DAKESSIAN CONSULTING

DR & BC PLANNING CONSULTANCY SERVICES

THE THREE STAGE APPROACH

- Stage I - Review & Assessment
- Stage II - Design & Development
- Stage III - Testing

STAGE I – REVIEW & ASSESSMENT

- Business Impact Analysis
- DR IT Infrastructure Assessment
- Partial Failover & Provide Recommendations
- Replication Mechanisms (RPO, RTO)

STAGE II – DESIGN & DEVELOPMENT

- Develop DR Strategy
- Develop DR Plan
- Develop DR Scenarios
- Develop DR Run Book

STAGE III – TESTING

- DR Testing & Validation Switchover
- Participate in DR Testing & Validation

BASIS OF DELIVERABLES

- Best Practice Report Templates
- Our Own Report Templates
- Reports Customized for your requirements

METHODOLOGY

- Disaster Disruption Scenarios
- Disaster Type Scenarios
- Identification Of Threats, Levels & Impacts
- Risk Scale & Actions
- Risk level Matrix

DISASTER TYPE SCENARIOS

- Infrastructure
- Financial
- Human Resources
- Political & Regulatory
- Products & Services
- Information Technology

DISASTER TYPE SCENARIOS

Infrastructure	Financial
• Total or partial destruction of Data Centre by fire • Hazardous waste spill results in extended denied or restricted access to Data Center • Destruction of a nearby electrical sub-station results in prolonged loss of power to Data Centre • Theft of vital hardware and/or key office systems or equipment • Destruction of some or all physical files and critical business records • Destruction of underground cables results in loss of voice and/or data communications	• A material financial loss results in capital depletion or cash flow strain • Material internal fraud or misappropriation of funds by a disgruntled employee • Material external fraud by a third-party from forged contracts, documents and invoices • Internal control breakdowns lead to data entry errors, unintentional accounting errors and failed mandatory reporting of financial positions • Senior management fictitiously adjust financial position to ensure bonuses • Adverse economic conditions likely to sharply reduce projected revenue • Insurer rejects insurance claim resulting in a material expense and future liability
Human Resources	**Political & Regulatory**
Products & Services	**Information Technology**

DISASTER TYPE SCENARIOS

Infrastructure	Financial
Human Resources	**Political & Regulatory**
• Major competitor head hunts your management team or key staff just before a peak business period • Flu pandemic greatly reduces workforce for extended periods • Strike or major employee dispute disrupts service delivery resulting in significant delays • Extreme weather reduces workforce for extended periods • Dust storm causing widespread air travel disruption preventing travel to key markets • Kidnap of CEO, CIO or a senior executive • Receipt of contaminated mail • Accusation that an employee has caused significant harm to another person or organization. • Armed individual enters the building threatening staff and customers	• Sudden regulatory changes require rapid alteration to current operating procedures • Government imposes travel restrictions during key business period • Loss of reputation from doing business with a regime in a banned country • Trade embargo imposed to key market • A major regulatory breach threatens your reputation, customer confidence and survival
Products & Services	**Information Technology**

DISASTER TYPE SCENARIOS

Infrastructure	Financial
Human Resources	**Political & Regulatory**
Products & Services	**Information Technology**
• Your most profitable product/service is tampered with • Accusation by a customer that major product/services caused significant damage or harm • Failure or bankruptcy of a key supplier impacting your ability to service customers • A bomb threat is received by reception from a disgruntled customer • A new project and/or product fails to deliver expected benefits resulting in material financial loss • A competitor gains access to information about your new product and/or intellectual property • Technical production line equipment fails resulting in significant delays to customers • Distribution channel fails due to a major contractual dispute with a distributor	• Security breach by an ex employee or a third party contractor is detected by your network security administrator • External hackers access confidential data • Hackers release confidential company information to media • A disgruntled current/former employee sabotages network files by placing passwords on shared documents and deleting important documents • A major virus or malicious code spreads over the entire network to all servers and end user devices leading to data/file corruption • A sustained DDOS attack.

THREAT LIKELIHOOD LEVELS

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede the vulnerability from being exercised.

IMPACT MAGNITUDES

Impact Magnitude	Impact Definition
High	Exercise of the vulnerability 1- may result in the highly costly loss of major tangible assets or resources; 2- may significantly violate, harm, or impede *your* mission, reputation, or interest; or 3- may result in human death or serious injury.
Medium	Exercise of the vulnerability 1- may result in the costly loss of tangible assets or resources; 2- may violate, harm, or impede *your* mission, reputation, or interest; or 3- may result in human injury.
Low	Exercise of the vulnerability 1- may result in the loss of some tangible assets or resources or 2- may noticeably affect your mission, reputation, or interest.

RISK SCALE & ACTIONS

Risk Level	Description and Necessary Action
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing IT system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, *you* must determine whether corrective actions are still required or decide to accept the risk.

