



# BSI Grundschutz mit den QSEC Suiten



Mit Sicherheit erfolgreich.



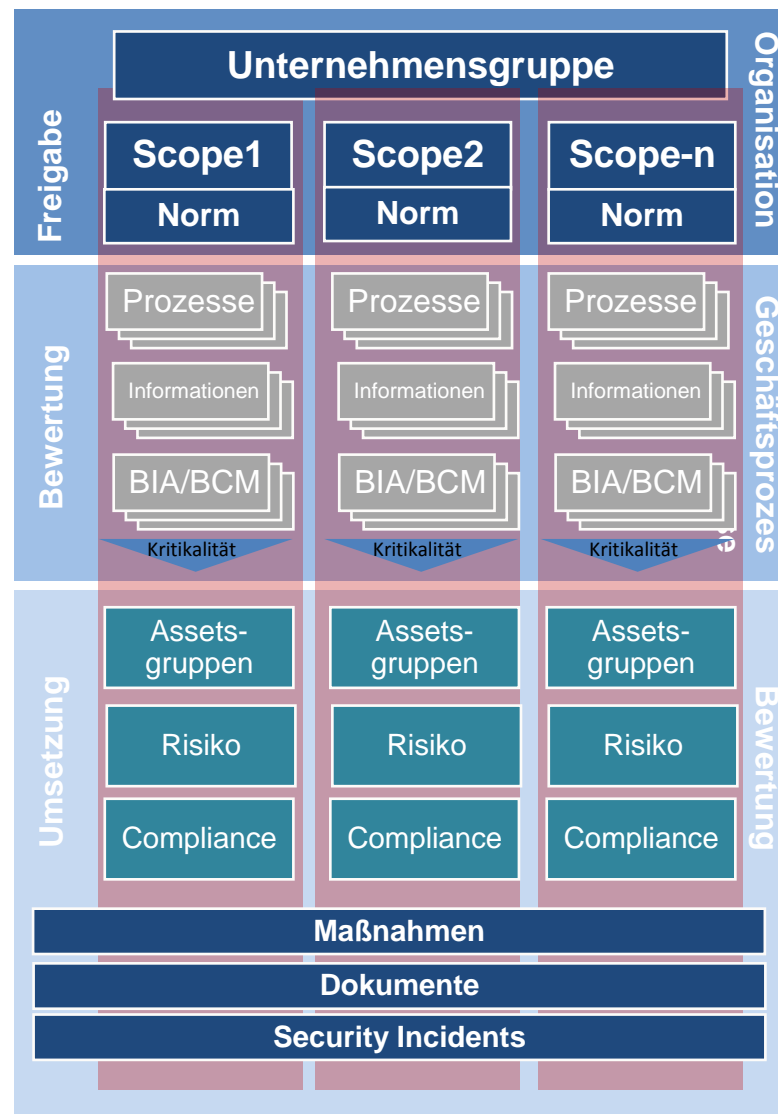
- Der Grundschutzkatalog (100-1) ist in QSEC integriert
- Verbindung/Verknüpfung der Grundschutzmaßnahmen mit der ISO/IEC 27001:2013
  - Bei Control-Bewertung der ISO/IEC 27001:2013 werden Maßnahmen des Grundschutzes als Vorschlag angeboten
- Im Risikomanagement werden die Aspekte des Gefährdungskatalogs (100-3) berücksichtigt und in Bedrohungen- und Schwachstellen aufgegliedert und bewertet
- Ableitung und Bewertung von individuelle Szenarien auf Assetgruppenebene
- Notfallvorsorge und Business Impact Analyse in Anlehnung an 100-4 und ISO 22301 integriert
- Manuelle Datenintegration aus dem GS-Tool

