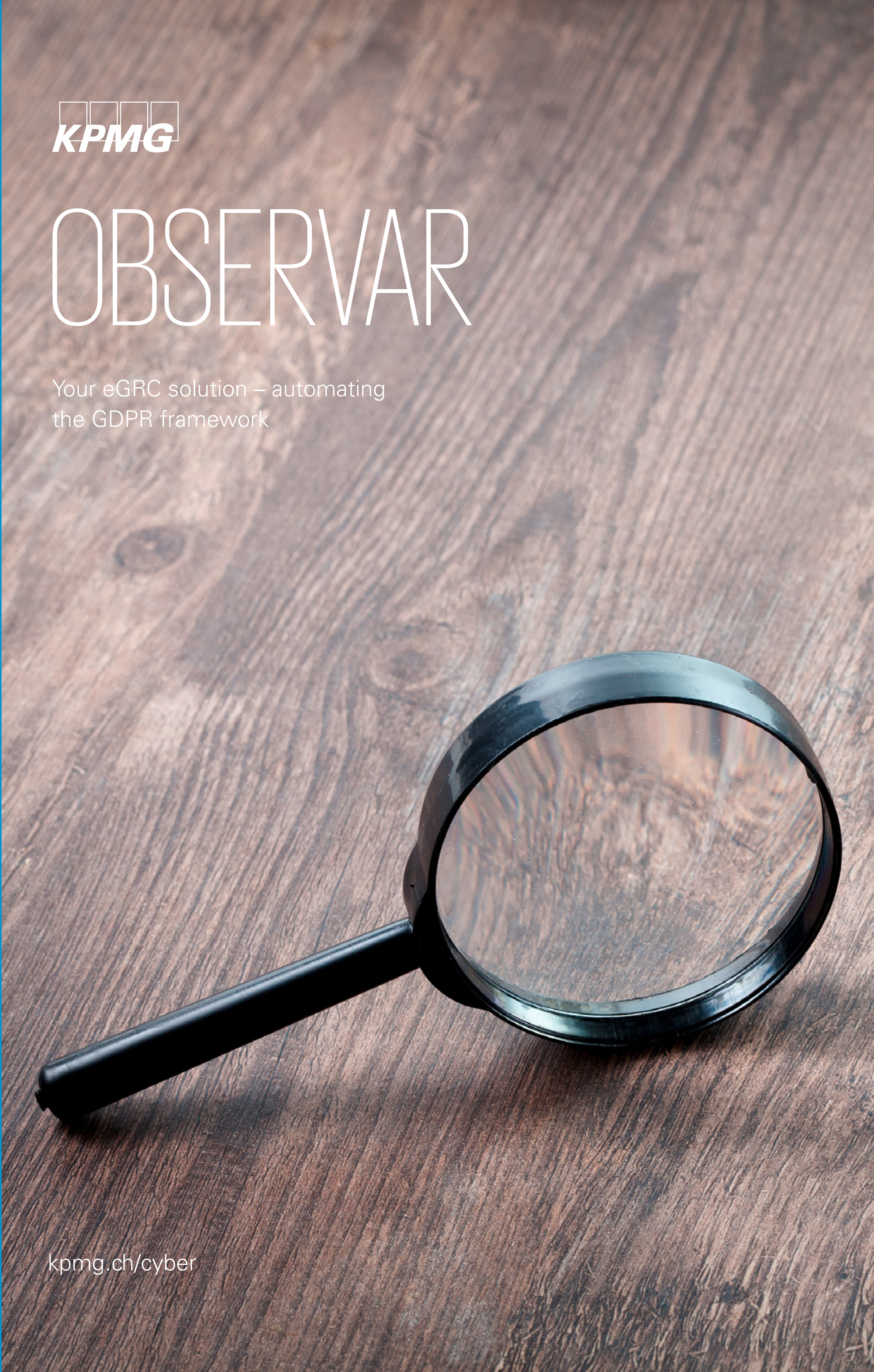
KPMG

OBSERVAR

Your eGRC solution – automating the GDPR framework

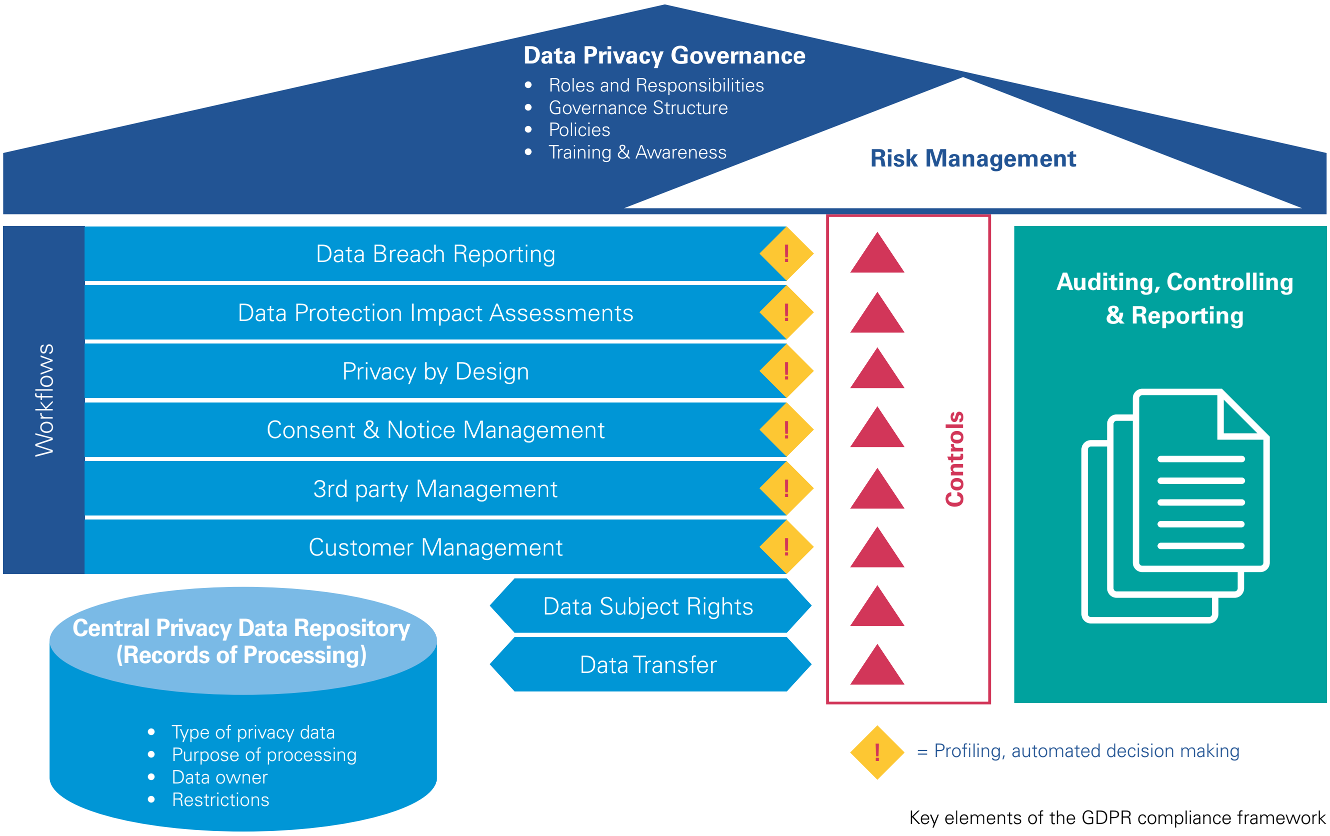


kpmg.ch/cyber

The finalization of the European General Data Protection Regulation (GDPR) and the recent draft of the Swiss Data Protection Act (DPA) have brought data protection compliance to the top of the priority list. Proper implementation and management of data privacy is crucial in order to manage future operational and reputational risks and to avoid potentially large fines for non-compliance.

What are the challenges for your company?

By May 2018, companies that fall under the European General Data Protection Regulation (GDPR) will have to be compliant with the new law. To be compliant, companies need to set up an appropriate governance structure, adapt any existing risk and compliance management frameworks and implement technical and organizational measures. IT system modifications are also often necessary. Last but not least, companies must also ensure that the implemented measures are able to be appropriately controlled and audited by applying the associated controls and reports. To simplify this change, a supporting tool is basically a must.



