



# Executive Summary

## Infrastructure & Web Service Security Statement



List of Distribution			Attribute
Realisator AG			Company
scip AG			Company
Version	Date	Author	Classification
1.0	12/18/2013	Stefan Friedli, scip AG	confidential

## Executive Summary

Realisator AG is proactively aware of the security risks and threats facing it in modern times. Best practices, together with a well-designed and maintained network infrastructure focusing on security and safety ensure that the standards required are kept. Additionally, externally handled security auditing tasks are done on a regular basis.

In a time where reports of incidents of intrusion and theft of sensitive data are frequent, it's a considerable achievement for a company to reach a level of security for an internal network that is as sophisticated as the one encountered in this test. Both on a physical as well as on a virtual level, the obstacles for an attacker are high and the implemented logging and monitoring mechanisms are likely to show an attack before it's able to get too close to any sensitive information, if at all.

Realisator personnel involved in this test were also able to confidently answer any questions regarding used technology issues and/or provide adequate documentation whenever and wherever requested.



Security auditing is a means to determine the potential and existing flaws in the current environment. Extensive testing with attack techniques were used to detect potentially existing issues. **The security environment of Realisator AG can be classified as “reaching excellent”**. The security level applied can be compared to the security level of a banking environment.



Zürich, 18.12.2013

Mr. Stefan Friedli (Lead Auditor)