Application Recovery Plan

Site Name	ACME Premises
Application Name	Microsoft Dynamics 365
Document Version	0.1
Date	15/09/2021

Contents

Table of Figures

1 DOCUMENT CONTROL

1.1 Document Responsibility

	Name, Department	Office Phone #	Additional Phone #
Application Custodian (accountable)			
Application Recovery Planner (responsible)			
Information Security Officer (informed or consulted)			

1.2 Document Revision History

Revision Date	Version	Revision Summary
2019-10-17	0.1	First version

2 SYSTEM OVERVIEW AND APPLICATION RECOVERY

2.1 Application recovery VS Disaster Recovery

The presented plan refers to the recovery of the ERP application, thus not includes scenarios related to outage of the on-premises infrastructure (Fig. 1). For the purposes of the AR plan, it is assumed, Microsoft Dynamics 365 ERP is implemented as its capabilities suit well to a medium-size company compared to solutions such as SAP, Oracle Fusion Cloud ERP.

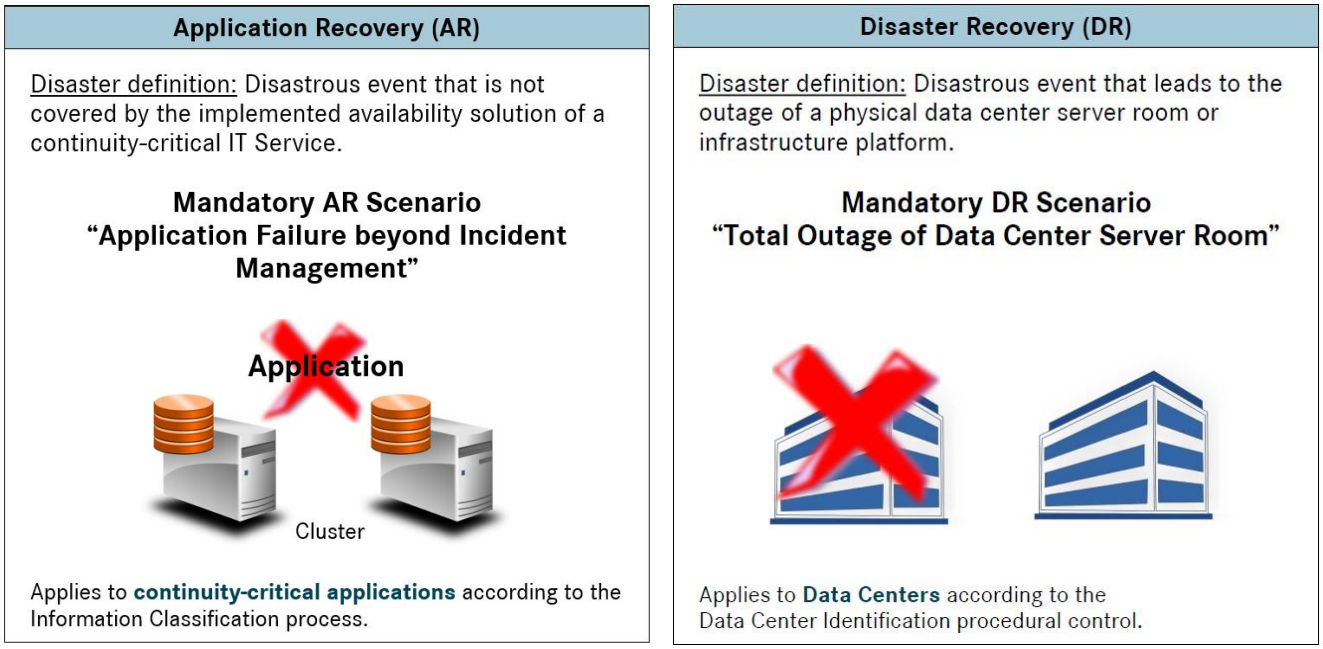

Figure 1 Application Recovery and Disaster Recovery definitions

2.2 System Overview

The ERP conceptual architecture provides performance, resilience, and core ERP component protection from cyber-attacks from within ACME local area networks, through virtualization and network segmentation. The hybrid architecture incorporates on-premises equipment for the primary ERP solution with application recovery enabled provided through commercial cloud infrastructure using infrastructure as code for system recovery and cloud storage for data backup and recovery. Assuming ACME's workforce will primarily access the ERP solution from internal networks, on-premises costs less than comparable cloud infrastructure and is not subject to connectivity or latency issues associated with internet hosted systems.