Key elements of the GDPR compliance framework

KPMG, along with its partner OBSERVAR, has developed a technical solution that enables companies to immediately implement GDPR processes and workflows, and therefore gain control over the operational implementation and monitoring of GDPR compliance. KPMG delivers a preconfigured GDPR compliance solution with all relevant content necessary to ensure compliance with the new regulations. The tool further offers customization possibilities and ongoing support.

Within the available enterprise governance risk and compliance (eGRC) functionality, four modules cover the following GDPR items:

- GDPR governance management
- Data ownership management
- GDPR staff training and assessment
- Data protection impact assessment
- Data breach notification
- Privacy by design
- Profiling compliance
- Data minimization management
- Consent management
- Processor and 3rd party management
- Controller management
- Notice management

The key advantages of using OBSERVAR for GDPR

The current situation includes an increasing number of regulations, and companies are struggling to keep the many regulations under control. As such, many firms are seeking a fast and cost-effective solution for GDPR compliance before the regulation becomes effective in May 2018. KPMG can offer exactly this with the help of the OBSERVAR tool.

Minimal implementation effort/costs

KPMG has parameterized OBSERVAR for GDPR implementation, ensuring that the tool provides the required governance structures, templates (e.g. policies), controls and processes. This saves project and implementation costs.

Time to market

The GPDR module with its pre-defined content enables you to achieve GDPR compliance within a very short timeframe. It covers:

- Governance models
- Roles and responsibilities
- Templates for policies, guidelines, etc.
- Default processes, e.g. breach reporting
- Standard set of controls and reports

Compliance functions available from day one

All work processes and results are immediately available:

- Workflows
- Documentation
- Progress tracking
- Controls
- Reporting
- Auditability
- Customer-specific configuration and parametrization takes only a few working days
- Customers can easily learn how to parametrize the system

Quick start – Fast technical integration

- Technical provisioning from the cloud is possible within one working day. In addition, it is possible to establish an alternative operation platform (internal or outside solution) at any time
- No system integration required, since the system is a web platform
- Easy integration into Active Directory
- OBSERVAR is a web-based platform and therefore does not require any system integration work

Customized operation platforms

As desired by the client, OBSERVAR can be operated in any scenario:

- Microsoft Azure Cloud
- On-site at the client’s premises
- At any outsourcing center

GPDR content service

- Receive the latest GDPR updates
- Get your compliance framework updated by KPMG

High security

- For additional security, OBSERVAR can deploy the tool to be used only in https (using our own certificate for cloud installations or the customer's certificate when installed on-site)
- OBSERVAR can also apply an extra security layer by encrypting the texts when inserted in the database, thus preventing an intruder from seeing entered texts and comments in the event of unauthorized access of the database
- The OBSERVAR eGRC solution can be protected through Cloud Access Security Broker solutions
- The underlying database can be encrypted through different mechanisms (TDE, always-encrypted, etc.)

Personal Data Breach Notification

Adequate actions by Data Protection Officer **(72 h)** →

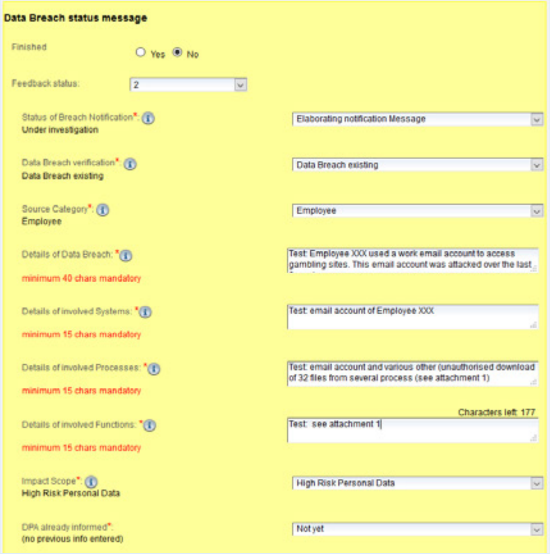
Selected Data Protection Officer has to fill in the yellow part with his findings, judgement, actions and recommendations.

In the master area the number and content of questions is scaleable and the “question types” include:

- **Text answers**
- **Select lists**
- **Icon selections**

Text answers can be set to have a minimum text e.g. 40 characters.

All the actions are saved with adate and time stamp.



