

# The Essentials of SharePoint Disaster Recovery Planning

*@spmcDonough on Twitter  
(for heckling purposes)*



Sean P. McDonough  
Chief Technology Officer  
PAIT Group





About

me

# aka



"How I got SharePoint chocolate  
in my DR peanut butter"

# About *me*

My background with disaster recovery (DR)

- started before I ever touched SharePoint
- began in the financial services & insurance industry

My background with SharePoint

- began in 2004 with SharePoint Portal Server 2003
- I switch between IT Pro and Developer hats

DR and SharePoint

- co-authored two SharePoint DR books
- regularly speak, blog, and "work" on DR topics

# About this talk: why?

Most DR presentations I've seen (and delivered myself) focus on "how to" technical concerns ...

- How to implement backups
- How to establish high-availability

Not enough has been done to discuss the choices and processes that go into DR planning

- aka, the "non-gearhead" stuff



# The prerequisites

This is a 100-level talk, so I don't assume much:

- you don't know much about DR (other than "it's a good idea for my organization")
- you are interested in the end-to-end DR process and more than just strictly technical concerns.

Don't take notes unless you really want to

- <http://SharePointInterface.com>

my blog



In the time we  
have ...





# The Agenda

- Discuss the "big picture"
- Analyze the DR process
- Explore how SharePoint and DR come together



"The Big Picture"



# "The Big Picture"



- many layers

# "The Big Picture"

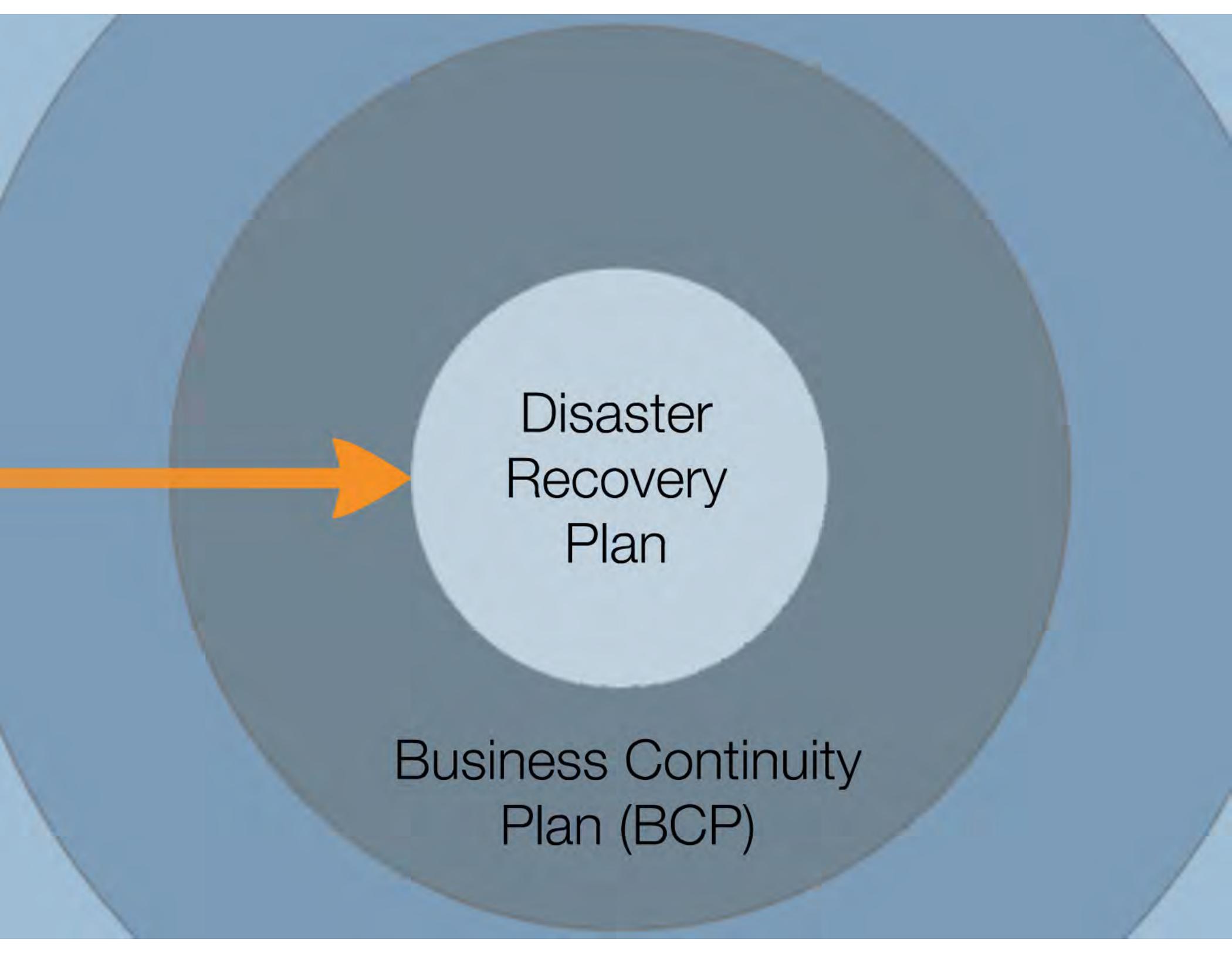


- many layers

- you're probably going to cry as you peel them back

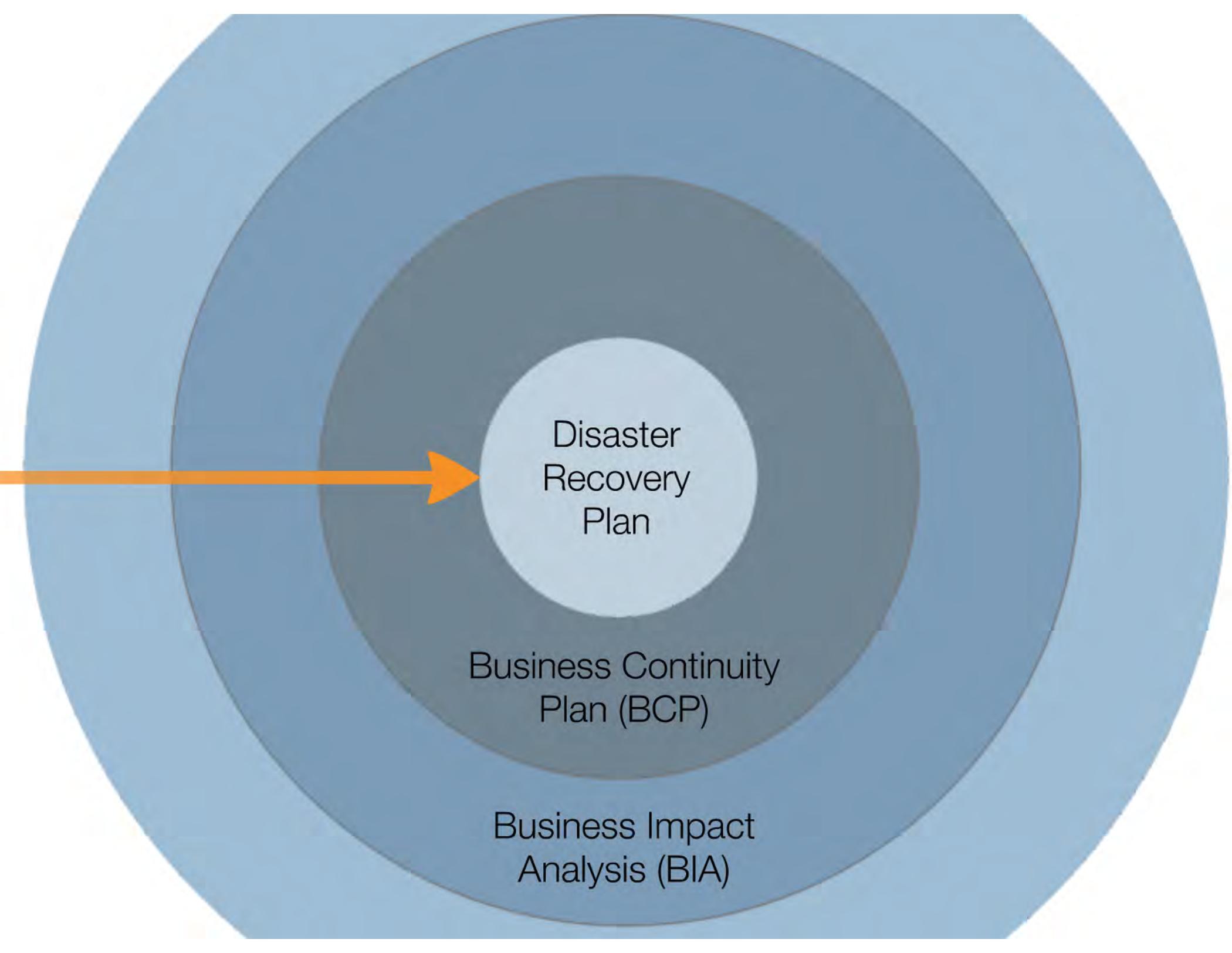


Disaster  
Recovery  
Plan



Disaster  
Recovery  
Plan

Business Continuity  
Plan (BCP)

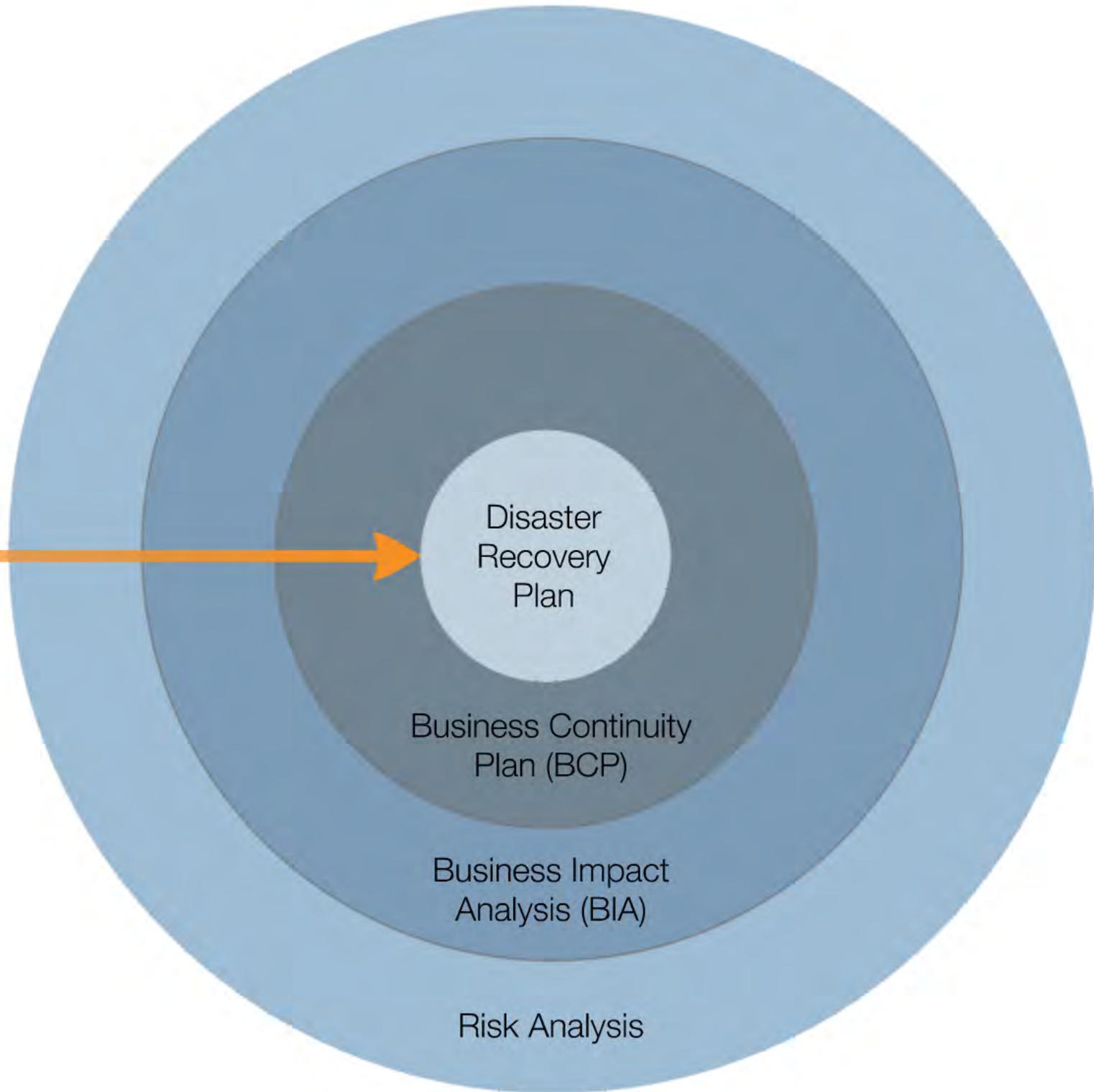


Disaster  
Recovery  
Plan

Business Continuity  
Plan (BCP)