Computer hardware continues to increase in capacity and decrease in cost while the compute requirements for server operating systems and certain applications remain relatively static (Microsoft, 2021). Virtualization technologies enable better utilization by hosting numerous systems on modest commercial server hardware at a much lower capital and environmental cost than running each system on individual hardware (Belanger & Casemore, 2019). Savings are such that completely redundant hardware can be implemented for additional solution resilience (Fig 2) at a lower cost than stand-alone servers (Dell, 2021) with no redundancy.

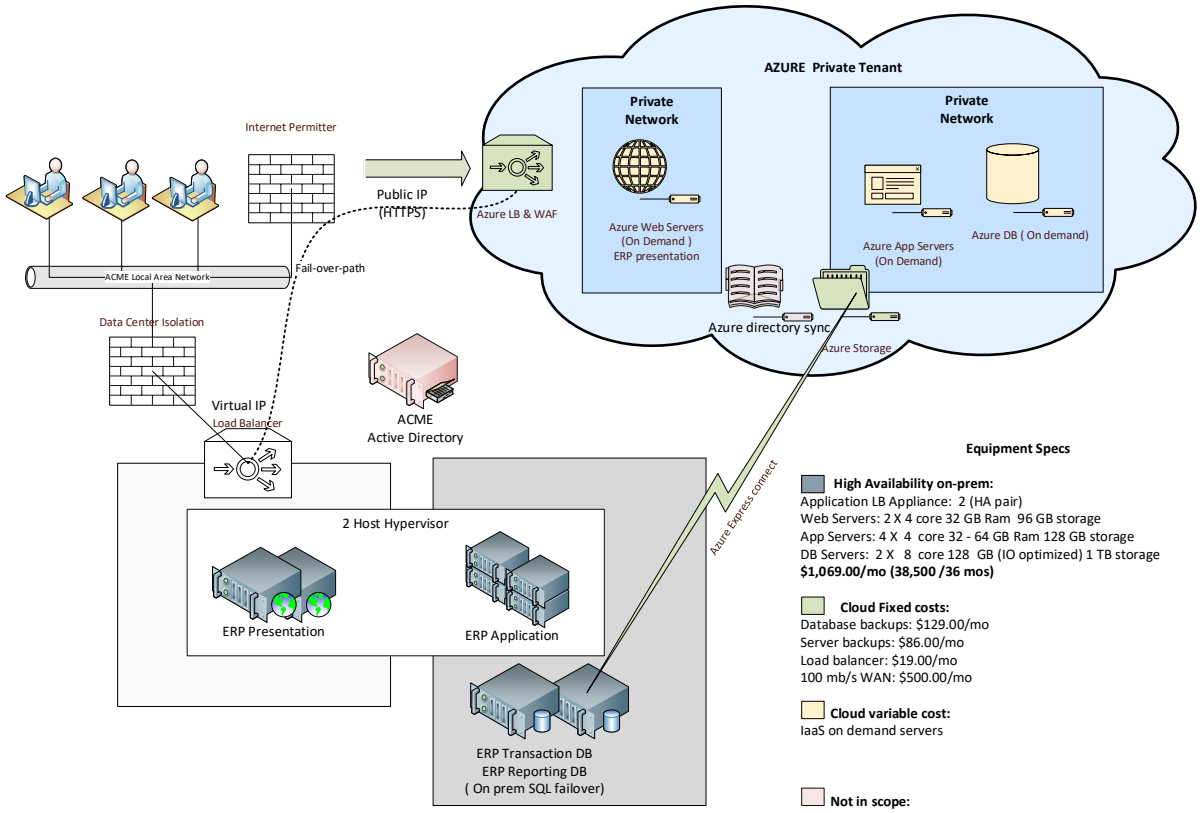

Figure 2 ERP Hybrid Resilience

Modern adversarial activity, either through automated malware or interactive command and control is designed to compromise enterprises by initially gaining access to user workstations behind corporate internet firewalls then pivoting to attack other internal systems. Therefore, additional firewalls between user workstation and server networks are recommended for high consequence information assets such as an ERP system (Paloalto Networks, 2021). ERP components can be placed in different zones with interzone communications protected via VLAN specific policies implemented within a Next Generation firewall. Cloud storage communications should take place over dedicated private circuits to isolate backup traffic from ERP users and reduce load on the segmentation firewall (Fig. 3).