# QSEC versus Grundschutz-Tool (GS-Tool)

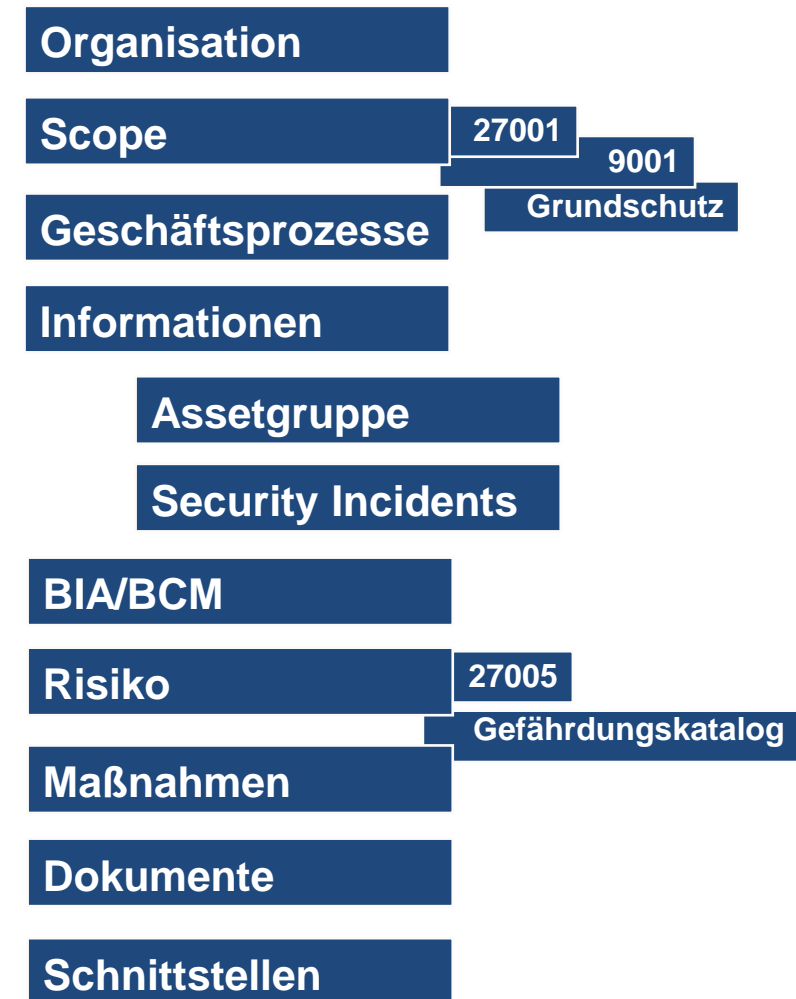
## GS-Tool - Methode



## Methode nach ISO/IEC 27001

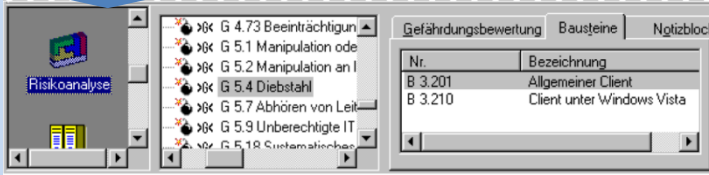
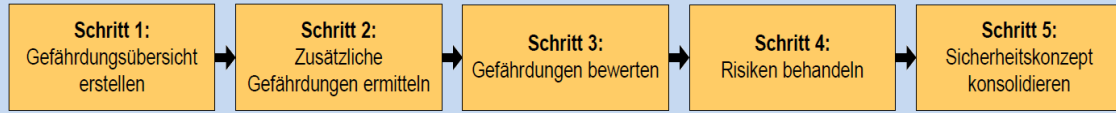


## QSEC - Methode

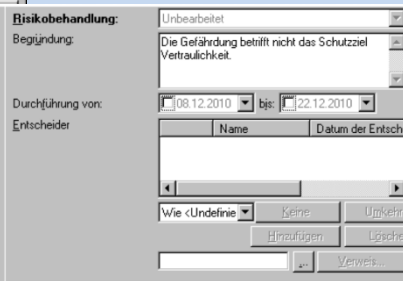
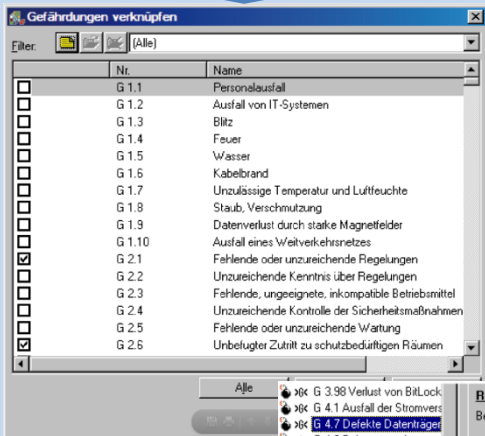