Business Impact  
Analysis (BIA)

START  
HERE

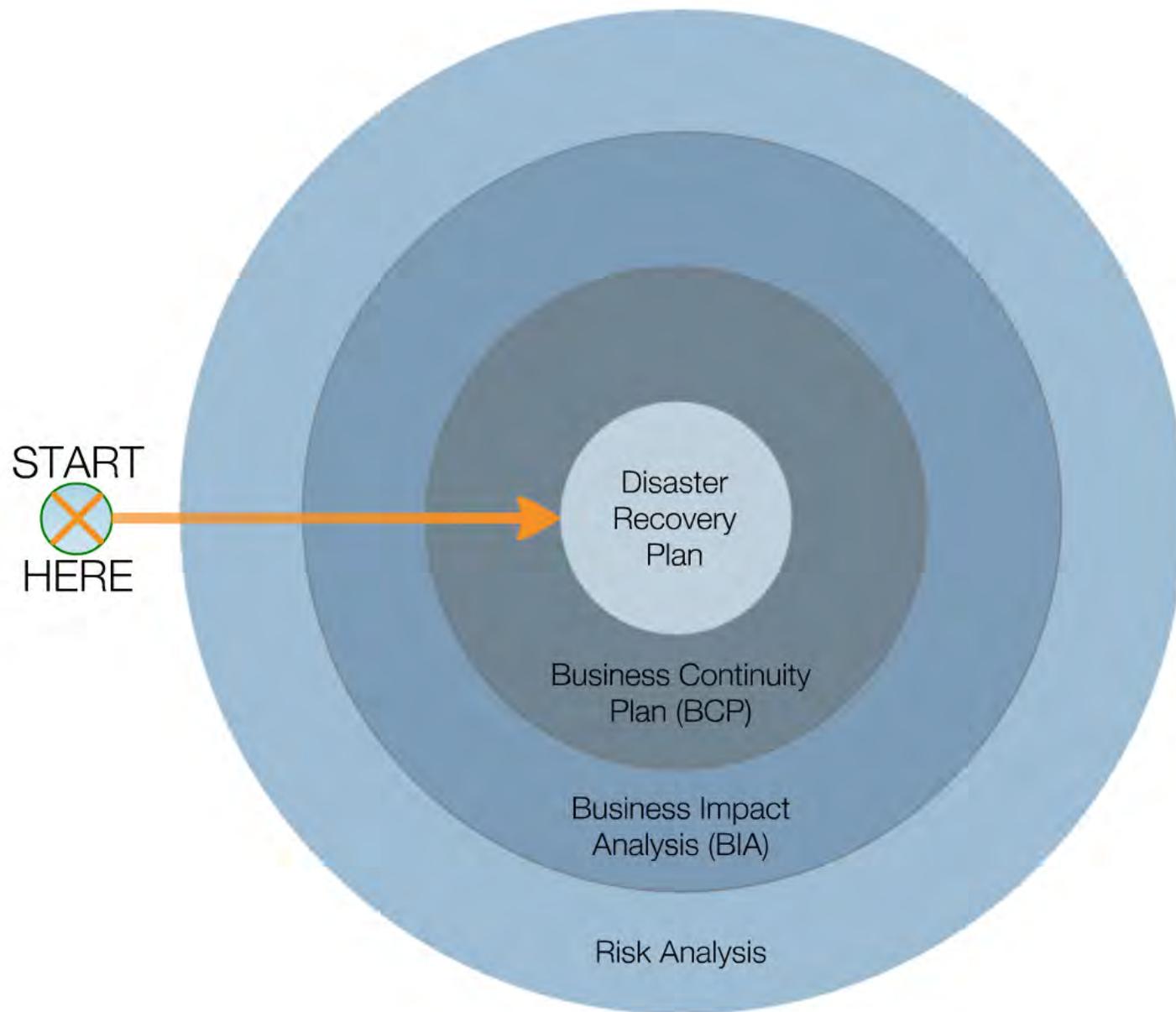


Disaster  
Recovery  
Plan

Business Continuity  
Plan (BCP)

Business Impact  
Analysis (BIA)

Risk Analysis



There's a lot that should happen before you ever get to AN ACTUAL DR plan



## Risk Analysis

### Risk Analysis

Identifies and quantifies the probable threats to normal business operations and activity

#### What could go wrong?

- Primary data center is flooded
- Your network is cyberattacked
- The bulk of employees fall ill
- Power is out in your location (who kicked the cord?)

#### Quantify it

- What is the realistic probability of the event?
- If the event occurs, how severe would the impact be?
- Probability x Severity = Overall Risk



## BIA

### BIA

A business impact analysis maps risks to business processes and systems that would be affected if something were to go wrong

#### What comes out of the BIA?

- A document or matrix that maps individual risks to one or more business processes and systems that would be affected
- An estimate of what each interrupted process or covered system might cost the organization, often times in dollars per hour (\$/hr)
- Prioritization of processes and systems to protect
- Acceptable loss and downtime windows



## BCP

### BCP

A business continuity plan addresses the findings of a BIA and defines processes to mitigate and/or minimize interruptions to normal business operations

#### What does a BCP cover?

- Manual procedures and work arounds to keep business moving in the absence of supporting systems
- Key information and logistical plans to address unavailable facilities, equipment, and personnel
- Communications plans
- Disaster recovery plans



## DR Plan

### DR Plan

Disaster recovery plans document requirements and steps for restoring systems to agreed-upon levels of functionality

#### What can be found in a plan?

- An overview of what the plan addresses and what it doesn't address (quality important?)
- Recovery priorities (hardware, software, facilities, personnel, etc)
- References to dependent information systems/items
- Procedures for recovery
- Measurable success criteria for recovery

# Risk Analysis

Identifies and quantifies the probable threats to normal business operations and activity

## What could go wrong?

- Primary data center is flooded
- Your network is cyberattacked
- The bulk of employees fall ill
- Power is lost to your location (who kicked the cord?)

## Quantify it

- What is the realistic probability of the event?
- If the event occurs, how severe would the impact be?
- Probability x Severity = Overall Risk

# Disaster Recovery Journal

<http://www.drj.com/>

Good online reference for disaster recovery articles, whitepapers, and other resources.

# BIA

A business impact analysis maps risks to business processes and systems that would be affected if something were to go wrong

## What comes out of the BIA?

- A document or matrix that maps individual risks to one or more business processes and systems that would be affected
- An estimate of what each interrupted process or downed system might cost the organization, oftentimes in dollars per hour (\$/hr)
- Prioritization of processes and systems to protect
- Acceptable loss and downtime windows 

e loss and downtime windows ✨



These are a key outputs from this phase of planning and will be used extensively in subsequent phases.

# BCP

A business continuity plan addresses the findings of a BIA and defines processes to mitigate and/or minimize interruptions to normal business operations

## What does a BCP cover?

- Manual procedures and work-arounds to keep business moving in the absence of supporting systems
- Key information and logistical plans to address unavailable facilities, equipment, and personnel
- Communications plans
- Disaster recovery plans

# DR Plan

(Disaster) recovery plans document requirements and steps for restoring systems to agreed-upon levels of functionality

## What can be found in a plan?

- An overview of what the plan addresses and what it doesn't address (equally important!)
- Recovery prerequisites (hardware, software, facilities, personnel, etc)
- References to dependent information/systems/items
- Procedures for recovery
- Measurable success criteria for recovery



## Risk Analysis

### Risk Analysis

Identifies and quantifies the probable threats to normal business operations and activity

#### What could go wrong?

- Primary data center is flooded
- Your network is cyberattacked
- The bulk of employees fall ill
- Power is out in your location (who kicked the cord?)

#### Quantify it

- What is the realistic probability of the event?
- If the event occurs, how severe would the impact be?
- Probability x Severity = Overall Risk



## BIA

### BIA

A business impact analysis maps risks to business processes and systems that would be affected if something were to go wrong

#### What comes out of the BIA?

- A document or matrix that maps individual risks to one or more business processes and systems that would be affected
- An estimate of what each interrupted process or covered system might cost the organization, often times in dollars per hour (\$/hr)
- Prioritization of processes and systems to protect
- Acceptable loss and downtime windows



## BCP

### BCP

A business continuity plan addresses the findings of a BIA and defines processes to mitigate and/or minimize interruptions to normal business operations

#### What does a BCP cover?

- Manual procedures and work arrounds to keep business moving in the absence of supporting systems
- Key information and logistical plans to address unavailable facilities, equipment, and personnel
- Communications plans
- Disaster recovery plans



## DR Plan

### DR Plan

Disaster recovery plans document requirements and steps for restoring systems to agreed-upon levels of functionality

#### What can be found in a plan?

- An overview of what the plan addresses and what it doesn't address (qualify important?)
- Recovery priorities (hardware, software, facilities, personnel, etc)
- References to dependent information systems/items
- Procedures for recovery
- Measurable success criteria for recovery



# Risk Analysis

**Risk Analysis**  
 Identifies and quantifies the probable threats to normal business operations and activity

**What could go wrong?**

- Primary data center is flooded
- Your network is cyber-attacked
- The bulk of employees fall ill
- Power is lost to your location (who locked the cord?)

**Quantify it**

- What is the realistic probability of the event?
- If the event occurs, how severe would the impact be?
- Probability x Severity = Overall Risk



# BIA

**BIA**  
 A business impact analysis maps risks to business processes and systems that would be affected if something were to go wrong

**What comes out of the BIA?**

- A document or matrix that maps individual risks to one or more business processes and systems that would be affected
- An estimate of what each impacted process or system might cost the organization, often times in dollars per hour (\$/hr)
- Prioritization of processes and systems to protect
- Acceptable loss and downtime windows



# BCP

**BCP**  
 A business continuity plan addresses the findings of a BIA and defines processes to initiate and/or minimize interruptions to normal business operations

**What does a BCP cover?**

- Manual procedures and work arounds to keep business moving in the absence of supporting systems
- Key information and logistical plans to address unavailable facilities, equipment, and personnel
- Communications plans
- Disaster recovery plans



# DR Plan

**DR Plan**  
 Disaster recovery plans document requirements and steps for restoring systems to agreed-upon levels of functionality

**What can be found in a plan?**

- An overview of what the plan addresses and what it does (it address (usually in part))
- Recovery prerequisites (hardware, software, facilities, personnel, etc)
- References to dependent information systems/terms
- Procedures for recovery
- Measurable success criteria for recovery

These are a key output from this phase of planning and will be used extensively in subsequent phases.

More abstract



More concrete

More strategic



More tactical

More "business-y"



More technical



# Risk Analysis

**Risk Analysis**  
 Identifies and quantifies the probable threats to normal business operations and activity.

**What could go wrong?**

- Primary data center is flooded
- Your network is cyberhacked
- The bank of employees tell it
- Power is out in your location (aka kicked the cord?)

**Quantify it**

- What is the realistic probability of the event?
- If the event occurs, how severe would the impact be?
- Probability x Severity = Overall Risk



# BIA

**BIA**  
 A business impact analysis maps risks to business processes and systems that would be affected if something were to go wrong.