RISK LEVEL MATRIX

Likelihood	Impact		
	Low (10)	Medium (50)	High(100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

IDENTIFY DISASTER TYPE CAUSES

Disaster Type Scenario	Natural Causes	Man Made Causes	Risk Level
Infrastructure	Yes	Yes	High
Financial	No	Yes	Medium
Human Resources	Yes	Yes	High
Political & Regulatory	No	Yes	Medium
Products & Services	No	Yes	Medium
Information Technology	No	Yes	High
Pandemics	Yes	Yes	High

NATURAL DISASTER APPLICABILITY

SITE 1 / NATURAL DISASTERS

Natural Disasters	Impact	Likelihood	Risk Level
Agricultural Diseases & Pests	Low 10	Low 0.1	1
Damaging Winds	Medium 50	Medium 0.5	25
Drought & Water Shortage	Medium 50	Medium 0.5	25
Earthquakes	High 100	High 1.0	100
Emergency Diseases / Pandemic	Medium 50	Medium 0.5	25
Heat Waves	High 100	High 1.0	100
Floods & Flash Floods	High 100	High 1.0	100
Hail Storms	Medium 50	Medium 0.5	25
Hurricanes & Tropical Storms	Low 10	Low 0.1	1
Landslides	Medium 50	Medium 0.5	25
Thunderstorms & Lightning	Medium 50	Medium 0.5	25
Tornadoes	Low 10	Low 0.1	1
Tsunamis	Low 10	Low 0.1	1
Wildfire	Low 10	Low 0.1	1
Winter & Ice Storms	Medium 50	Medium 0.5	25
Sinkholes	Low 10	Low 0.1	1

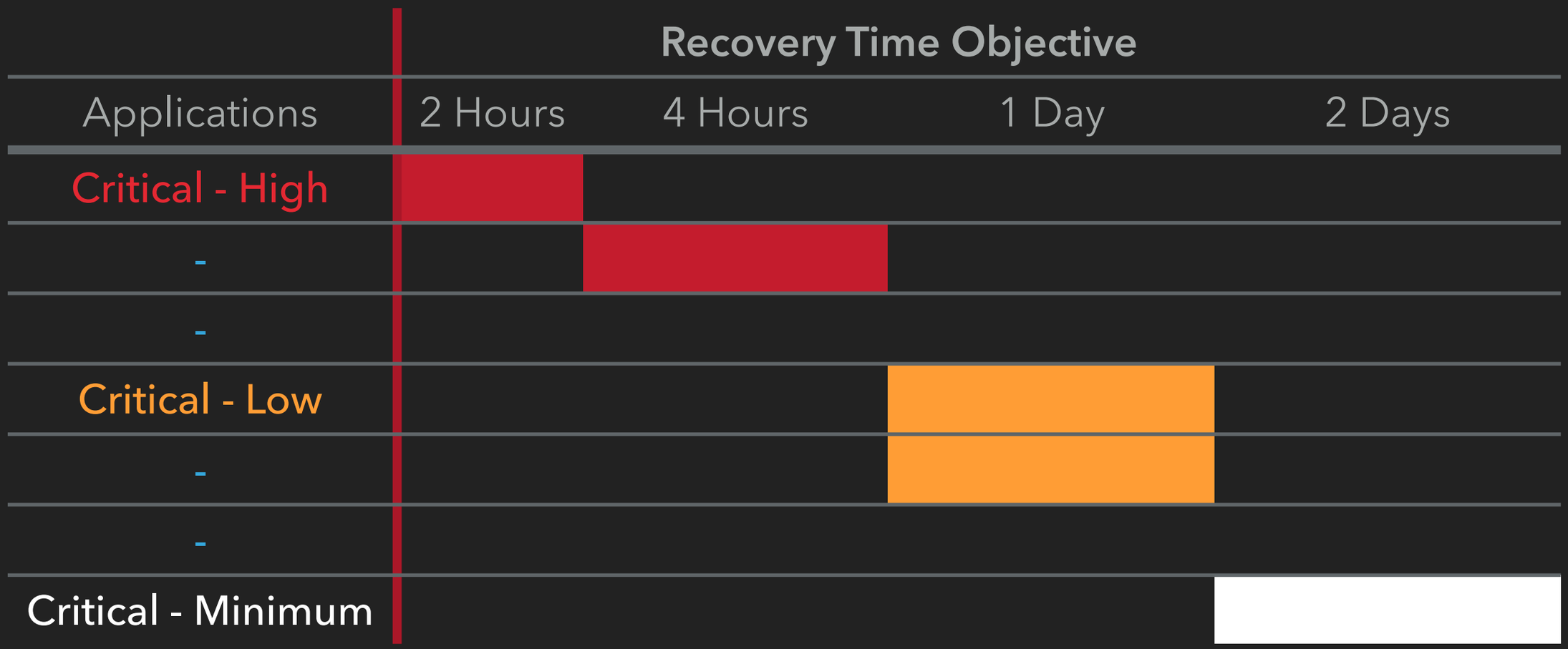
MAN MADE DISASTER APPLICABILITY

SITE 1 BUILDING / MAN MADE DISASTERS

Man Made Disasters	Impact	Likelihood	Risk Level
Hazardous Materials	Medium 50	Medium 0.5	25
Power Disruption & Blackout	High 100	High 1.0	100
Nuclear Plant Blast	Low 10	Low 0.1	1
Chemical & Biological Weapons Threat	Medium 50	Low 0.1	5
Cyber Attacks	High 100	High 1.0	100
Explosions	High 100	Medium 0.5	50
Civil Unrest	High 100	High 1.0	100
Arson	Medium 50	Medium 0.5	25
Terrorism	High 100	High 1.0	100

