Kennen. Können. Tun.

«Glenfis Cloud Talk» Sicherheit in der Cloud

Sicherheit in der Cloud

Shared Responsibility Model (IaaS)

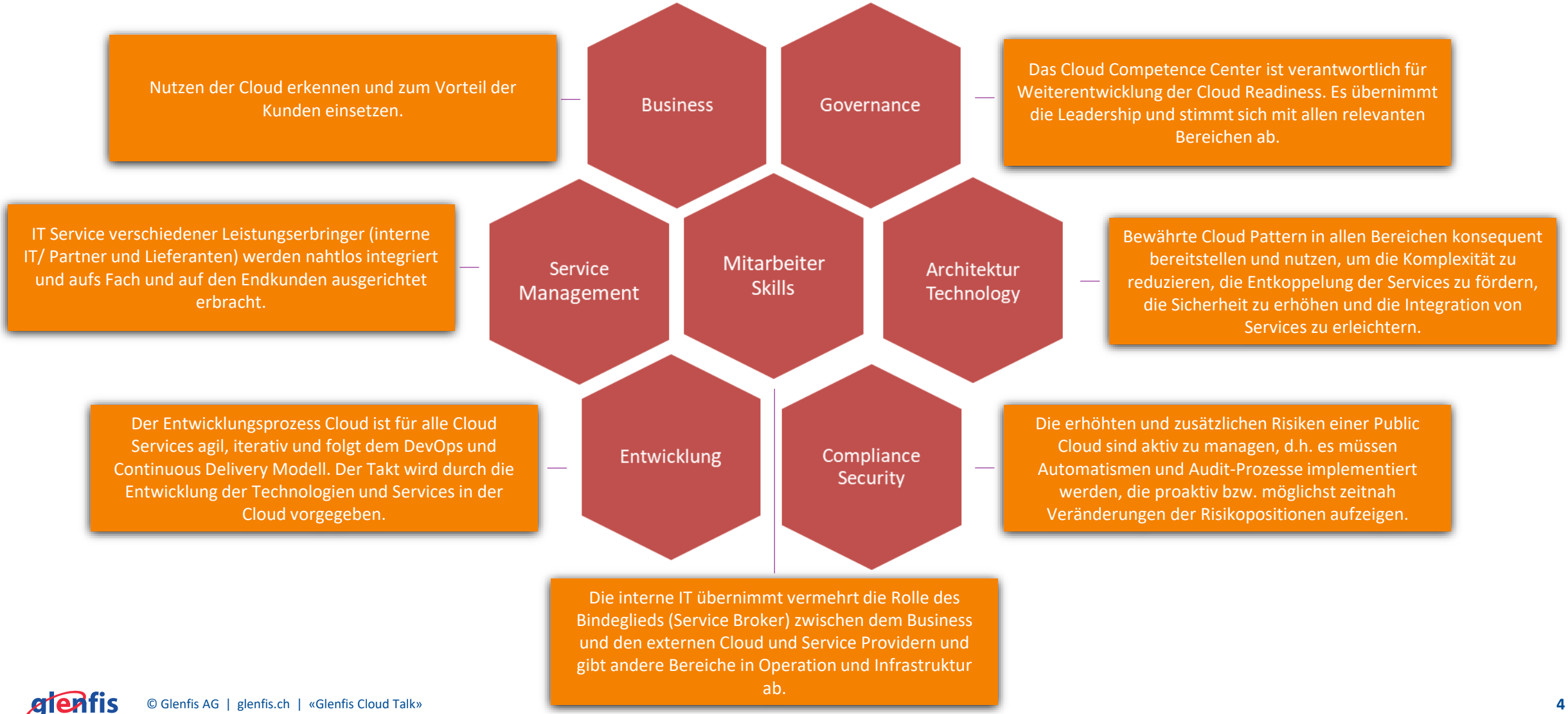
Gartner: "By 2020 95% of cloud security failures will be the customer's fault"