**What comes out of the BIA?**

- A document or matrix that maps individual risks to one or more business processes and systems that would be affected
- An estimate of what each interrupted process or downed system might cost the organization, often times in dollars per hour (\$/hr)
- Prioritization of processes and systems to protect
- Acceptable loss and downtime windows

↑  
 These are a key output from the phase of planning and will be used extensively in subsequent phases



# BCP

**BCP**  
 A business continuity plan addresses the findings of a BIA and defines processes to mitigate and/or minimize interruptions to normal business operations.

**What does a BCP cover?**

- Mutual procedures and workarounds to keep local loss moving in the absence of supporting systems
- Key information and logistical plans to address unavailable facilities, equipment, and personnel
- Communications plans
- Disaster recovery plans



# DR Plan

**DR Plan**  
 Disaster recovery plans document requirements and steps for restoring systems to agreed upon levels of functionality.

**What can be found in a plan?**

- An overview of what the plan addresses and what it doesn't address (locality in particular)
- Recovery procedures (hardware, software, facilities, personnel, etc.)
- References to dependent information systems (links)
- Procedures for recovery
- Measurable success criteria for recovery

More abstract



More concrete

More strategic



More tactical

More "business-y"



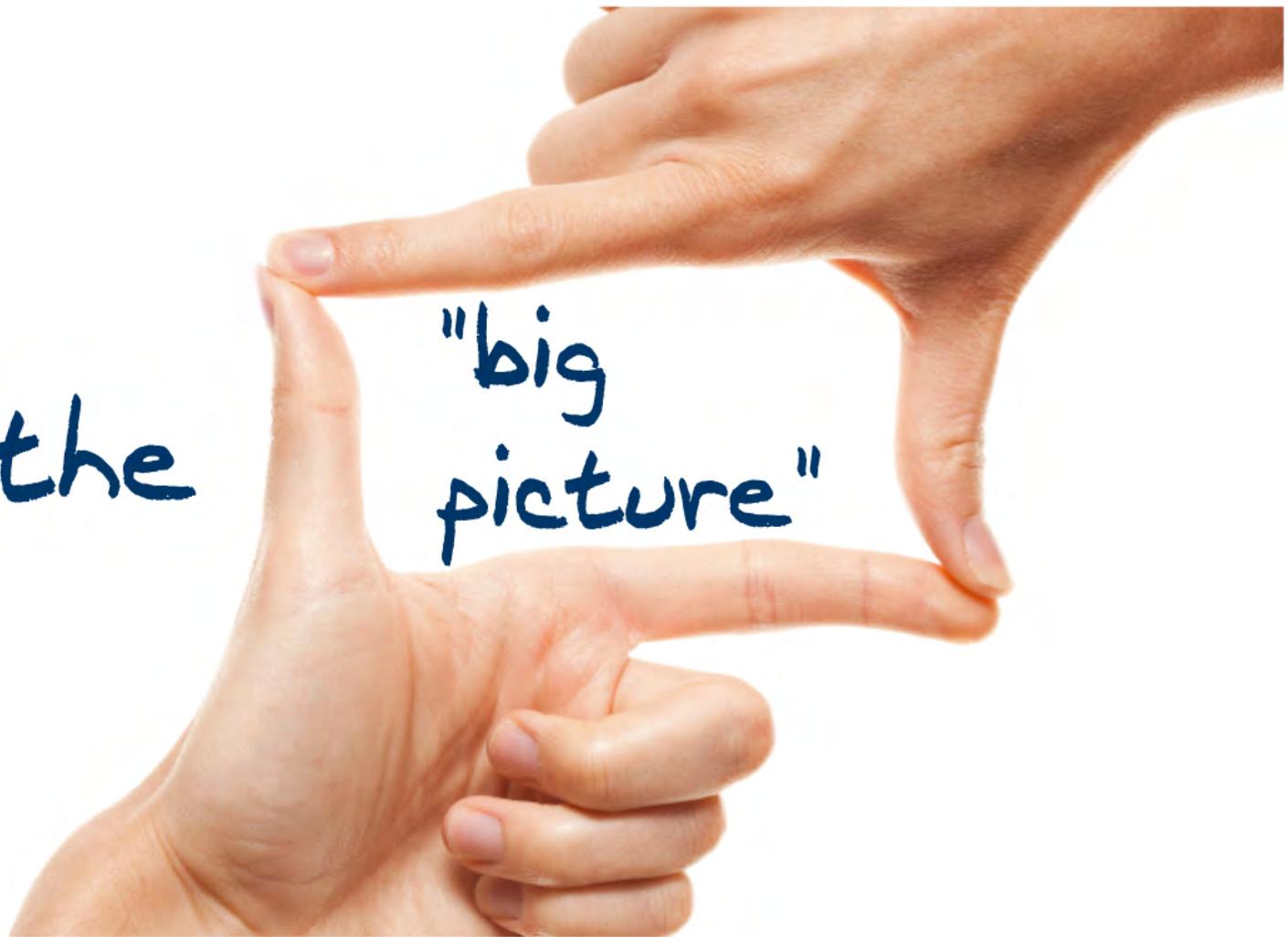
More technical

## Disclaimer

There are many approaches to quantifying disaster risks and building contingency plans; I'm presenting only one. Form isn't nearly as important as simply ensuring you have a strategy!

that was the

"big  
picture"



The focus going forward  
is on ...

the DR



Process

The focus going forward  
is on ...

the DR  Process

... which is driven by  
RPO and RTO  
requirements

This is a good point to define those acronyms

RPO

RTO

This is a good point to define those acronyms

# RPO



Recovery  
Point  
Objective

# RTO



Recovery  
Time  
Objective

# RPO



Recovery  
Point  
Objective

# RTO



Recovery  
Time  
Objective

*That's all great, but what do they really MEAN?*

They define operational windows that guide and inform your selection of technologies and strategies for recovery

RPPO



# RPO (Recovery Point Objective)

Monday Jul 4 2011

1:00 AM 2:00 AM 3:00 AM 4:00 AM 5:00 AM 6:00 AM 7:00 AM 8:00 AM 9:00 AM 10:00 AM 11:00 AM 12:00 PM 1:00 PM 2:00 PM 3:00 PM 4:00 PM 5:00 PM 6:00 PM 7:00 PM 8:00 PM 9:00 PM 10:00 PM

- "looks backwards"
- defines maximum acceptable data loss

Monday Jul 4 2011

AM 9:00 AM 10:00 AM 11:00 AM 12:00 PM 1:00 PM 2:00 PM 3:00

wards"

mium accenta

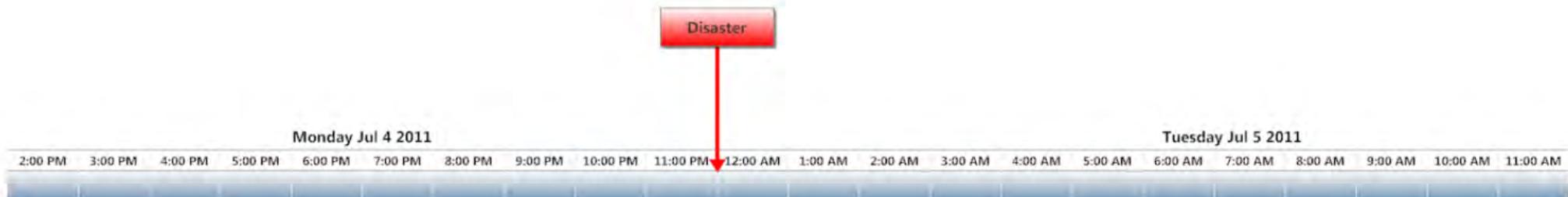




Your data center just  
took a mortar ...

RPO

# RPO (Recovery Point Objective)





Disaster

Monday Jul 4 2011

6:00 PM

7:00 PM

8:00 PM

9:00 PM

10:00 PM

11:00 PM

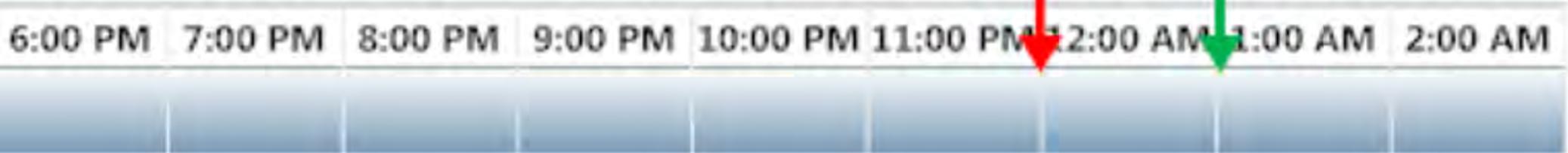
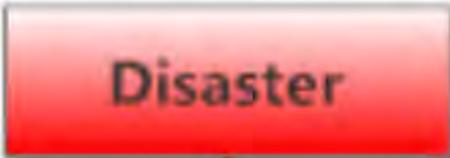
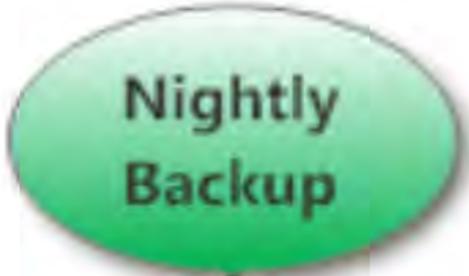
12:00 AM

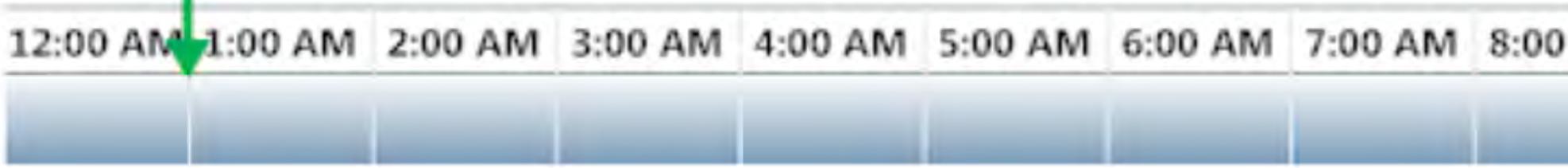
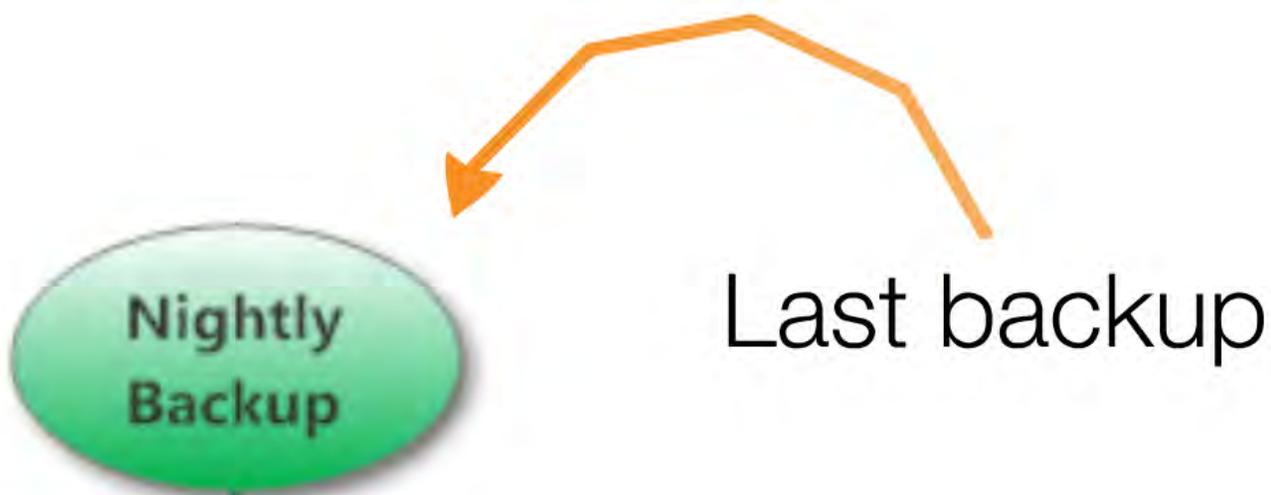
1:00 AM