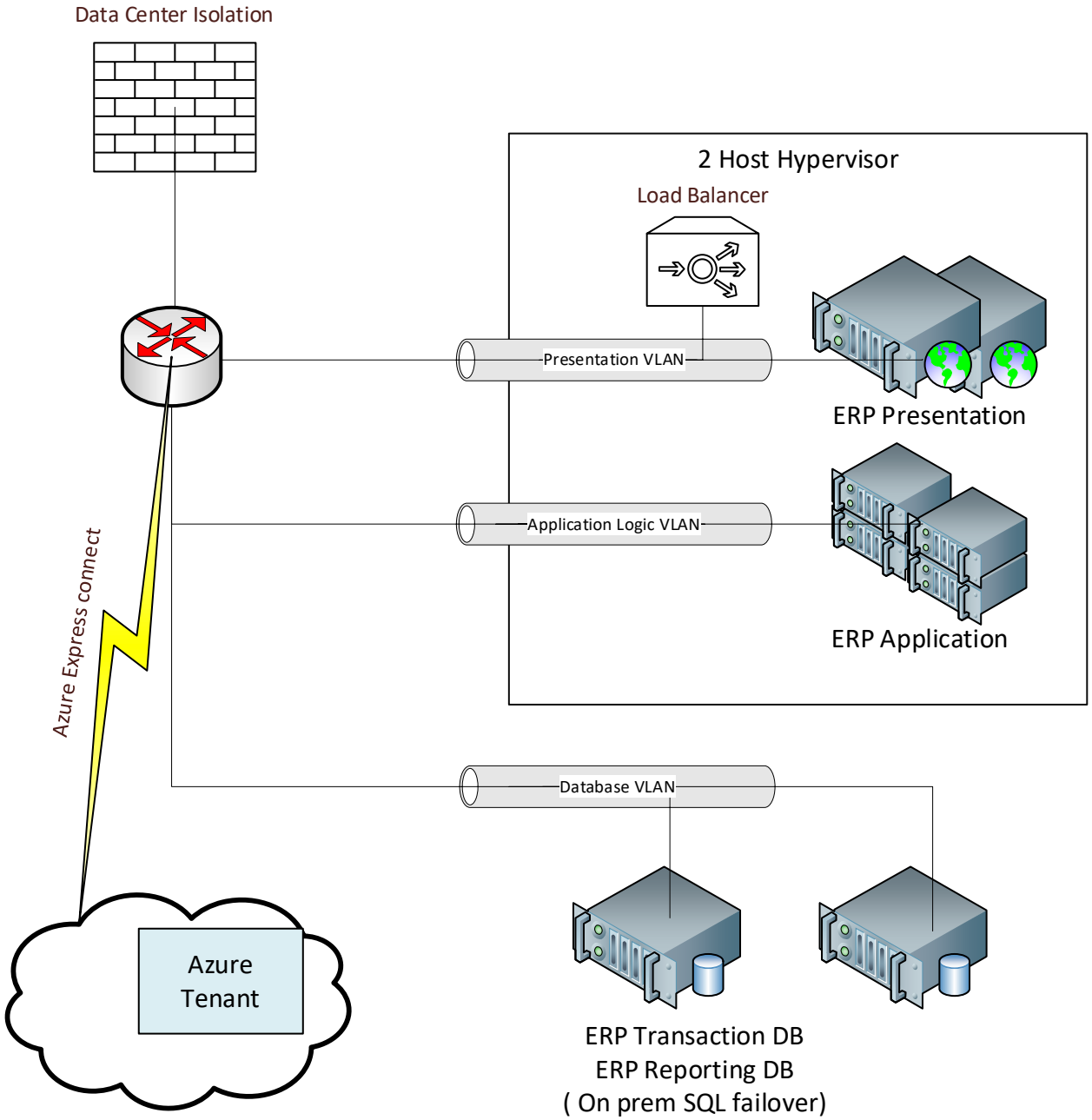

Figure 3 User LAN and zone segmentation

2.3 Application Recovery Scenario

SID	Scenario Name	Scenario Enablers
A1	Web server failure beyond incident management	• *Human factor (malicious or accidental)* • *Hardware failure* • *Denial of service (malicious, accidental, or environmental)* • *Ransomware infection*
A2	Application server failure beyond incident management	• *Human factor (malicious or accidental)* • *Hardware failure* • *Denial of service (malicious, accidental, or environmental)* • *Ransomware infection*
A3	Database server failure beyond incident management	• *Human factor (malicious or accidental)* • *Hardware failure* • *Denial of service (malicious, accidental, or environmental)* • *Ransomware infection*
A4	Data loss/corruption beyond incident management	• *Human factor (malicious or accidental)* • *Ransomware infection*

The AR Strategy is structured along the architecture/implementation tiers of the application. Specific recovery activities are assigned and documented for each tier. The overall concept is focused on recovery of the service delivered by the application for business purposes within the agreed RTO (Recovery Time Objective) and RPO (Recovery Point Objective). Interim solutions with temporarily degraded application performance could be accepted parts of the recovery plan, when necessary to achieve RTO / RPO. Application and information security or key application functionalities may not be abandoned, though.

The overall architecture of the application avoids single points of failure or at least provides fast recovery capabilities.

The operational processes as well as the application itself are documented, maintained, and tested in accordance with all relevant operations standards. Where external partners are involved, adequate SLA reflecting standards and RTO / RPO are in place. References to additional information are documented in section “3.6 Required Resources for Recovery Activities.”