Kennen – beraten und unterstützen
Use Case: Cloud Readiness Assessment

Kundensituation	Schweizer Versicherung ist seit einigen Jahren auf der Reise in die Cloud und will besser verstehen, welche Risiken und Sicherheitslücken bestehen. Verbesserungspotentiale für die Sicherheit der Cloud Services sollen identifiziert und anschliessend eliminiert oder reduziert werden.
Herausforderung	Ein Assessment soll die in der Strategie definierte Handlungsfelder berücksichtigen und möglichst viele der etablierten Frameworks (Cobit, ITIL, etc.) berücksichtigen.
Was haben wir gemacht	Glenfis erhielt den Auftrag ein Cloud Readiness Assessment auszuarbeiten und durchzuführen.
Was war der Nutzen	Im Abschlussbericht wurde Stärken, Schwächen, Chance und Gefahren transparent aufgezeigt und konkrete Verbesserungsmassnahmen für die Umsetzung ausformuliert. Die erfolgreiche Umsetzung der definierten Massnahmen wird mittels eines weiteren Assessments in 6 Monaten überprüft.

Kennen – beraten und unterstützen

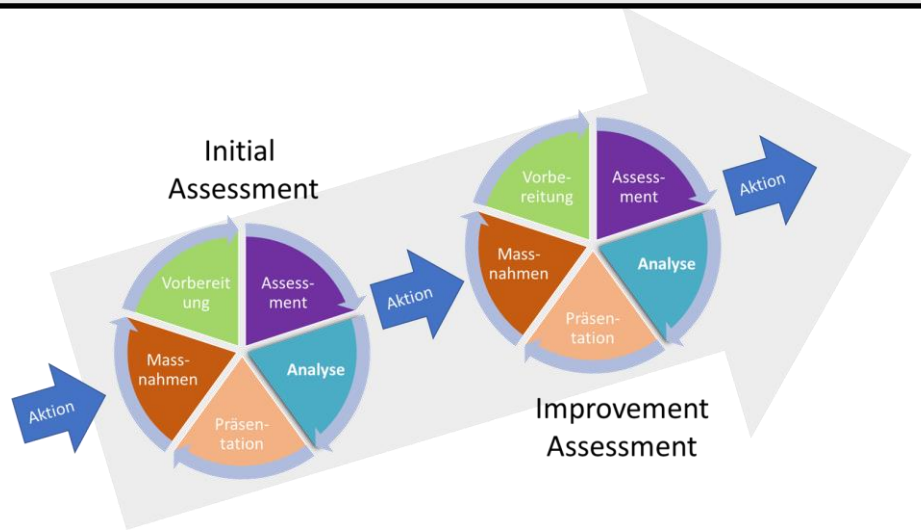
Use Case: Cloud Readiness Assessment

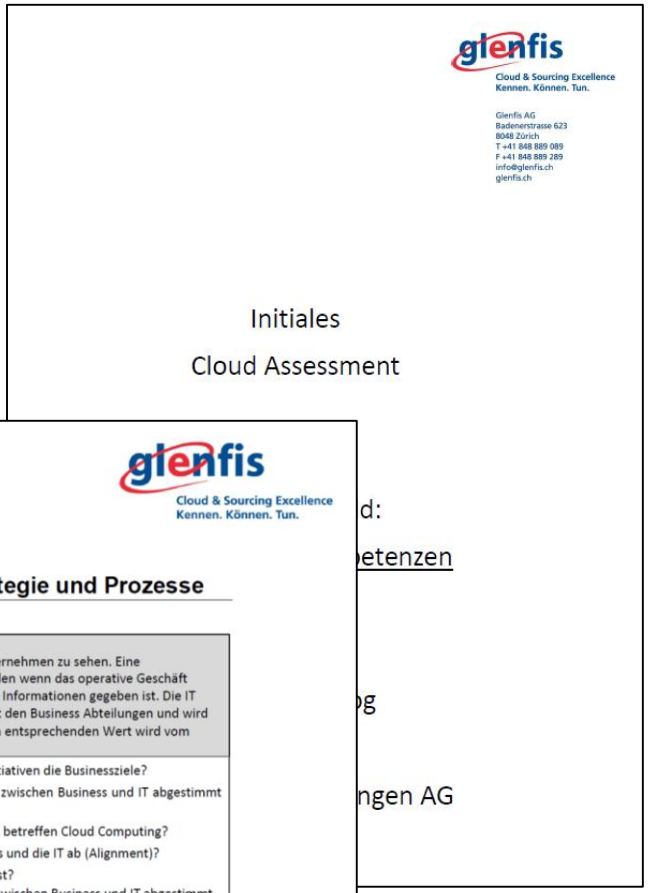


Kennen – beraten und unterstützen

Use Case: Cloud Readiness Assessment

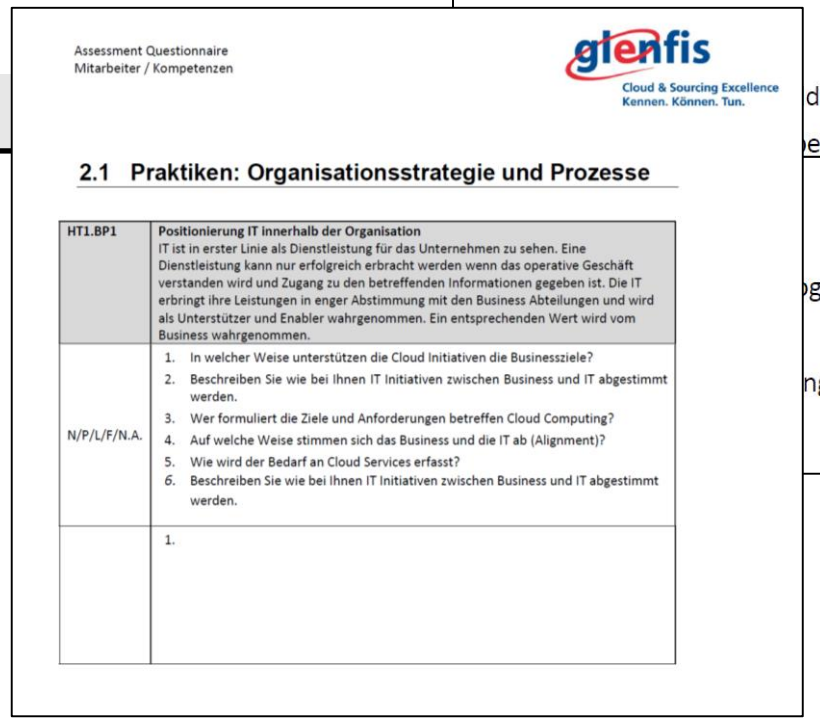
Umfang Fragenkatalog	
Handlungsfelder	7 Dimensionen gemäss Strategie
Hauptthemen	Je Handlungsfeld 6 Hauptthemen (42)
Themenbereiche	Je Hauptthema ca. 5 Themenbereiche (200)