# RPO (Recovery Point Objective)

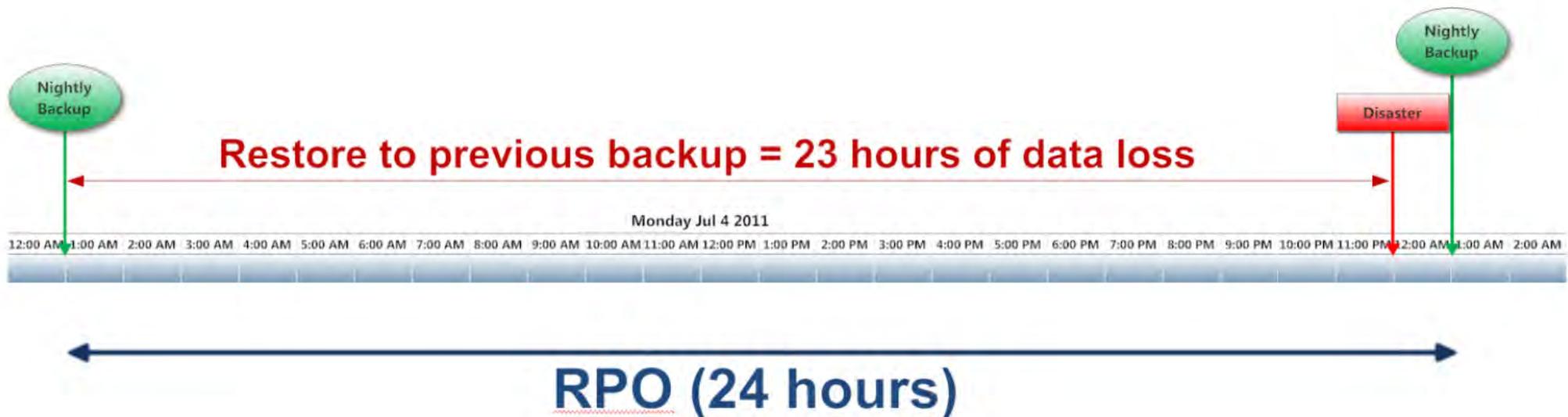


Next scheduled backup





# RPO (Recovery Point Objective)



# RTTO



# RTO (Recovery Time Objective)



- "looks forward"
- defines how much time you have to get things working again

# RTO (Recovery Time Objective)



← RTO (8 hours) →

# RTO (Recovery Time Objective)



← RTO (8 hours) →

The focus going forward  
is on ...

the DR  Process

... which is driven by  
RPO and RTO  
requirements

The focus going forward  
is on ...

the DR  Process

... which is driven by  
RPO and RTO  
requirements

Please allow me a  
moment to preach ...





Risk analysis

BIA

*RPO and RTO are determined up here*

BCP



DR Plan

*Implementation takes place down here*



Risk analysis

Business

BIA

*RPO and RTO are determined up here*

BCP



DR Plan

*Implementation takes place down here*

Technical

*If you're trying to build a DR Plan without business input, you're doing it wrong.*



Risk analysis

Business

BIA

*RPO and RTO are determined up here*

BCP



*Implementation takes place down here*

DR Plan



Technical

*If you're trying to build a DR Plan without business input, you're doing it wrong.*

*Kind of like ...*

Kind of like ...

DR Plan



Kind of like ...

DR Plan



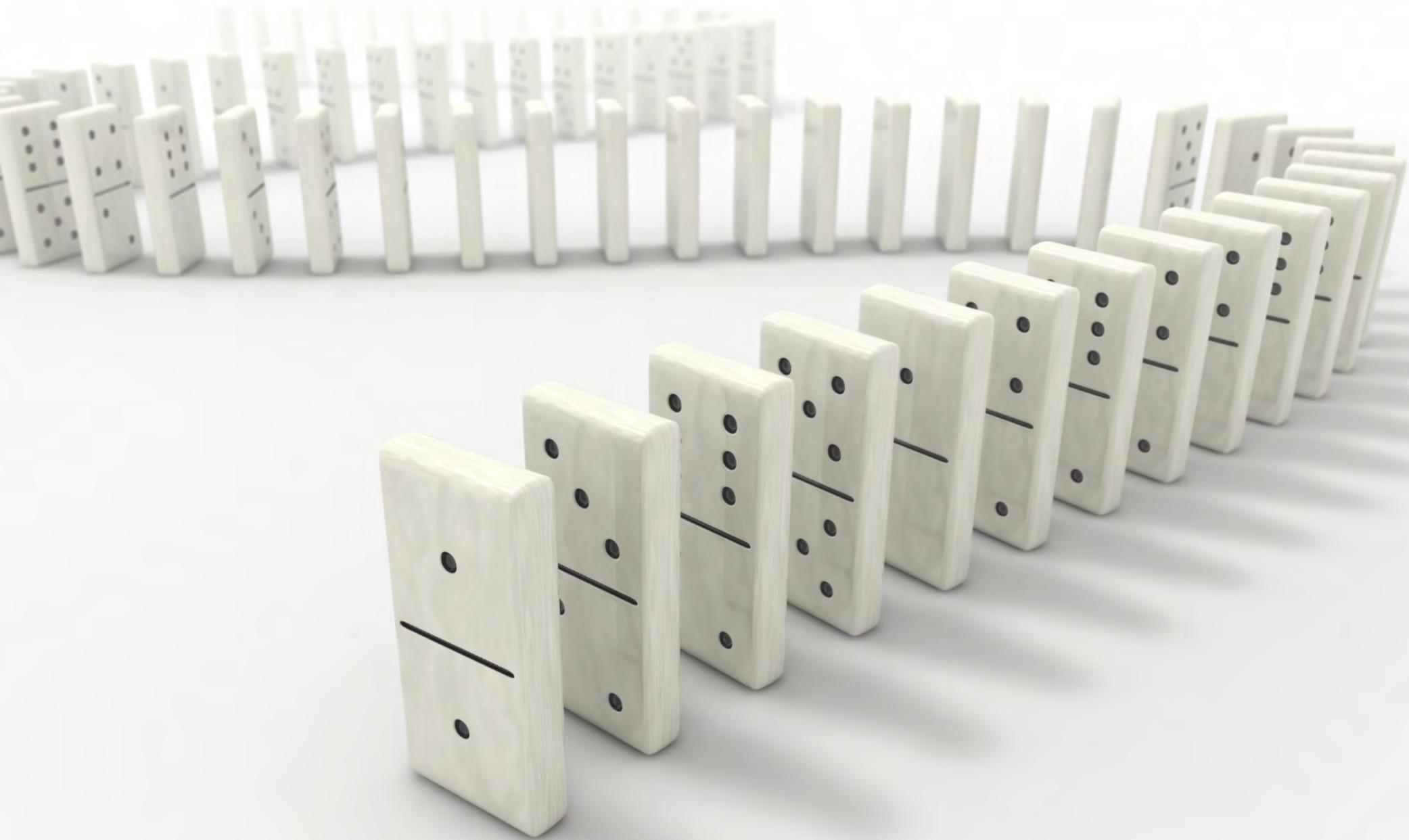
Business  
Continuity  
Strategy



If I haven't beat the horse  
to death enough for you ...



<http://sharepointinterface.com/2009/07/08/rpo-and-rto-prerequisites-for-informed-sharepoint-disaster-recovery-planning/>



The DR Process



**Assessment**



**Planning**



**Maintenance**



**Implementation**

The DR Process





# Assessment

# Assessment

Building an understanding of

- The SharePoint platform itself
- Your SharePoint environment as it exists today

# Assessment

Building an understanding of

- The SharePoint platform itself
- Your SharePoint environment as it exists today

Accomplished through two "D" words

# Assessment

Building an understanding of

- The SharePoint platform itself
- Your SharePoint environment as it exists today

Accomplished through two "D" words

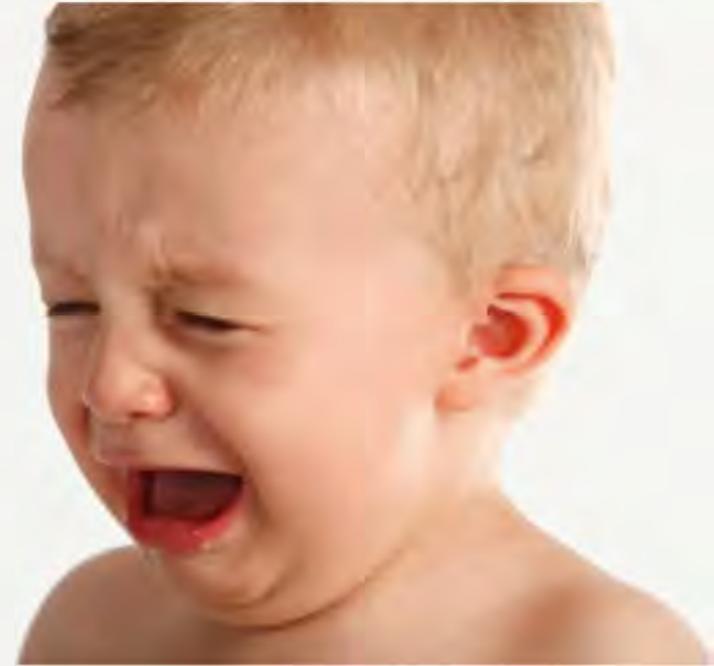
## Discovery

# Discovery

- Logical architecture
- Physical deployment
- Configuration data
- Business data (content)
- Dependencies and interfaces

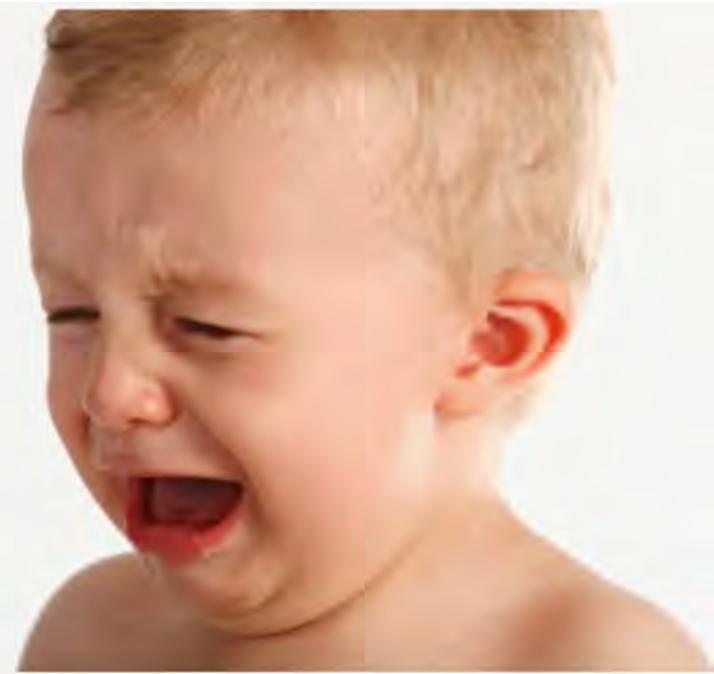
Before we go too far, we should probably talk about the other "D" word

Before we go too far, we should probably talk about the other "D" word



You're going to have to document your discoveries and SharePoint itself

Before we go too far, we should probably talk about the other "D" word



You're going to have to document your discoveries and SharePoint itself

Believe it or not, there are tools that can help.