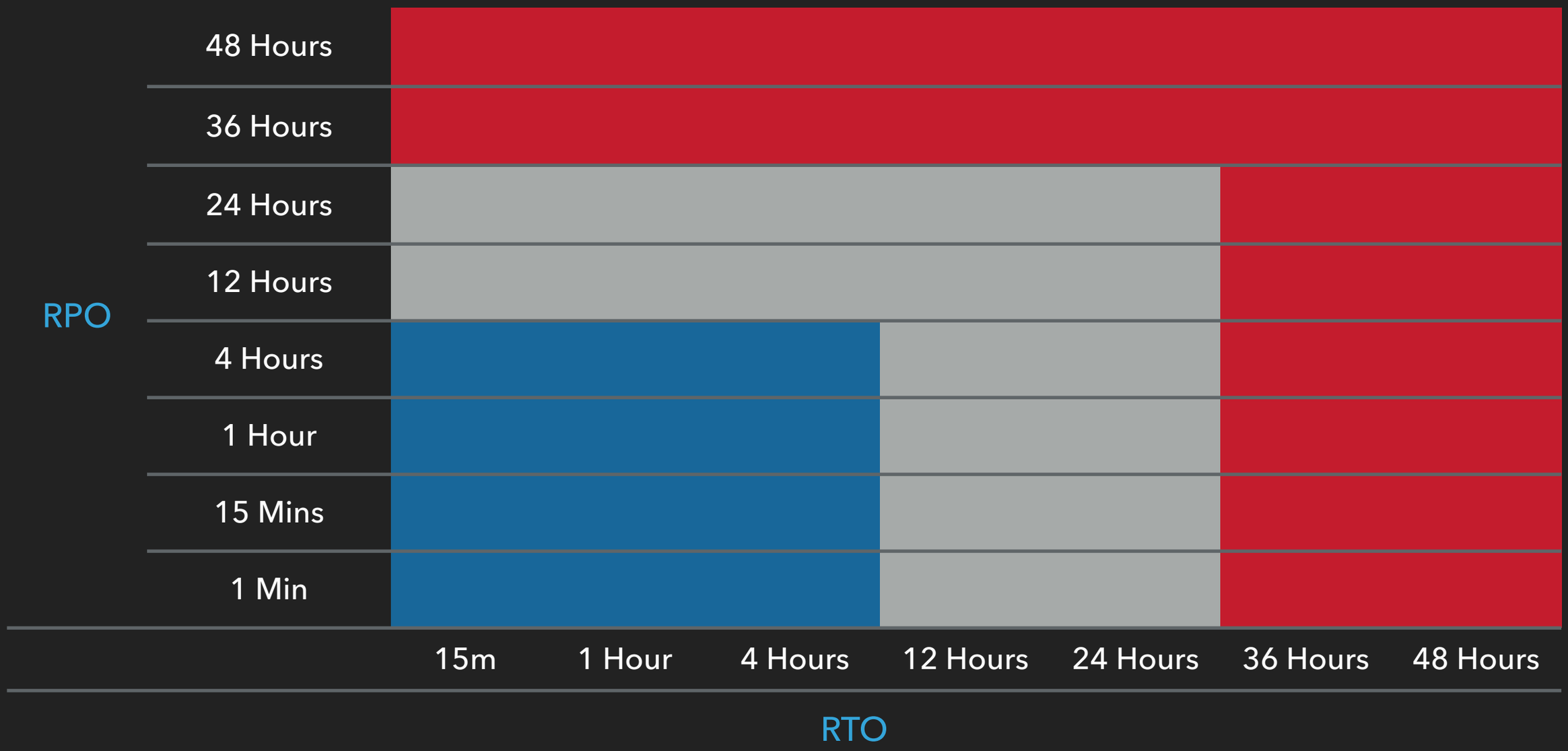
RTO SETTINGS

Recovery Time Objective (RTO) , is the target time set for the recovery of your IT and business activities after a disaster has occurred. The objective is to calculate how quickly you need to recover, which will dictate the type or preparations you need to implement and the overall budget assigned to business continuity.



RPO SETTINGS

Recovery Point Objective (RPO), is focused on data and your loss tolerance in relation to your data. RPO is determined by looking at the time between failover and fallback and the amount of data that could be lost in between.



Q & A SESSION

Vatche Dakessian / CEO