# QSEC versus BSI Grundschutz - Risikomanagement

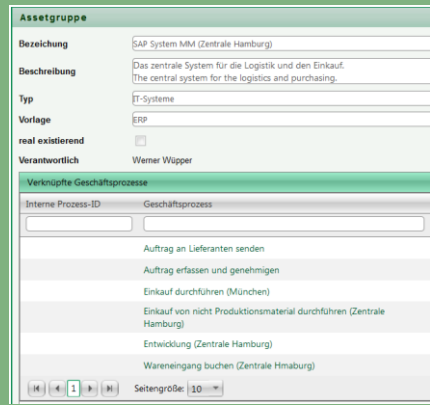
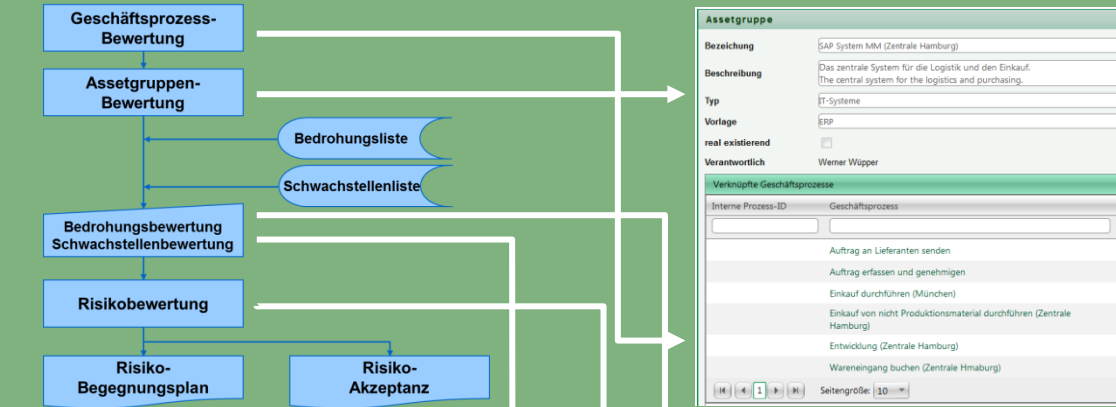
## Methode nach Grundschutz (100-3)



Einstufige Gefährdungen



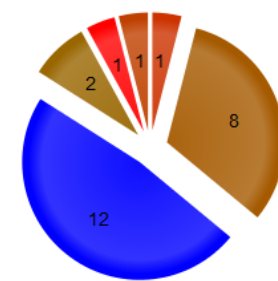
## Methode nach ISO/IEC 27005



ID	Kategorie	Bedrohung	Hinweis	Bewertung
10	Höhere Gewalt	Erdbeben	0 - tritt häufiger als 1x pro Jahr auf	5
20	Höhere Gewalt	Überflutung	0 - ist nicht vorhanden	5
30	Höhere Gewalt	Sturm	0 - tritt häufiger als 1x pro Jahr auf	5
40	Höhere Gewalt	Blitz	0 - tritt häufiger als 1x pro Jahr auf	5
70	Höhere Gewalt	Feuer	0 - tritt seltener als 1x pro Jahr auf	5
75	Höhere Gewalt	Technische Katastroph		5
77	Höhere Gewalt	Beeinträchtigungen d.		5
140	Höhere Gewalt	Hohe Luftfeuchtigkeit		5
150	Höhere Gewalt	Staub, Verschmutzung		5
160	Höhere Gewalt	EM-Einstrahlung		5
170	Höhere Gewalt	Elektrostatische Entlad		5
50	Vorsätzliche Handlungen	Bombe		5
60	Vorsätzliche Handlungen	Waffengebrauch		5
65	Vorsätzliche Handlungen	Vandalismus		5
80	Vorsätzliche Handlungen	Sabotage		5
180	Vorsätzliche Handlungen	Diebstahl (Hard- Softw		5
250	Vorsätzliche Handlungen	Entscheidung einer Be		5
260	Vorsätzliche Handlungen	Schadhafte (Viren) Soft		5
340	Vorsätzliche Handlungen	Abhören von Netzwerk		5

ID	Kategorie	Schwachstellen	Hinweis	Bewertung
5	Umgebung und Infrastruktur	Unterbringung in Einsturz gefährdetem Gebäude	0 - ist leicht erkennbar und leicht auszubau	5
10	Umgebung und Infrastruktur	Fehlender physischer Schutz von Gebäuden, Türen und Fenstern	0 - ist nur schwierig oder mit hohem Aufwand auszub	5
20	Umgebung und Infrastruktur	Unangemessene oder nachlässige Verwendung von Zutrittskontrollmechanismen	0 - ist mit mittlerem Aufwand auszubau	5
30	Umgebung und Infrastruktur	Unstabile Stromversorgung	0 - ist nicht vorhanden oder nicht auszubau	5

Risikostatus kritische Assetgruppen



- Risikowert 16
- Risikowert 13
- noch nicht bewertet
- Risikowert 12
- Risikowert 20
- Risikowert 15

Anzeige der Assetgruppen, sortiert nach dem jeweiligen Risikowerte

Einzelrisiken	Status	Bedrohungen	schad	3	Fehlendes Vulnerability Management	3	12	Vertraulichkeitsverlust
Schadhafte (Viren) Software (Malware)				3	Fehlendes oder unzureichendes Patch Management	3	12	Vertraulichkeitsverlust

# Migration der GS-Tool-Daten in die QSEC Suite