# Logical Architecture

- Focuses on the SharePoint's software/service components, what they do, and how they relate to one another
- Particular attention is placed on platform elements you use

## Commonly documented

- IIS application pools
- SharePoint Web applications
- Service applications (Search, BCS, Managed Metadata, etc.)
- Zones and alternate access mappings
- Web application policies
- Content databases
- Site collections
- My Sites

# Commonly documented

- IIS application pools
- SharePoint Web applications
- Service applications (Search, BCS, Managed Metadata, etc.)
- Zones and alternate access mappings
- Web application policies
- Content databases
- Site collections
- My Sites

Goal: show which pieces of SharePoint are in-use, how they interrelate, and how they work together

Think "birds-eye" view of logical farm components - not physical layout/usage

# Physical Architecture

- Focuses on SharePoint's implementation across a set of infrastructure components and hardware

## Commonly documented

- Physical servers used by SharePoint
- SQL Servers
- Storage area networks (SANs)
- Switches
- Wide area network (WAN) connections
- Firewalls
- Hardware load balancers
- Active Directory domain controllers
- Email relays and gateways

The modern monkeywrench that makes all of this more complicated:



# Virtualization



**Logical Architecture**



**Physical Architecture**

- 33% of small and mid-size businesses (SMBs) admitted that they do not back up virtual servers as often as physical servers
- 49% back up virtual machines weekly or monthly
- 37% back up virtual machines each day

Source: Acronis Global Disaster Recovery Index 2012  
[http://acronisinfo.com/?attachment\\_id=521](http://acronisinfo.com/?attachment_id=521)

The modern monkeywrench that makes all of this more complicated:



# Virtualization



**Logical Architecture**



**Physical Architecture**

# Configuration Data

- Focuses on the data and settings that make SharePoint and its constituent components/pieces operate.

## Commonly includes

- Farm configuration database
- Non-content service application databases
- Web.config files
- IIS7 configuration files
- Other configuration stores tied to logical architecture items

# Configuration Data

- Focuses on the data and settings that make SharePoint and its constituent components/pieces operate.

## Commonly includes

- Farm configuration database
- Non-content service application databases
- Web.config files
- IIS7 configuration files
- Other configuration stores tied to logical architecture items

Initially, it is more important to understand where data resides and the form it takes than to document actual settings

# Commonly includes

- Farm configuration database
- Non-content service application databases
- Web.config files
- IIS7 configuration files
- Other configuration stores tied to logical architecture items

Initially, it is more important to understand where data resides and the form it takes than to document actual settings

Pay close attention to secure configuration data, configuration data that is stored in a tough-to-reach manner, and distributed configuration

# Business Data

- This is data that gets created and exists within SharePoint as a result of day-to-day business

If you remember nothing else,  
remember this:

Content  
databases

=



as in "most important business  
data locations to protect"

# Dependencies & interfaces

- These are the points where SharePoint touches other line of business systems - including other SharePoint farms.

# Dependencies & interfaces

- These are the points where SharePoint touches other line of business systems - including other SharePoint farms.

## Some examples

- HR Data consumed through an external list using BCS
- Search that is supplied through a separate services-only SharePoint farm
- A Page Viewer web part that exposes a non-SharePoint Web application using an iframe
- InfoPath forms that pull data from (or write data to) non-SharePoint systems

# Some examples

- HR Data consumed through an external list using BCS
- Search that is supplied through a separate services-only SharePoint farm
- A Page Viewer web part that exposes a non-SharePoint Web application using an iframe
- InfoPath forms that pull data from (or write data to) non-SharePoint systems

These are important to identify for purposes of determining what is ultimately included in (and excluded from) your SharePoint DR plan

# Documentation tools



# Creating SharePoint diagrams

Technical diagrams for SharePoint 2013

[https://technet.microsoft.com/en-us/library/cc263199\(v=office.15\).aspx](https://technet.microsoft.com/en-us/library/cc263199(v=office.15).aspx)

Visio stencils for IT Pro posters

<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=11616>

# PowerShell farm documentation

Document farm configuration settings (SharePoint Foundation 2013)

[https://technet.microsoft.com/en-us/library/ff645391\(v=office.15\).aspx](https://technet.microsoft.com/en-us/library/ff645391(v=office.15).aspx)

Document farm configuration settings in SharePoint 2013

[https://technet.microsoft.com/en-us/library/ff645391\(v=office.15\).aspx](https://technet.microsoft.com/en-us/library/ff645391(v=office.15).aspx)

# Documentation Toolkit for SharePoint

<http://www.spdockit.com/>

*note: not free*



**Assessment**



**Planning**



**Maintenance**



**Implementation**

The DR Process





# Planning



### Planning

RTO  
RPO  
Recovery Plan

#### Scope and Breadth

**Common Questions**  
- What systems are critical?  
- What data is critical?  
- How long will it take to recover?  
- How much data can we afford to lose?



What, there is a little more to it than just that

#### Recovery Targets

**Recovery Point Objective (RPO)**  
- How much data can we afford to lose?  
**Recovery Time Objective (RTO)**  
- How long will it take to recover?

#### Custom approach

- Backup and restore  
- High availability (HA)  
- Your data will only be available if you have high availability (HA)

- Disaster Response

What is the appropriate combination of strategies and technologies to address your recovery targets?

#### Disaster Response

Recovery Point Objective (RPO)	Recovery Time Objective (RTO)
1 hour	4 hours
4 hours	8 hours
8 hours	16 hours
16 hours	32 hours
32 hours	64 hours
64 hours	128 hours
128 hours	256 hours
256 hours	512 hours
512 hours	1024 hours
1024 hours	2048 hours
2048 hours	4096 hours
4096 hours	8192 hours
8192 hours	16384 hours
16384 hours	32768 hours
32768 hours	65536 hours
65536 hours	131072 hours
131072 hours	262144 hours
262144 hours	524288 hours
524288 hours	1048576 hours
1048576 hours	2097152 hours
2097152 hours	4194304 hours
4194304 hours	8388608 hours
8388608 hours	16777216 hours
16777216 hours	33554432 hours
33554432 hours	67108864 hours
67108864 hours	134217728 hours
134217728 hours	268435456 hours
268435456 hours	536870912 hours
536870912 hours	1073741824 hours
1073741824 hours	2147483648 hours
2147483648 hours	4294967296 hours
4294967296 hours	8589934592 hours
8589934592 hours	17179869184 hours
17179869184 hours	34359738368 hours
34359738368 hours	68719476736 hours
68719476736 hours	137438953472 hours
137438953472 hours	274877906944 hours
274877906944 hours	549755813888 hours
549755813888 hours	1099511627776 hours
1099511627776 hours	2199023255552 hours
2199023255552 hours	4398046511104 hours
4398046511104 hours	8796093022208 hours
8796093022208 hours	17592186044416 hours
17592186044416 hours	35184372088832 hours
35184372088832 hours	70368744177664 hours
70368744177664 hours	140737488355328 hours
140737488355328 hours	281474976710656 hours
281474976710656 hours	562949953421312 hours
562949953421312 hours	1125899906842624 hours
1125899906842624 hours	2251799813685248 hours
2251799813685248 hours	4503599627370496 hours
4503599627370496 hours	9007199254740992 hours
9007199254740992 hours	18014398509481984 hours
18014398509481984 hours	36028797018963968 hours
36028797018963968 hours	72057594037927936 hours
72057594037927936 hours	144115188075855872 hours
144115188075855872 hours	288230376151711744 hours
288230376151711744 hours	576460752303423488 hours
576460752303423488 hours	1152921504606846976 hours
1152921504606846976 hours	2305843009213693952 hours
2305843009213693952 hours	4611686018427387904 hours
4611686018427387904 hours	9223372036854775808 hours
9223372036854775808 hours	18446744073709551616 hours
18446744073709551616 hours	36893488147419103232 hours
36893488147419103232 hours	73786976294838206464 hours
73786976294838206464 hours	147573952589676412928 hours
147573952589676412928 hours	295147905179352825856 hours
295147905179352825856 hours	590295810358705651712 hours
590295810358705651712 hours	1180591620717411303424 hours
1180591620717411303424 hours	2361183241434822606848 hours
2361183241434822606848 hours	4722366482869645213696 hours
4722366482869645213696 hours	9444732965739290427392 hours
9444732965739290427392 hours	18889465931478580854784 hours
18889465931478580854784 hours	37778931862957161709568 hours
37778931862957161709568 hours	75557863725914323419136 hours
75557863725914323419136 hours	151115727451828646838272 hours
151115727451828646838272 hours	302231454903657293676544 hours
302231454903657293676544 hours	604462909807314587353088 hours
604462909807314587353088 hours	1208925819614629174706176 hours
1208925819614629174706176 hours	2417851639229258349412352 hours
2417851639229258349412352 hours	4835703278458516698824704 hours
4835703278458516698824704 hours	9671406556917033397649408 hours
9671406556917033397649408 hours	19342813113834066795298816 hours
19342813113834066795298816 hours	38685626227668133590597632 hours
38685626227668133590597632 hours	77371252455336267181195264 hours
77371252455336267181195264 hours	154742504910672534362390528 hours
154742504910672534362390528 hours	309485009821345068724781056 hours
309485009821345068724781056 hours	618970019642690137449562112 hours
618970019642690137449562112 hours	1237940039285380274899124224 hours
1237940039285380274899124224 hours	2475880078570760549798248448 hours
2475880078570760549798248448 hours	4951760157141521099596496896 hours
4951760157141521099596496896 hours	9903520314283042199192993792 hours
9903520314283042199192993792 hours	19807040628566084398385987584 hours
19807040628566084398385987584 hours	39614081257132168796771975168 hours
39614081257132168796771975168 hours	79228162514264337593543950336 hours
79228162514264337593543950336 hours	158456325028528675187087900672 hours
158456325028528675187087900672 hours	316912650057057350374175801344 hours
316912650057057350374175801344 hours	633825300114114700748351602688 hours
633825300114114700748351602688 hours	1267650600228229401496703205376 hours
1267650600228229401496703205376 hours	2535301200456458802993406410752 hours
2535301200456458802993406410752 hours	5070602400912917605986812821504 hours
5070602400912917605986812821504 hours	10141204801825835211973625643008 hours
10141204801825835211973625643008 hours	20282409603651670423947251286016 hours
20282409603651670423947251286016 hours	40564819207303340847894502572032 hours
40564819207303340847894502572032 hours	81129638414606681695789005144064 hours
81129638414606681695789005144064 hours	162259276829213363391578010288128 hours
162259276829213363391578010288128 hours	324518553658426726783156020576256 hours
324518553658426726783156020576256 hours	649037107316853453566312041152512 hours
649037107316853453566312041152512 hours	1298074214633706907132624082305024 hours
1298074214633706907132624082305024 hours	2596148429267413814265248164610048 hours
2596148429267413814265248164610048 hours	5192296858534827628530496329220096 hours
5192296858534827628530496329220096 hours	10384593717069655257060992658440192 hours
10384593717069655257060992658440192 hours	20769187434139310514121985316880384 hours
20769187434139310514121985316880384 hours	41538374868278621028243970633760768 hours
41538374868278621028243970633760768 hours	83076749736557242056487941267521536 hours
83076749736557242056487941267521536 hours	166153499473114484112975882535043072 hours
166153499473114484112975882535043072 hours	332306998946228968225951765070086144 hours
332306998946228968225951765070086144 hours	664613997892457936451903530140172288 hours
664613997892457936451903530140172288 hours	1329227995784915872903807060280344576 hours
1329227995784915872903807060280344576 hours	2658455991569831745807614120560689152 hours
2658455991569831745807614120560689152 hours	5316911983139663491615228241121378304 hours
5316911983139663491615228241121378304 hours	10633823966279326983230456482242756608 hours
10633823966279326983230456482242756608 hours	21267647932558653966460912964485513216 hours
21267647932558653966460912964485513216 hours	42535295865117307932921825928971026432 hours
42535295865117307932921825928971026432 hours	85070591730234615865843651857942052864 hours
85070591730234615865843651857942052864 hours	170141183460469231731687303715884105728 hours
170141183460469231731687303715884105728 hours	340282366920938463463374607431768211456 hours
340282366920938463463374607431768211456 hours	680564733841876926926749214863536422912 hours
680564733841876926926749214863536422912 hours	1361129467683753853853498429727072845824 hours
1361129467683753853853498429727072845824 hours	2722258935367507707706996859454145691648 hours
2722258935367507707706996859454145691648 hours	5444517870735015415413993718908291383296 hours
5444517870735015415413993718908291383296 hours	10889035741470030830827987437816582766592 hours
10889035741470030830827987437816582766592 hours	21778071482940061661655974875633165533184 hours
21778071482940061661655974875633165533184 hours	43556142965880123323311949751266331066368 hours
43556142965880123323311949751266331066368 hours	87112285931760246646623899502532662132736 hours
87112285931760246646623899502532662132736 hours	174224571863520493293247799005065244265472 hours
174224571863520493293247799005065244265472 hours	348449143727040986586495598010130488530944 hours
348449143727040986586495598010130488530944 hours	696898287454081973172991196020260977061888 hours
696898287454081973172991196020260977061888 hours	1393796574908163946345982392040521954123776 hours
1393796574908163946345982392040521954123776 hours	2787593149816327892691964784081043908247552 hours
2787593149816327892691964784081043908247552 hours	5575186299632655785383929568162087816495104 hours
5575186299632655785383929568162087816495104 hours	11150372599265311570767859136324173632990208 hours
11150372599265311570767859136324173632990208 hours	22300745198530623141535718272648347265980416 hours
22300745198530623141535718272648347265980416 hours	44601490397061246283071436545296694531960832 hours
44601490397061246283071436545296694531960832 hours	89202980794122492566142873090593389063921664 hours
89202980794122492566142873090593389063921664 hours	178405961588244985132285746181186778127843328 hours
178405961588244985132285746181186778127843328 hours	356811923176489970264571492362373556255686656 hours
356811923176489970264571492362373556255686656 hours	713623846352979940529142984724747112511373312 hours
713623846352979940529142984724747112511373312 hours	1427247692705959881058285969449494225022746624 hours
1427247692705959881058285969449494225022746624 hours	2854495385411919762116571938898988450045493248 hours
2854495385411919762116571938898988450045493248 hours	5708990770823839524233143877797976900090986496 hours
5708990770823839524233143877797976900090986496 hours	11417981541647679048466287755595953800181972992 hours
11417981541647679048466287755595953800181972992 hours	22835963083295358096932575511191907600363945984 hours
22835963083295358096932575511191907600363945984 hours	45671926166590716193865151022383815200727891968 hours
45671926166590716193865151022383815200727891968 hours	91343852333181432387730302044767630401455783936 hours
91343852333181432387730302044767630401455783936 hours	182687704666362864775460604089535260802911567872 hours
182687704666362864775460604089535260802911567872 hours	365375409332725729550921208179070521605823135744 hours
365375409332725729550921208179070521605823135744 hours	730750818665451459101842416358141043211646271488 hours
730750818665451459101842416358141043211646271488 hours	1461501637330902918203684832716282086423292542976 hours
1461501637330902918203684832716282086423292542976 hours	2923003274661805836407369665432564172846585085952 hours
2923003274661805836407369665432564172846585085952 hours	5846006549323611672814739330865128345693171171904 hours
58460065493236116728147393308651283	