In case of AR disaster case declaration, execution of the Application Recovery Plan will be authorized by the Application Custodian or their representative in agreement with the Major Incident Manager and business representative(s). See section “3.2 Invocation of Application Recovery Plan Execution” for authorization of AR Plan execution.

2.4 AR Solution for Scenario A1 (Web server failure beyond incident management)

Recovery Activities								
SID	Responsible Function/Role/ Person	Duration	Start*	End*	Description of Recovery Activity	Prerequisite for Recovery Activity	References / More detailed Information	Remarks / Expected Results
A1	Application UI developer	00:05			- Schedule next "Status & Decision" meeting with Application Custodian. - Start recovery logbook using the "Status & Decision" template.	AR invoked by Application Custodian.		- Next "Status & Decision" meeting scheduled - Logbook started
A1	Application UI developer and Cloud Service Provider Operations Unit	00:30			Issue request to Cloud Service Provider Operations Unit: - Restore of last known good V-Host system configuration, if V-Host is affected - Restore of last known good guest OS and web server installation	Point in time of last known good backup determined		Guest OS and web server installation/ restored
A1	Application UI developer	00:15			Restore of last known good web server configuration and content data.	Point in time of last known good backup determined		Web server configuration and content data restored
A1	Application UI developer	00:15			Check overall configuration and start web server	- Guest OS is running - Web server content data is accessible		- Web server is running and reachable - Communication with application server is established
A1	Application UI developer	00:15			Execute web server functionality check	Web server is running and reachable		Web server is recovered
A1	Application UI developer	00:15			Confirm recovery of web server to Application Custodian	Successful test		Web server recovery confirmed