Fragen	Je Themenbereich ca. 5 Fragen (1’000)
Verbesserungen	24 ausformulierte Verbesserungsmassnahmen




glenfis
Cloud & Sourcing Excellence
Kennen. Können. Tun.

Glenfis AG
Badenerstrasse 623
8048 Zürich
T +41 848 889 089
F +41 848 889 289
info@glenfis.ch
glenfis.ch

Initiales
Cloud Assessment


Assessment Questionnaire
Mitarbeiter / Kompetenzen

glenfis
Cloud & Sourcing Excellence
Kennen. Können. Tun.

2.1 Praktiken: Organisationsstrategie und Prozesse

HT1.BP1	**Positionierung IT innerhalb der Organisation** IT ist in erster Linie als Dienstleistung für das Unternehmen zu sehen. Eine Dienstleistung kann nur erfolgreich erbracht werden wenn das operative Geschäft verstanden wird und Zugang zu den betreffenden Informationen gegeben ist. Die IT erbringt ihre Leistungen in enger Abstimmung mit den Business Abteilungen und wird als Unterstützer und Enabler wahrgenommen. Ein entsprechenden Wert wird vom Business wahrgenommen.
N/P/L/F/N.A.	1. In welcher Weise unterstützen die Cloud Initiativen die Businessziele? 2. Beschreiben Sie wie bei Ihnen IT Initiativen zwischen Business und IT abgestimmt werden. 3. Wer formuliert die Ziele und Anforderungen betreffen Cloud Computing? 4. Auf welche Weise stimmen sich das Business und die IT ab (Alignment)? 5. Wie wird der Bedarf an Cloud Services erfasst? 6. Beschreiben Sie wie bei Ihnen IT Initiativen zwischen Business und IT abgestimmt werden.
	1.