Planning

# Assessment Results



# Plannning

Assessment Results



+

RTO

RPO

# Planning

Assessment Results



$$+ \begin{matrix} \text{RTO} \\ \text{RPO} \end{matrix} =$$

# Recovery Plan



Well, there is a little more to it than just that

- Define scope and granularity
- Define recovery targets
- Define approach (technology)

# Scope and Granularity

# Scope and Granularity

## Common Questions

- Do you treat your SharePoint farm as one big system or as multiple functional pieces?
- What's not in-scope for your plan? Are one or more separate (but dependent systems) included?
- How do you handle regional disasters such as earthquake, flood, or attack? The choice carries data center implications\*
- Can you (or do you even want to) leverage the cloud?\*

- 23% of all businesses don't have an offsite backup strategy in place today
- 42% rely on onsite backups to tape or disk and then take those (physically) offsite each day

Source: Acronis Global Disaster Recovery Index 2012  
[http://acronisinfo.com/?attachment\\_id=521](http://acronisinfo.com/?attachment_id=521)

# Scope and Granularity

## Common Questions

- Do you treat your SharePoint farm as one big system or as multiple functional pieces?
- What's not in-scope for your plan? Are one or more separate (but dependent systems) included?
- How do you handle regional disasters such as earthquake, flood, or attack? The choice carries data center implications\*
- Can you (or do you even want to) leverage the cloud?\*

# Cloud computing



- Is not a DR "magic bullet"
- Simplifies some aspects of DR (availability) but complicates others (RPO/RTO, security)
- Comes in many different shapes, forms, and hybrids (Office 365, ITaS, private cloud, etc.)

Figure out if the cloud will be part of your DR strategy early on!

# Scope and Granularity

## Common Questions

- Do you treat your SharePoint farm as one big system or as multiple functional pieces?
- What's not in-scope for your plan? Are one or more separate (but dependent systems) included?
- How do you handle regional disasters such as earthquake, flood, or attack? The choice carries data center implications\*
- Can you (or do you even want to) leverage the cloud?\*

# Scope and Granularity

## Common Questions

- Do you treat your SharePoint farm as one big system or as multiple functional pieces?
- What's not in-scope for your plan? Are one or more separate (but dependent systems) included?
- How do you handle regional disasters such as earthquake, flood, or attack? The choice carries data center implications\*
- Can you (or do you even want to) leverage the cloud?\*

Answers to these questions help determine how you ultimately define ...

Answers to these questions help determine how you ultimately define ...

# Recovery Targets

# Recovery Targets

- Specify what to restore in SharePoint through mapping of business processes to SharePoint functional area
- Prioritized from most critical to least critical (RPO, RTO, \$\$\$)

# Recovery Targets

- Specify what to restore in SharePoint through mapping of business processes to SharePoint functional area
- Prioritized from most critical to least critical (RPO, RTO, \$\$\$)

## Simple example

"I need to restore the HR intranet"

May entail building and/or restoring:

- A SharePoint farm (baseline environment)
- Content database housing the HR site collection
- BCS and associated connections to external line-of-business systems housing HR data
- Secure Store service for required BCS credential sets
- InfoPath Services for HR-related forms

These are all  
recovery targets



- A S
- Conte
- BCS an
- business s
- Secure
- Infop



## Define Approach

What is the appropriate combination of strategies and technologies to address your recovery targets?

# Common approaches with MANY VARIATIONS

- Backup and restore
- High availability (HA)



Your choice will likely be guided by a few key considerations:

- RPO
- RTO
- Resources (Cost)

# Factors when selecting

Backup & Restore

High Availability

RPO

Typically hours

From minutes  
down to zero

RTO

Typically hours

From minutes  
down to zero

Resources

Less expensive

Significantly  
more expensive

Examples

SharePoint native backups  
SQL Server backups  
Enterprise backup systems  
3rd party SharePoint backups

Windows clustering  
Replication products  
SQL Server AlwaysOn  
Transaction log shipping

# Factors when selecting

	Backup & Restore	High Availability
RPO	Typically hours	From minutes down to zero
RTO	Typically hours	From minutes down to zero
Resources	Less expensive	Significantly more expensive
Examples	SharePoint native backups SQL Server backups Enterprise backup systems 3rd party SharePoint backups	Windows clustering Replication products SQL Server AlwaysOn Transaction log shipping



VIRTUALIZATION



Cloud



What should you protect?



# What should you protect?

Technical (recovery) targets you select depend on your strategy, but most plans include the following critical (technical) items at a minimum:

## Databases

- Content ✨
- Service Apps

## Solution packages (WSPs)

## Documentation

- Farm configuration
- Server configuration
- Accounts & permissions

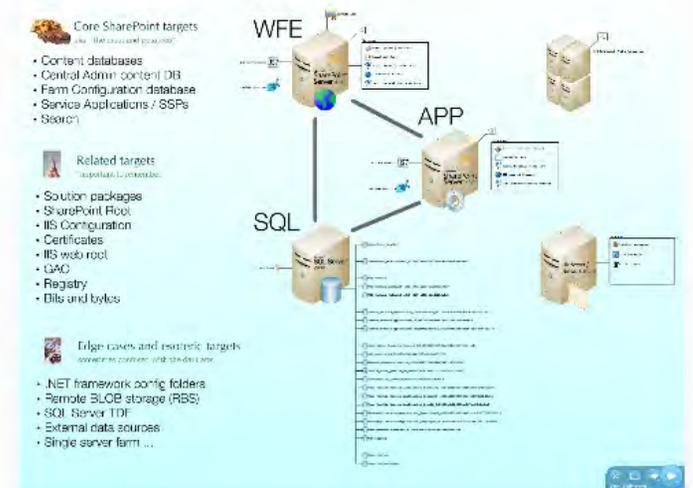


# ? FREQUENTLY ASKED QUESTION

How do I get a list of  
everything I should protect?

# Answer:

There is no definitive "list of everything." No two Sharepoint farms (or DR plans) are the same.





## Core SharePoint targets

aka, "the meat and potatoes"

- Content databases
- Central Admin content DB
- Farm Configuration database
- Service Applications / SSPs
- Search



## Related targets

"important to remember"

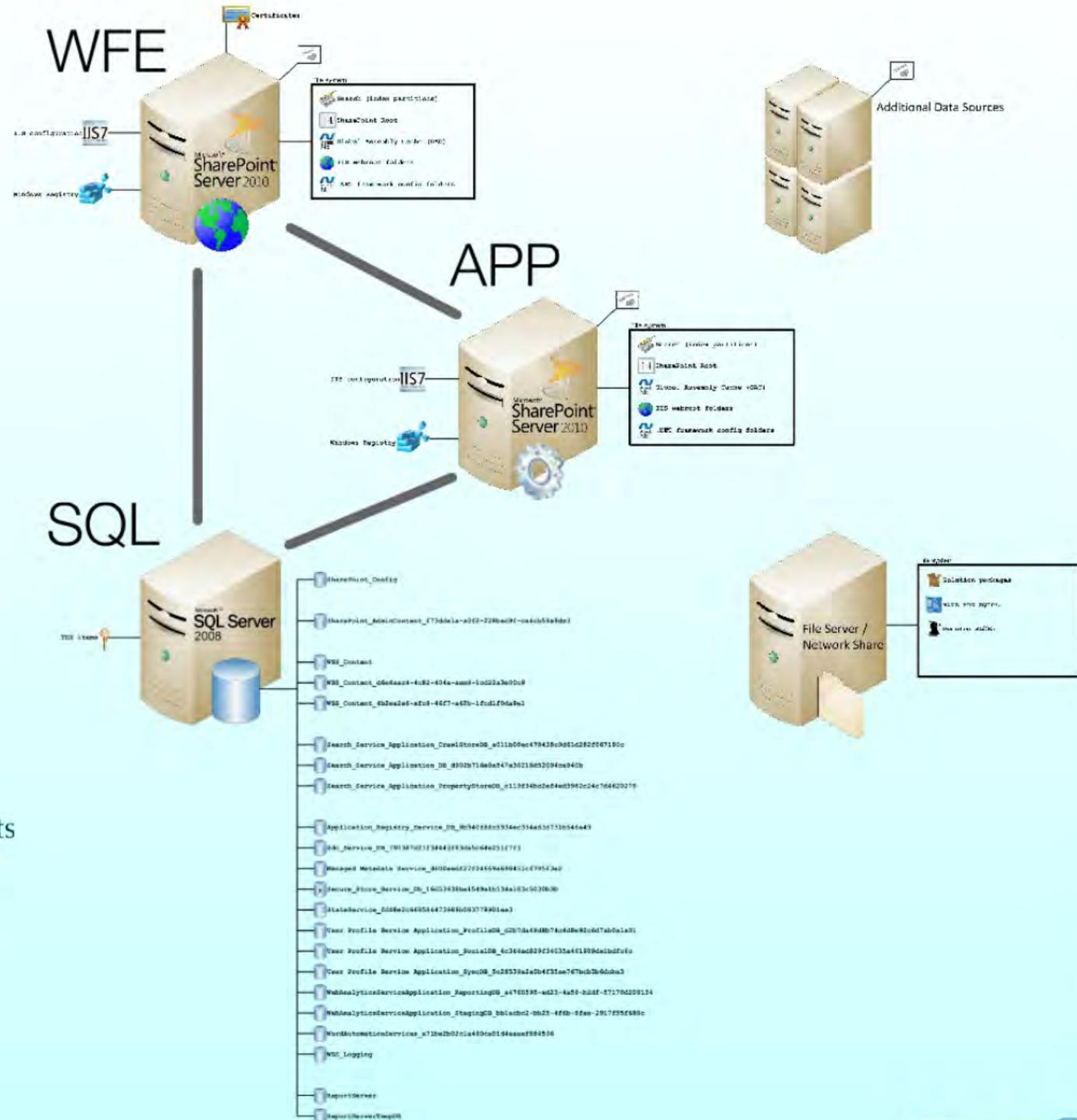
- Solution packages
- SharePoint Root
- IIS Configuration
- Certificates
- IIS web root
- GAC
- Registry
- Bits and bytes