* Start and end times to be filled in during plan execution

2.5 AR Solution for Scenario A2 (Application server failure beyond incident management)

Recovery Activities								
SID	Responsible Function/Role/ Person	Duration	Start*	End*	Description of Recovery Activity	Prerequisite for Recovery Activity	References / More detailed Information	Remarks / Expected Results
A2	Application backend architect and developer	00:05			- Schedule next "Status & Decision" meeting with Application Custodian. - Start recovery logbook using the "Status & Decision" template.	AR invoked by Application Custodian.		- Next "Status & Decision" meeting scheduled - Logbook started
A2	Application backend architect and developer and Cloud Service Provider Operations Unit	00:30			Issue request to Cloud Service Provider Operations Unit: - Restore of last known good OS and middleware installation/configuration data	Point in time of last known good backup determined		OS and application server installation restored
A2	Application backend architect and developer	00:15			Restore of last known good application executables and configuration data	Point in time of last known good backup determined		Application server restored
A2	Application backend architect and developer	00:15			Check overall configuration and start application	- OS is running - Configuration data is accessible		- Application is running and reachable - Interfaces to linked applications technically established
A2	Application backend architect and developer	00:05			Confirm recovery of application server to Application Custodian	Successful test		Application server recovery confirmed
A2	Application backend architect and developer	00:05			- Schedule next "Status & Decision" meeting with Application Custodian. - Start recovery logbook using the "Status & Decision" template.	AR invoked by Application Custodian.		- Next "Status & Decision" meeting scheduled - Logbook started

* Start and end times to be filled in during plan execution

2.6 AR Solution for Scenario A3 (Database server failure – Data loss/ corruption beyond incident management)

Recovery Activities								
SID	Responsible Function/Role/ Person	Duration	Start*	End*	Description of Recovery Activity	Prerequisite for Recovery Activity	References / More detailed Information	Remarks / Expected Results
A3 – A4	DB architect and administrator	00:05			- Schedule next "Status & Decision" meeting with Application Custodian. - Start recovery logbook using the "Status & Decision" template.	AR invoked by Application Custodian.		- Next "Status & Decision" meeting scheduled - Logbook started
A3 – A4	DB architect and administrator and Cloud Service Provider Operations Unit	00:30			Issue request to Cloud Service Provider Operations Unit: - Restore of last known good V-Host system configuration, if V-Host is affected - Restore of last known good guest OS and DBMS installation	Point in time of last known good server backup determined		Guest OS and DBMS installation restored
A3 – A4	DB architect and administrator	00:15			Restore of last known good DBMS configuration	Point in time of last known good configuration backup determined		DBMS configuration restored
A3 – A4	DB architect and administrator	00:15			Check overall configuration and start DBMS	- Guest OS is running - (Recovered) database data is accessible		- DBMS is running and reachable - Database data accessible
A3 – A4	DB architect and administrator	00:15			Execute DBMS functionality check	- DBMS is running and reachable - Database data accessible		DBMS is recovered
A3 – A4	DB architect and administrator	00:30			Roll forward of transactions from DBMS transaction logs to the desired point in time (before data loss/corruption occurred).	- Point in time of last known good data determined		Database data restored to last known good transaction
A3 – A4	DB architect and administrator	00:05			Confirm recovery of database server to Application Custodian	Successful test		Database server recovery confirmed