Können – lernen und anwenden

Use Case: Secure Cloud Services

Kundensituation	Industriebetrieb hat bereits einige Cloud Services im Einsatz. Der Wechsel von technologie- hin zu serviceorientiertem IT-Management bereitet der IT Schwierigkeiten. Die Sicherheit der Cloud Services wird nicht aktiv gemanagt.
Herausforderung	Die Mitarbeiter mussten von der Veränderung überzeugt und dazu motiviert werden die Verantwortung für die Cloud Services wahrzunehmen.
Was haben wir gemacht	Ein auf die Kundenbedürfnisse zugeschnittenes Mitarbeiter-Entwicklungsprogramm wurde ausgearbeitet. Business Simulationen unterstützten die Mitarbeitermotivation für den Veränderungsprozess. Kombinierte E-Learning Module und direkter Unterricht steigerten die Effizienz und senkten die Kosten.
Was war der Nutzen	Bei den Mitarbeitern konnte das Basiswissen für sichere Cloud Services vermittelt werden. Die kontinuierliche Weiterentwicklung wird mittels Coaching und Beratungsleistungen sichergestellt.

Können – lernen und anwenden

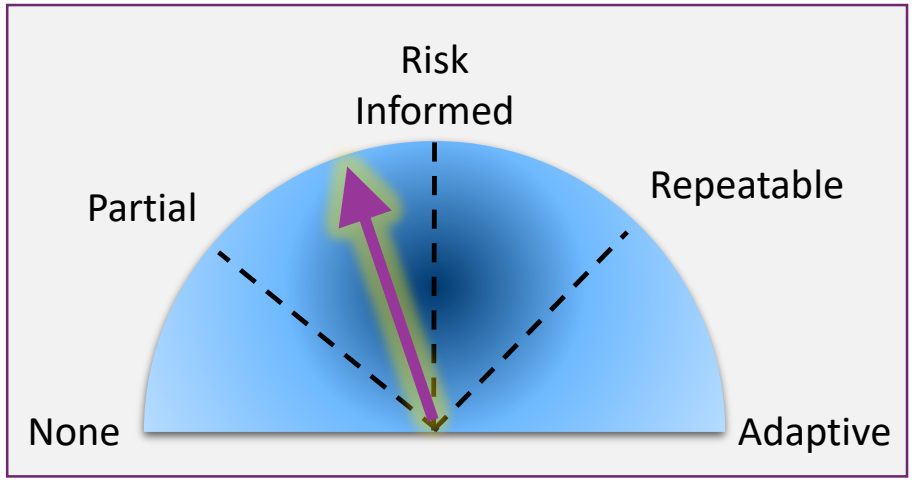
Use Case: Secure Cloud Services

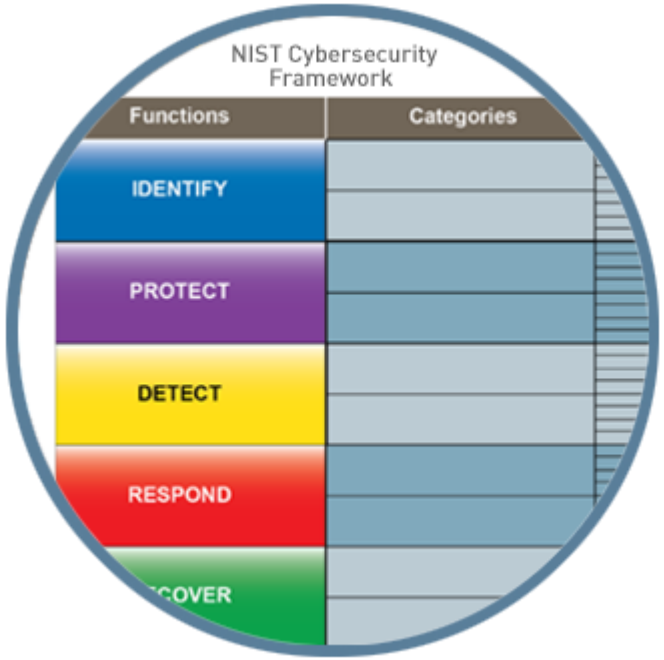
Glenfis hat basierend auf den Kundenbedürfnissen ein zugeschnittenes Ausbildungsprogramm erstellt und umgesetzt.