Data Breach status message

Finished ○ Yes ● No

Feedback status: 2

Status of Breach Notification*: Under investigation — Elaborating notification Message

Data Breach verification*: Data Breach existing — Data Breach existing

Source Category*: Employee — Employee

Details of Data Breach: * minimum 40 chars mandatory — Test: Employee XXX used a work email account to access gambling sites. This email account was attacked over the last

Details of involved Systems: * minimum 15 chars mandatory — Test: email account of Employee XXX

Details of involved Processes: * minimum 15 chars mandatory — Test: email account and various other (unauthorised download of 32 files from several process (see attachment 1)

Characters left: 177

Details of involved Functions: * minimum 15 chars mandatory — Test: see attachment 1

Impact Scope*: High Risk Personal Data — High Risk Personal Data

DPA already informed*: (no previous info entered) — Not yet

Sample screenshot: Workflow after a breach has been reported

But OBSERVAR can offer much more

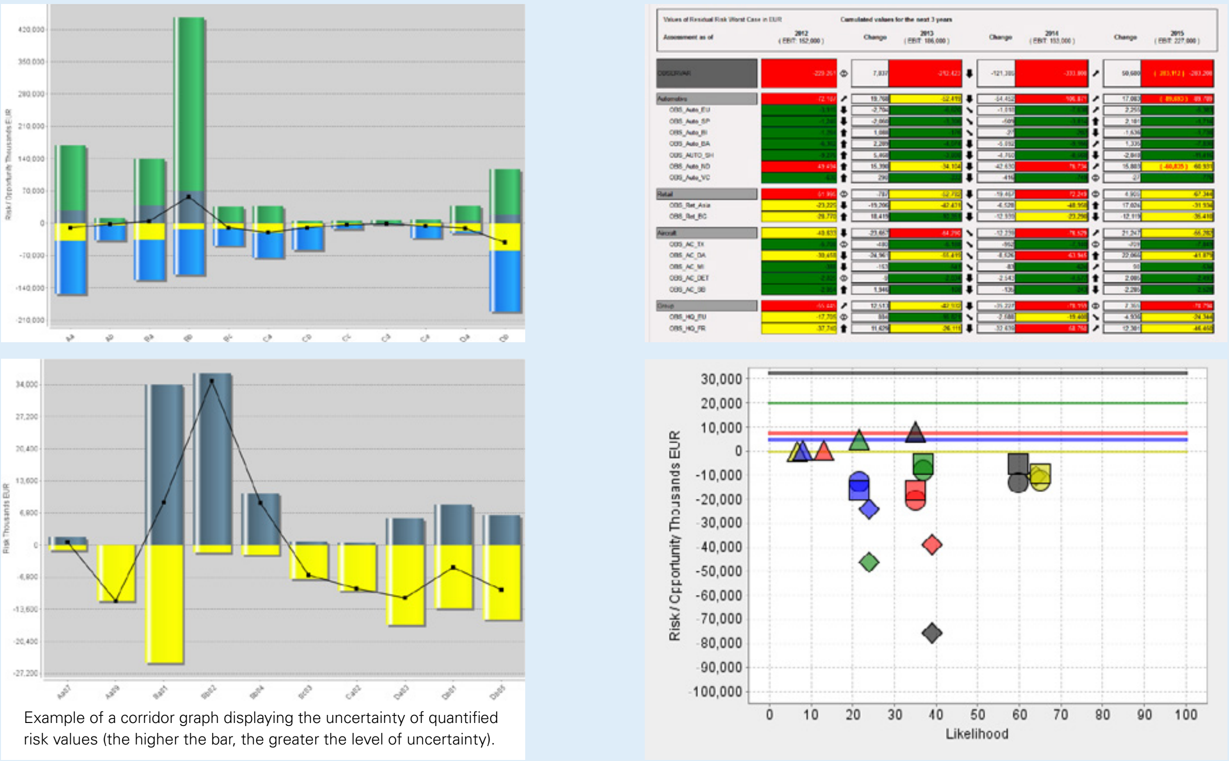
In recent years, there has been increasing demand for eGRC tools to be able to have a tool to oversee all processes relevant to risk and compliance. As a result, OBSERVAR contains a vast number of functionalities covering all requirements within compliance management.