## Edge cases and esoteric targets

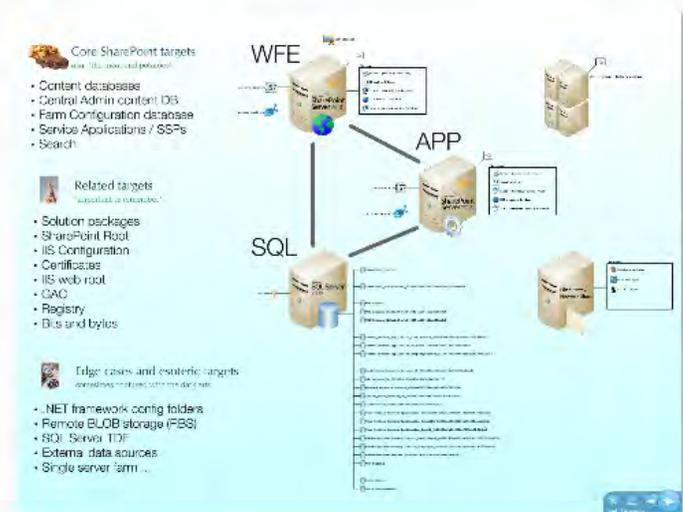
sometimes confused with the dark arts ...

- .NET framework config folders
- Remote BLOB storage (RBS)
- SQL Server TDE
- External data sources
- Single server farm ...



# Answer:

There is no definitive "list of everything." No two SharePoint farms (or DR plans) are the same.



You'll have to build your own list based on what you use in your farm

# Documentation



Of course you need to document your DR plan!

Documentation of the plan spans this phase and the next phase ...

Plan!

Documentation of the plan  
spans this phase and the  
next phase ...

Let's be honest:

documentation spans every  
phase of the DR process.

There's a focus on it here

and in the next phase, though.



**Assessment**



**Planning**

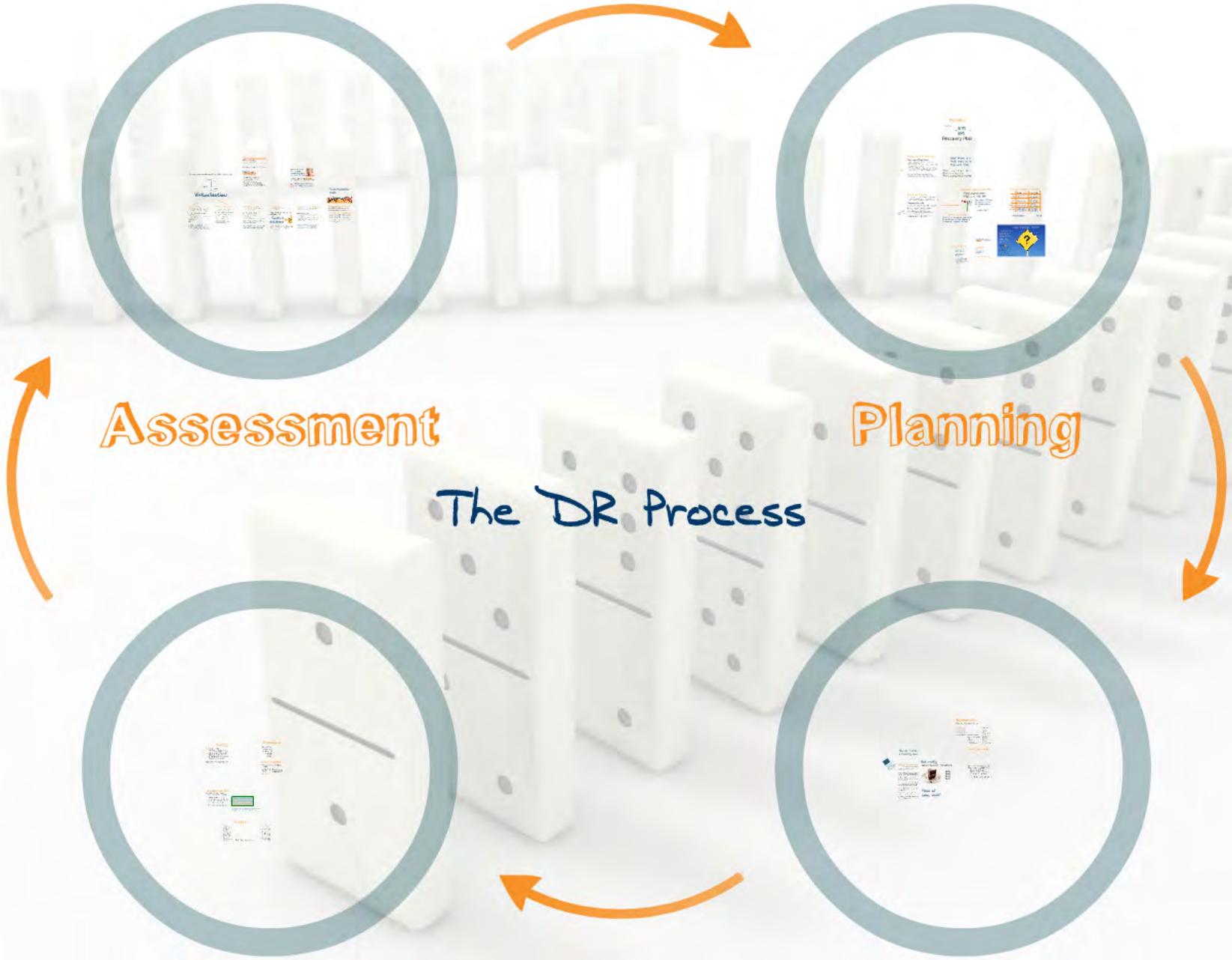


**Maintenance**



**Implementation**

*The DR Process*



# Implementation



# Implementation

Where the rubber meets the road

# Implementation

Where the rubber meets the road



Write the plans ...



Assemble resources ...

# 2 FREQUENTLY ASKED QUESTION

How do I write  
A recovery plan?

How do I write  
A recovery plan?

Writing a recovery plan



Start by talking to those in your organization who have some responsibility for business continuity.

Write

How do I write  
A recovery plan?

Writing a recovery plan

Characteristics of a good recovery plan

# A recovery plan:

## Writing a recovery plan

Characteristics of a good recovery plan

- The plan should address a discrete system or subsystem

# Writing a recovery plan

## Characteristics of a good recovery plan

- The plan should address a discrete system or subsystem
- Clearly identifies any assumptions made by the plan - hardware, software, dependent system restores, knowledge to execute, etc.

# Writing a recovery plan

## Characteristics of a good recovery plan

- The plan should address a discrete system or subsystem
- Clearly identifies any assumptions made by the plan - hardware, software, dependent system restores, knowledge to execute, etc.
- Identifies participants and the role they play in the plan - typically by group or company rather than individual

- The plan should address a discrete system or subsystem
- Clearly identifies any assumptions made by the plan - hardware, software, dependent system restores, knowledge to execute, etc.
- Identifies participants and the role they play in the plan - typically by group or company rather than individual
- Outlines steps for recovery in explicit detail - written to a lowest common denominator without requiring specialized knowledge

the plan - hardware, software, dependent system restores, knowledge to execute, etc.

- Identifies participants and the role they play in the plan - typically by group or company rather than individual
- Outlines steps for recovery in explicit detail - written to a lowest common denominator without requiring specialized knowledge
- For each step, potential misteps are spelled-out along with corrective actions that may be taken (if applicable)

- Identifies participants and the role they play in the plan - typically by group or company rather than individual
- Outlines steps for recovery in explicit detail - written to a lowest common denominator without requiring specialized knowledge
- For each step, potential misteps are spelled-out along with corrective actions that may be taken (if applicable)
- Specifies objective criteria for recovery confirmation and/or success

written to a lowest common denominator without requiring specialized knowledge

- For each step, potential misteps are spelled-out along with corrective actions that may be taken (if applicable)
- Specifies objective criteria for recovery confirmation and/or success
- Includes any post-recovery notes directing personnel to further actions or plans that are coupled (implicitly or explicitly) to the current recovery plan

- The plan should address a discrete system or subsystem
- Clearly identifies any assumptions made by the plan - hardware, software, dependent system restores, knowledge to execute, etc.
- Identifies participants and the role they play in the plan - typically by group or company rather than individual
- Outlines steps for recovery in explicit detail - written to a lowest common denominator without requiring specialized knowledge
- For each step, potential mistakes are spelled-out along with corrective actions that may be taken (if applicable)
- Specifies objective criteria for recovery confirmation and/or success
- Includes any post-recovery notes directing personnel to further actions or plans that are coupled (implicitly or explicitly) to the current recovery plan



Piece of  
cake, right?

# Not really.

Recovery plans are living documents



Iterate  
Iterate  
Iterate  
Iterate

....

# Implementation

Where the rubber meets the road



Write the plans ...



Assemble resources ...



Assemble resources ...

Some things to consider

#### Software

- Licenses
- Install media

#### Physical storage

- Documents/plans/lists/etc.
- Secure or sensitive items

#### Hardware

- SharePoint Servers
- SQL Servers
- Switches
- Storage/SANs
- Firewalls
- AD controllers/appliances
- DNS servers/appliances
- Load balancers

#### Facilities (if required)

- Rent/buy space
- Data center build-out
- WAN connectivity
- HVAC
- Fire suppression
- (Voice) communications
- Security
- Backup generators/power

Don't lose sight





Your SharePoint recovery plans should be tying into one or more bigger BCPs

- Communications plan tie-ins
- Criteria for DR plan activation
- Clear documentation of (manual) workarounds for non-restored functionality
- Integration points with other DR plans