Trainingsmodule:	Kurs: 1	Kurs: 2	Kurs: 3	Methodik:
	• **Service Management Basic Training** – ITIL Einführung – Service Integration & Management (SIAM)	• **Cloud Computing Basic Training** – NIST Cloud Modell – Cloud Service Management – Cloud Governance	• **Cloud Security Basic Training** – Cybersecurity Foundation (NIST) – Risiko Management Prozesse und Praktiken – Information Security based on ISO 27001	Präsenzkurs kombiniert mit E-Learning und Business Simulation

Können – lernen und anwenden

Use Case: Secure Cloud Services





Training Cybersecurity Framework NIST

- Ermöglicht Flexibilität bei der Umsetzung und bringt Konzepte für Reifegradmodelle ein
- Reflektiert wie ein Unternehmen die Kernfunktionen des Frameworks implementiert und seine Risiken steuert
- Progressiv, von partiell (Stufe 1) bis adaptiv (Stufe 4), wobei jede Stufe auf der vorherigen Stufe aufbaut
- Merkmale werden auf Organisationsebene definiert und auf das Framework angewendet, um zu bestimmen, wie eine Kategorie implementiert ist

Tun – umsetzen und implementieren

Use Case: DevOps Collaboration

Kundensituation	IT Dienstleister betreibt DevOps seit Monaten und stellt fest, dass zwar mit DevOps Tools (Azure DevOps) gearbeitet wird und einige Methoden (Kanban, Scrum) angewandt werden, die teamübergreifende Zusammenarbeit jedoch nicht wie erhofft funktioniert. Vor allem die Zusammenarbeit mit Security ist nicht gewährleistet.
Herausforderung	Die Teamleiter sind sich nicht bewusst, dass die übergreifende Zusammenarbeit der wichtigste Baustein einer erfolgreichen DevOps Transformation sind.
Was haben wir gemacht	In einer Business Simulation (The Phoenix Project) erfuhren die Teamleiter wie wichtig die kulturelle Veränderung und die übergreifende Zusammenarbeit ist.
Was war der Nutzen	Die Motivation zu einer besseren teamübergreifenden Zusammenarbeit konnte gesteigert werden. Es wurden konkrete Schwachstellen aufgedeckt (Communication-, Facilitation & Leadership Skills) die nun aktiv mittels Training und Coaching angegangen wird.

Tun – umsetzen und implementieren

Use Case: DevOps Collaboration

Beispiel: Graben basierend auf unterschiedlicher Sichtweise zwischen Security und Entwicklung:

ISMS Richtlinien Beispiel
Wesentlicher Bestandteil einer ISO 27001 Dokumentation

2. Backuprichtlinie *Beispielseite*

2.1. Erstellung von Datensicherungen

Grundsätzlich werden alle zentralen Systeme gesichert.
Die zu sichernden Systeme werden in einer zentralen durch die IT verwaltete Datei aufgelistet. Es gibt zentrale Systeme, die von der Sicherung ausgeschlossen werden können (z.B. Test-Systeme). Die Ausnahmen hierzu müssen in genannter Datei schriftlich begründet werden.

Zusätzlich werden Einzelplatzgeräte gesichert, wenn diese Nutzdaten enthalten, die nicht zentral gespeichert werden.

Dies trifft z.B. auf Spezialsoftware, Smartphones oder kleinere Betriebe zu. Denken Sie beispielsweise an lokale Bankensoftware.

Datensicherungen werden automatisch protokolliert und bei entstandenen Fehlern wird eine Alarmierung durch E-Mail oder das Monitoring System ausgelöst.

Alle Datensicherungen werden gespiegelt in zwei Standorten gespeichert, um einen Verlust durch Brand vorzubeugen.

