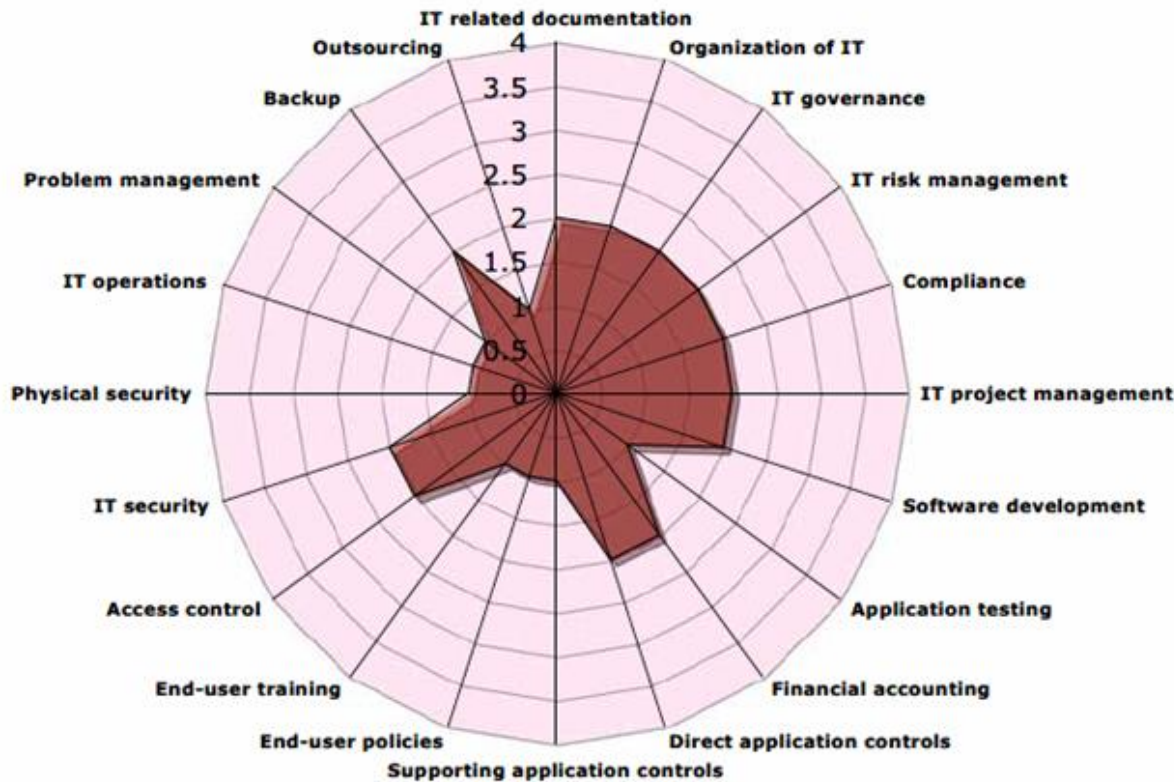
The Process in Detail - Phase 2

IT maturity assessment

inexistent control maturity	low control maturity	adequate control maturity	high control maturity
<ul style="list-style-type: none"> •(almost) nothing •no •not •none (at all) 	<ul style="list-style-type: none"> •informal •basic •sometimes •not documented •incomplete / inconsistent / partially / isolated •ad-hoc / on a case-by-case basis / on request •occasionally / rarely •known 	<ul style="list-style-type: none"> •formal •standard •defined / determined •in general / mostly •documented •fully implemented •monitored / logged (incompletely) •reviewed rarely or not at all 	<ul style="list-style-type: none"> •formal •always •formally documented •fully implemented •completely logged •reviewed regularly / periodically •compliance formally verified

The Process in Detail - Phase 2

IT maturity assessment



The Process in Detail - Phase 2

Conclusion

- It enables reliable estimation of risks through the assessment of the maturity of controls.
- It tells the financial auditor which controls are reliable.
- It provides information useful for the annual IT audit planning.

Outline

1. Introduction – Audit Planning in General
2. Our Audit Approach
3. The Process in Detail
4. The Next Steps

Next steps

- Report to the client regarding the identified weaknesses including a recommendation to improve these.
- If a lot of criteria are assessed with maturity level 2 and 1 a full scale IT audit should be considered.

Mattig-Suter und Partner Schwyz

Treuhand- und Revisionsgesellschaft



Thank you for your attention.



Mitglied von EXPERTsuisse



SWISS
EXCELLENCE
FORUM

GGI
INDEPENDENT MEMBER

Disclaimer

Diese Präsentation wurde zur allgemeinen Orientierung erarbeitet und stellt keine rechtliche Beratung dar. Sie sollten nicht aufgrund der Informationen in dieser Präsentation und ohne Einholung spezifischer rechtlicher Beratung handeln. Es wird keine Zusicherung oder Gewährleistung (weder ausdrücklich noch stillschweigend) für die Richtigkeit oder Vollständigkeit der in dieser Präsentation enthaltenen Informationen gegeben, und, soweit gesetzlich zulässig, übernimmt MSuP, ihre Mitarbeiter und Vertreter keine Haftung oder Verantwortung für Handlungen oder Unterlassungen, die Sie oder jemand anders im Vertrauen auf die in dieser Präsentation enthaltenen Informationen vornehmen oder Entscheidungen, die auf dieser Präsentation basieren.

Disclaimer

This presentation has been prepared for general guidance on matters of interest only, and does not constitute legal advice. You should not act upon the information contained in this presentation without obtaining specific legal advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this presentation, and, to the extent permitted by law, MSuP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this presentation or for any decision based on it.

Wichtiger Haftungsausschluss

Keine Person, Organisation oder Unternehmen sollte gestützt auf Informationen, die in dieser Präsentation enthalten sind, handeln ohne vorher eine Beratung von einer entsprechend qualifizierten Person oder Firma im Zusammenhang mit den jeweiligen Umständen der involvierten Parteien eingeholt zu haben. Diese Präsentation sollte nicht als Angebot verstanden werden und enthält keine vollständige Abhandlung in Bezug auf die steuerlichen Aspekte. Der Autor lehnt ausdrücklich jegliche Haftung und Verantwortung für Personen, Organisationen oder juristische Personen ab, die ohne Einholung einer Beratung für den konkreten Fall gestützt auf diese Präsentation handeln.

Important Disclaimer

No person, entity or corporation should act or rely upon any matter or information contained or implied within this presentation without first obtaining advice from an appropriately qualified professional person or firm of advisors related to the particular circumstances of the parties involved. This presentation should not be regarded as offering a complete explanation of the taxation matters that are contained within this presentation. The author expressly disclaims all and any liability and responsibility to any person, entity or corporation who acts or fails to act as a consequence of any reliance upon the whole or any part of the contents of this presentation without having obtained advice with regard to the specific case.