**Assessment**



**Planning**

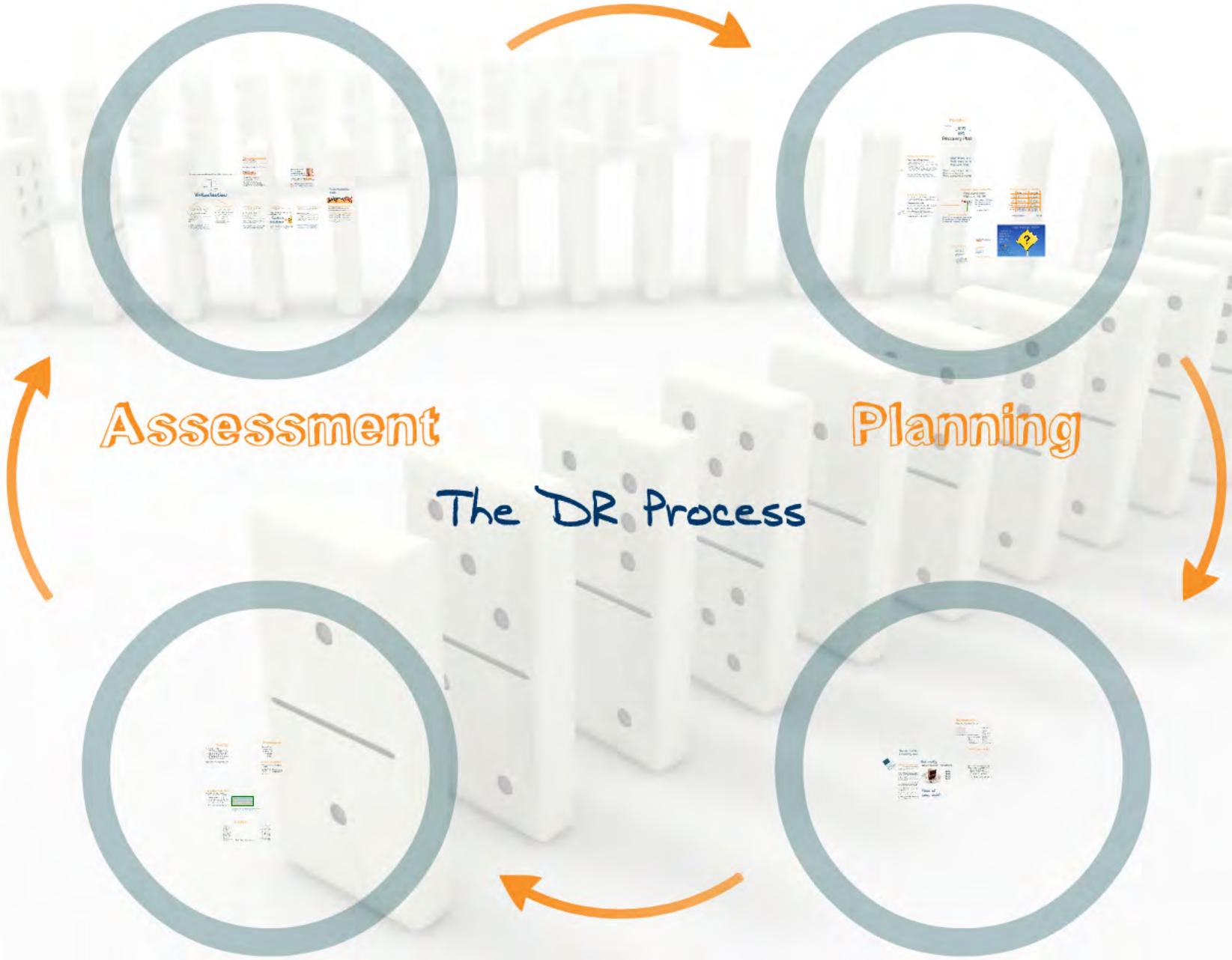


**Maintenance**



**Implementation**

*The DR Process*





# Maintenance

# Maintenance

The part that  
many of us  
wish would  
simply go  
away.



# What's included?

- Exercises that test and validate DR plans
- Updates to your plans as SharePoint environments change
- Budgeting for the changes that will happen

**PASS**



**FAIL**



# Testing

**PASS**



**FAIL**



# Testing

How testing can help you

- Identify gaps in plans so that you can address them before a disaster
- Validate that you can actually hit RPO and (especially) RTO targets
- With repetition, you can reduce your RTO (practice makes perfect!)

## How testing can help you

- Identify gaps in plans so that you can address them before a disaster
- Validate that you can actually hit RPO and (especially) RTO targets
- With repetition, you can reduce your RTO (practice makes perfect!)

*Bottom line: without testing you'll never know if your recovery plans actually work*

# Updating Your Plan

As your SharePoint environments change, so too must your recovery plans

# Updating Your Plan

As your SharePoint environments change, so too must your recovery plans

- RPO and RTO may change
- SharePoint farms grow and evolve
- SharePoint used for new purposes
- Offsite DR facilities change

# Updating Your Plan

As your SharePoint environments change, so too must your recovery plans

- RPO and RTO may change
- SharePoint farms grow and evolve
- SharePoint used for new purposes
- Offsite DR facilities change

*Your DR plans are living documents ...*



Don't leave your  
recovery plans to  
become "undead"



Don't leave your  
recovery plans to  
become "undead"

They don't "go away" because you abandon them;  
they just take on an un-life of their own ...

# Budgeting





Both time AND money

# Time

- Carry out DR tests (personnel, facilities time, business downtime)
- Review, maintain and update DR plans
- Review changes to SharePoint farms
- Audit plans with an eye towards compliance with any regulations



Both time and

# Money

- Salary costs associated with dedicating time to DR activities
- Costs associated with offsite facilities
  - Recurring licensing costs\*
- Costs associated with independent auditing of systems and DR plans



nd money



**Assessment**



**Planning**

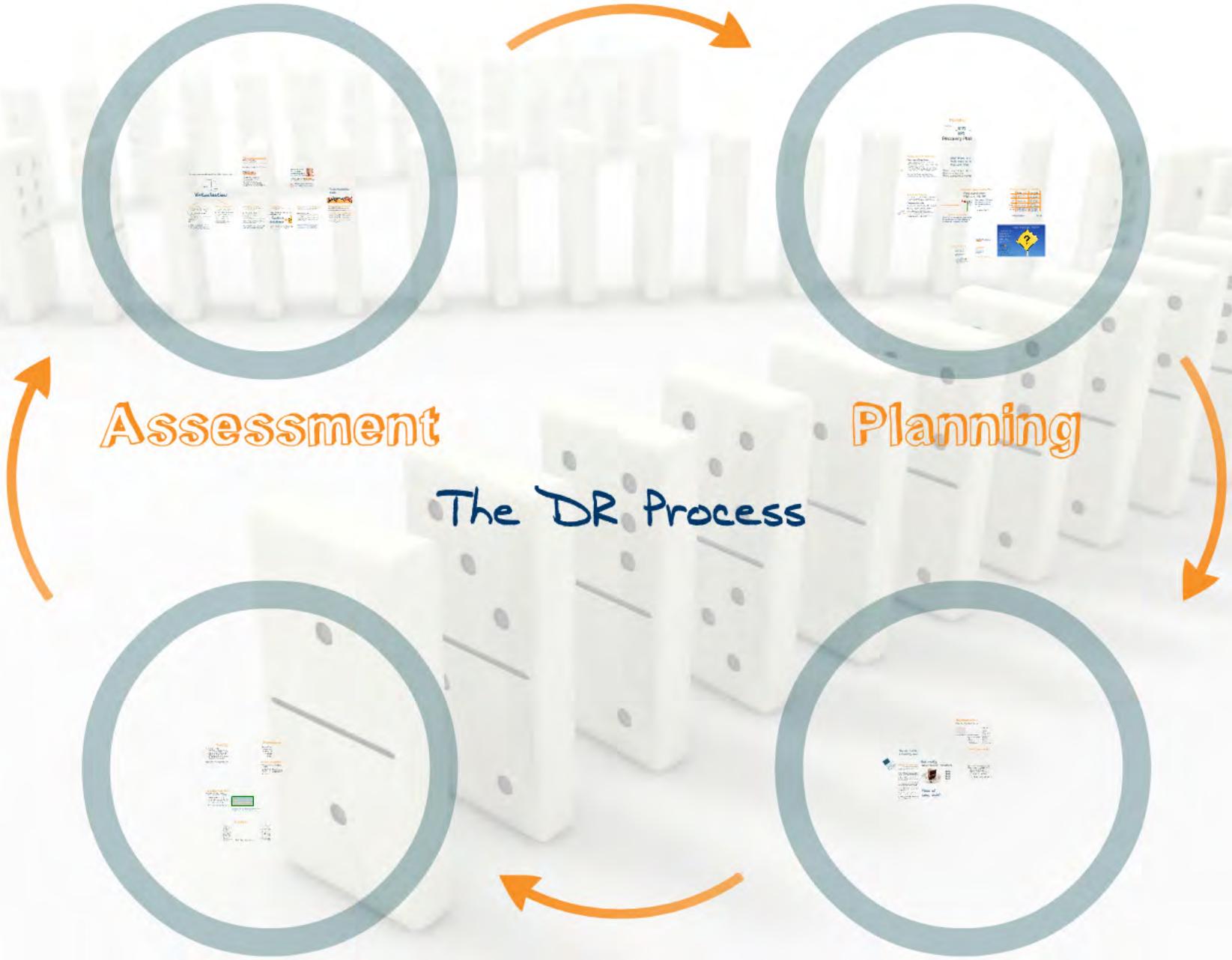


**Maintenance**



**Implementation**

*The DR Process*



# The dirty secret

Nobody gets this "right" the first time; that's why it's a continuous process



Assess



An  
important  
resource

NIST Special Publication 800-34 Rev. 1

**Contingency Planning Guide for  
Federal Information Systems**

Marianne Swanson  
Pauline Bowen  
Amy Wohl Phillips  
Dean Gallup  
David Lynes

May 2010



U.S. Department of Commerce  
*Gary Locke, Secretary*

National Institute of Standards and Technology  
*Patrick D. Gallagher, Director*

NIST Special Publication 800-34, Rev. 1, Contingency  
Planning Guide for Federal Information Systems

[http://www.nist.gov/manuscript-publication-search.cfm?pub\\_id=905266](http://www.nist.gov/manuscript-publication-search.cfm?pub_id=905266)

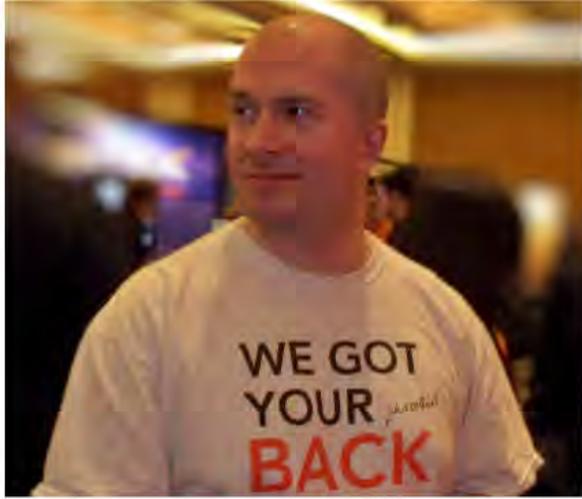
# Wrap-up

- Remember the order of operations:

Risk Analysis → BIA → BCP → DR Plan

- RPO AND RTO drive MANY of the DR planning decisions you'll make
- No two SharePoint environments are alike; no two DR plans are identical
- Recovery plans are living documents that you'll constantly test AND revise

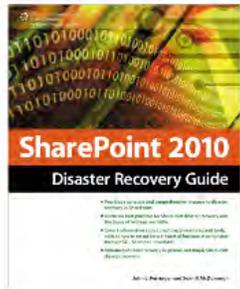
# SEAN P. McDONOUGH



Twitter: @spmcdonough

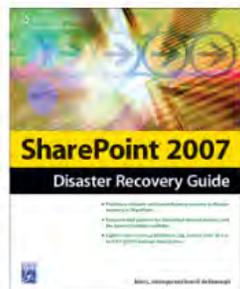
Blog: <http://SharePointInterface.com>

About: <http://about.me/spmcdonough>



SharePoint 2010 Disaster Recovery Guide

<http://tinyurl.com/SPDRGuide2010>



SharePoint 2007 Disaster Recovery Guide

<http://tinyurl.com/SPDRGuide2007>

## Feedback Please!

### Session Surveys via Event App

Select "Schedule" -> Select Session  
-> Scroll to "Session Survey"

### Download the App:

Event URL <https://crowd.cc/spfdc17>

Your App URL

<https://crowd.cc/s/zN7K>

Or search for "SharePoint Fest" in  
App Store



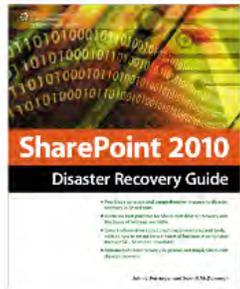
# SEAN P. McDONOUGH



Twitter: @spmcdonough

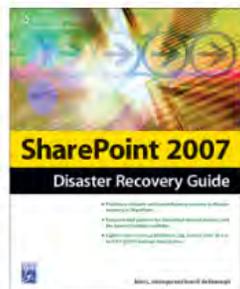
Blog: <http://SharePointInterface.com>

About: <http://about.me/spmcdonough>



SharePoint 2010 Disaster Recovery Guide

<http://tinyurl.com/SPDRGuide2010>



SharePoint 2007 Disaster Recovery Guide

<http://tinyurl.com/SPDRGuide2007>