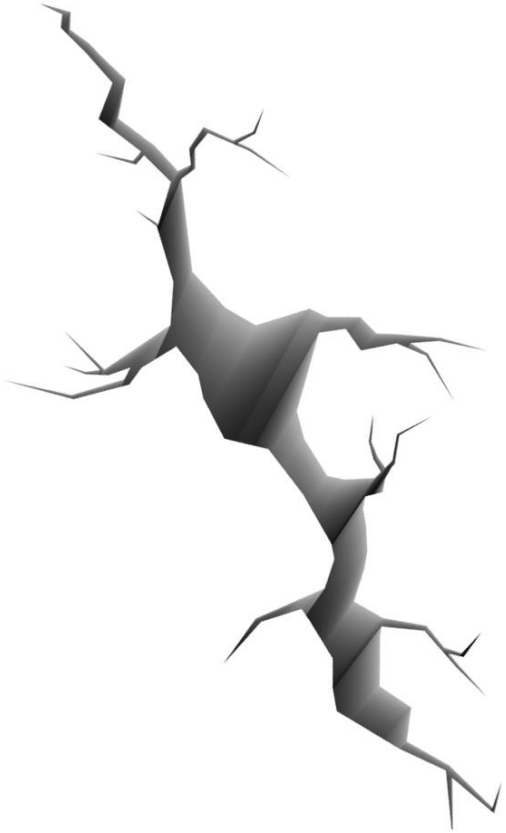
Fassen Sie die Ziele Ihrer Backup-Strategie hier zusammen.

Die detaillierte Vorgehensbeschreibung liegt im Zweifelsfall der Fachabteilung vor. Konzentrieren Sie sich hier auf die übergeordneten Anforderungen.

Backups sollten, wenn möglich, unabhängig von Ihrem Rechenzentrum gespeichert werden (für Fälle wie Brand o.ä.); z.B. durch Spiegeln in einen anderen Standort oder die Nutzung eines Cloud-Dienstes, der Ihre Backups ebenfalls vorhält.

2.2. Test von Datensicherungen

Datensicherungen werden regelmäßig auf Wiederherstellbarkeit geprüft. Alle Datensicherungen werden im Quartalstakt auf virtuellen Maschinen testweise widerhergestellt und die Funktion der Programme als auch die Vollständigkeit der Daten überprüft. Die Überprüfung geschieht außerplanmäßig, wenn Änderungen am



Azure Policy-Beispiel
Zulassen eines benutzerdefinierten VM-Images aus einer Ressourcengruppe

```
{
    "type": "Microsoft.Authorization/policyDefinitions",
    "name": "custom-image-from-rg",
    "properties": {
        "displayName": "Allow custom VM image from a Resoruce Group",
        "description": "This policy allows only usage of images from a resource group",
        "parameters": {
            "resourceGroupName":{
                "type":"String",
                "metadata":{
                    "displayName": "Resource Group Name",
                    "strongType": "ExistingResourceGroups"
                }
            }
        },
        "policyRule": {
            "if": {
                "allOf": [
                    {
                        "field": "type",
                        "equals": "Microsoft.Compute/virtualMachines"
                    },
                    {
                        "not": {
                            "field": "Microsoft.Compute/imageId",
                            "contains": "[concat('resourceGroups/',parameters('resourceGroupName'))]"
                        }
                    }
                ]
            },
            "then": {
                "effect": "deny"
            }
        }
    }
}
```

Glenfis Prinzip

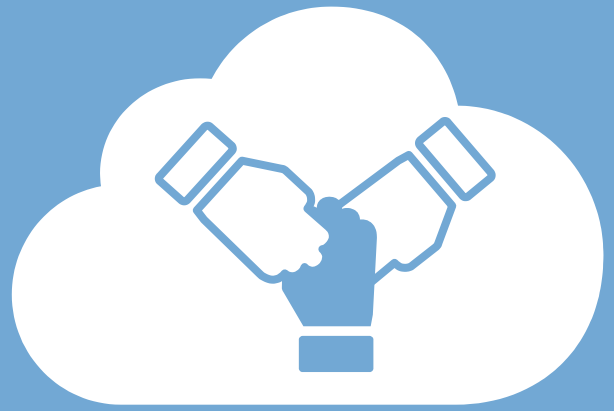
Vom Kennen – Zum Können – Zum Tun

Kennen.

Wir beraten Sie, wie Sie Ihre IT-Anforderungen in einen Mehrwert für Ihr Unternehmen umsetzen können.

Können.

Wir schulen Sie und Ihr Team, damit Sie schon heute fit für die Digitalisierung von morgen sind.



Tun.

Wir begleiten Sie bei der Umsetzung Ihrer IT-Strategie.