* Start and end times to be filled in during plan execution

3 SUPPORTING INFORMATION

3.1 Recovery Time & Point Objectives

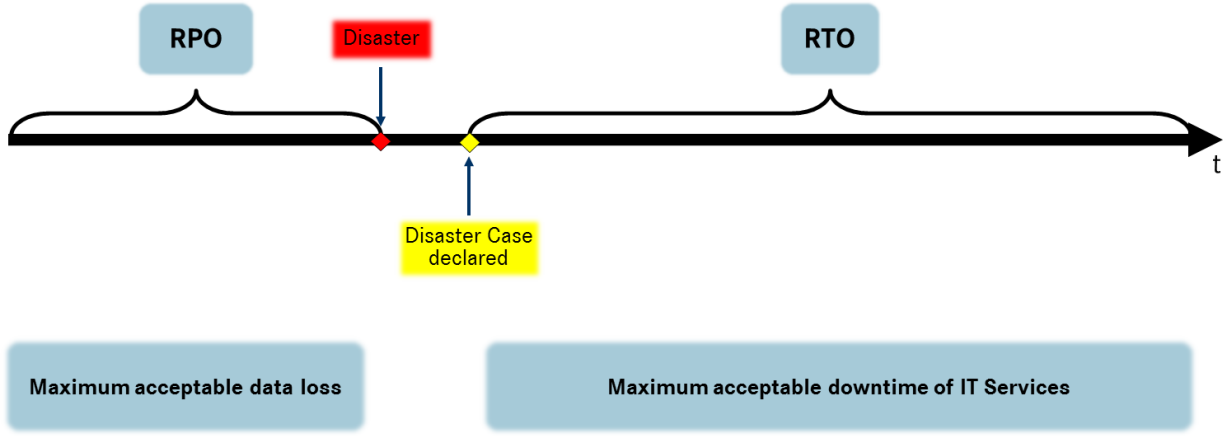

Figure 4 RTO and RPO

RTO: Business objective for the maximum timeframe for recovery of IT Services, starting with Disaster Case declaration

RPO: Business objective for the maximum timeframe for permanent data loss

The business requirements for the recovery of this application are:

Recovery Time Objective (RTO)	Recovery Point Objective (RPO)
4 Hours	15 Minutes

3.2 Invocation of Application Recovery Plan Execution

Disaster declaration may be requested as the outcome of the (Major) Incident Management process.

- If declaration of the disaster case is accepted, execution of Application Recovery is authorized.
- If declaration of the disaster case is rejected, the (Major) Incident Management process will be resumed.

The following persons or functions are entitled to accept or to reject declaration of the Application Disaster case.

Function / Unit / Person	Office Phone #	Additional Phone #

3.3 Approval Authorization

The following persons or functions have approval authorization for the listed tasks:

Task	Function / Unit / Person	Office Phone #	Additional Phone #
Financial Decision Authority e.g. for ad hoc ordering of IT expert services, exceeding existing contracts			

3.4 Internal/External Communications

Communication of situation/status information and on ongoing recovery activities to stakeholders (e.g. executive management, staff, suppliers, customers, shareholders, official authorities) must follow the organization's mandatory communication policy. Especially regarding communication to external stakeholders that is not covered by **N**on-**D**isclosure-**A**greements (e.g. the media and official authorities) approved communication procedures must be applied.

The following persons or functions are authorized to initiate and/or approve internal/external communication:

Function / Unit / Person	Office Phone #	Additional Phone #

The following stakeholders (e.g. executive management, staff, suppliers, customers, shareholders, official authorities) will be informed about ongoing recovery activities:

Function / Unit / Person	Office Phone #	Additional Phone #

3.5 Recovery Team and Third Parties

Required functions/persons will be contacted following the communication chain initiated by a function/person authorized to invoke the AR Plan execution. The listed Recovery Team members are responsible for conducting the respective recovery actions:

Microsoft Dynamics 365						
#	Name	Function and Responsibility	Will contact	Contact Information		
				Phone #	Email	Location
(1)		Application Custodian executes and controls recovery process	(2) (3) (4) (5)			ACME HQ
(2)		IT/APP dept. senior management				ACME HQ
(3)		Application UI developer: Webserver recovery	(6)			ACME HQ
(4)		Application backend architect and developer: Application server recovery	(6)			ACME HQ
(5)		DB architect and administrator Database server and data recover	(6)			ACME HQ

Third Parties / Suppliers						
No.	Name	Function and Responsibility	Will contact	Contact Information		
				Phone #	Email	Location
(6)	Cloud Service Provider	Data center operations execute recovery tasks Accountable for contract fulfillment				

3.6 Required Resources for Recovery Activities

Resource	Supportive Documentation	Contact Information
Backup data / media	Not disclosed	
Contract and SLA with Cloud Service Provider	Documentation Description Location	
Installation media and license information for standard software	Documentation Description Location	
Application installation, configuration, and operations guide	Documentation Description Location	
DBMS installation, configuration and operations guide	Documentation Description Location	

4 ANNEX - TEMPLATE "STATUS & DECISION"

Incident (Ticket Number)	
Short description of initial situation	

Date/Time	**Status/Decision**	**Responsible**	**Remarks**