- Internal control system management
- Corporate risk management
- ISO 27001, ISO 31000, ONR 489000, COSO ERM implementations
- Project portfolio/program management
- Management of other specific regulations

For many of these services, KPMG can provide managed content services that will assure your framework is always up to date.

Simple and easy management of the compliance framework

The OBSERVAR suite reduces the number of controlling and monitoring activities needed to be undertaken by a compliance or date protection officer. Using automated alerts and reminders means that management of this area instead becomes highly automated. Moreover, reporting is carried out easily through cockpits that can be chosen from the standard portfolio or customized by the client.



Values of Residual Risk Worst Case in EUR

Cumulated values for the next 3 years

Assessment as of	2012 (EBIT 152,000)		Change	2013 (EBIT 106,000)		Change	2014 (EBIT 153,000)		Change	2015 (EBIT 227,000)
OBSERVAR	-229.261	⇔	7,837	-292.423	⬇	-121.380	-333.800	↗	50,680	(283.112) -283.200
Automotive	-72.107	↗	19.768	-52.419	⬇	-54.452	-106.871	↗	17.083	(89.692) -89.789
OBS_Auto_EU	[illegible]	⬇	-2,704	[illegible]	↘	-1.018	[illegible]	↗	2,255	[illegible]
OBS_Auto_SP	[illegible]	⬇	-2.060	[illegible]	↘	-609	[illegible]	⬆	2,181	[illegible]
OBS_Auto_BI	[illegible]	⬆	1.088	[illegible]	↘	-27	[illegible]	⬇	-1.636	[illegible]
OBS_Auto_BA	[illegible]	⬆	2,288	[illegible]	⬇	-5.092	[illegible]	↗	1,336	[illegible]
OBS_AUTO_SH	[illegible]	⬆	5,468	[illegible]	⬇	-4.760	[illegible]	⬇	-2,840	[illegible]
OBS_Auto_ND	-49.494	⬆	15.398	-34.104	⬇	-42.630	-76.734	↗	15,883	(-60,835) -60.931
OBS_Auto_VC	[illegible]	⬆	290	[illegible]	⬇	-416	[illegible]	⇔	27	[illegible]
Retail	-51.995	⇔	-787	-52.782	⬇	-19.467	-72.249	⇔	4.903	-67.344
OBS_Ret_Asia	-23.229	⬇	-19.206	-42.431	↘	-6.528	-48.958	⬆	17.024	-31.934
OBS_Ret_BC	-28.770	⬆	18.419	[illegible]	⬇	-12.939	-23.290	⬇	-12.119	-35.410
Aircraft	-40.633	⬇	-23.657	-64.290	↘	-12.239	-76.529	↗	21.247	-55.282
OBS_AC_TX	[illegible]	⇔	-400	[illegible]	↘	-992	[illegible]	⇔	-729	[illegible]
OBS_AC_DA	-30.458	⬇	-24.961	-55.419	↘	-8.526	-63.945	⬆	22.066	-41.879
OBS_AC_MI	[illegible]	⬇	-153	[illegible]	↘	-83	[illegible]	↗	90	[illegible]
OBS_AC_DET	[illegible]	⇔	-9	[illegible]	⬇	-2.543	[illegible]	⬆	2.086	[illegible]
OBS_AC_SB	[illegible]	⬆	1.946	[illegible]	⬇	-136	[illegible]	⬇	-2.289	[illegible]
Group	-55.445	↗	12.513	-42.932	⬇	-35.227	-78.159	⇔	7.365	-70.794
OBS_HQ_EU	-17.705	⇔	884	[illegible]	↘	-2.588	-19.408	↘	-4.936	-24.344
OBS_HQ_FR	-37.740	⬆	11.629	-26.111	⬇	-32.639	-58.750	↗	12.301	-46.450

Example of a corridor graph displaying the uncertainty of quantified risk values (the higher the bar, the greater the level of uncertainty).

Sample screenshot: Various tool generated reports incl. multi-year comparison and overall group consolidation of risks and opportunities

Contact

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch/cyber

Matthias Bossardt
Partner
Consulting

+41 58 249 36 98
mbossardt@kpmg.com

Thomas Bolliger
Partner
Consulting

+41 58 249 28 13
tbolliger@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence.