Frequently Asked Questions

about the ServiceNow's business continuity management program

servicenow.

What is the ServiceNow business resiliency (business continuity and/or disaster recovery plan)?

ServiceNow has a formally documented Information System Contingency Plan (ISCP) which describes the recovery resources, procedures, and priorities necessary to provide seamless customer access in the event a disaster takes place that impacts customer data at the data center(s). The ISCP is dependent on ServiceNow's Advanced High Availability (AHA) data center architecture which provides replication and redundancy. ServiceNow's data centers are arranged in pairs. All customer production data is stored in both data centers in a pair and kept in sync using asynchronous database replication. Subproduction instances are only located in a single data center and are not replicated between data centers. Both data centers in a pair are active at all times and have identical processing capabilities; each data center has the ability to support the combined production load of the pair. Each data center has multiple ISPs coming into every data center cage, redundant network paths throughout the network, redundant disks in RAID arrays, redundant power suppliers, and many other hardware and configurations designed to remove single points of failure from the architecture. In the event of a disaster, ServiceNow activates a failover process that transfers customer operations to the alternate data center in the pair. From this perspective, ServiceNow is providing customers with business continuity as opposed to disaster recovery.

The ISCP is tested annually to validate and improve the ISCP. Additionally, the failover process is informally tested on a daily basis as ServiceNow uses failover to reduce the impact of maintenance on its service. ServiceNow's ISCP controls are validated on an annual basis during its ISO 27001 assessment.

ServiceNow's ISCP is reviewed at least annually by senior management and is available electronically to all employees. The ISCP is replicated between both data centers in the pair. Key ServiceNow personnel have been trained in their emergency response and recovery roles. The executive sponsor of the ISCP is the Chief Product Officer.

The ISCP is based on National Institute of Standards and Technology (NIST) Special Publication 800-34 ""Contingency Planning Guide for Information Technology (IT) Systems"" which provides instructions, recommendations, and considerations for government IT contingency planning.

At this time, we do not have a remedy for dual data center loss, but have geographic diversity between data center pairs to reduce that risk.

Please refer to the ISCP here:
https://community.servicenow.com/community?id=community_article&sys_id=aa4c22a1dbd0dbc01dcaf3231f9619a2

Please refer to the ISCP Test Report here:
https://community.servicenow.com/community?id=community_article&sys_id=e7fca6a5dbd0dbc01dcaf3231f961992

Please refer to the Corporate Business Continuity SOP here:
https://community.servicenow.com/community?id=community_article&sys_id=0dbcaa25dbd0dbc01dcaf3231f961962

Does the business resiliency program include a formal annual (or more frequent) executive management review of business continuity key performance indicators, accomplishments, and issues?

ServiceNow's ISCP is reviewed at least annually by senior management and is available electronically to all employees. The ISCP is replicated between both data centers in the pair. Key ServiceNow personnel have been trained in their emergency response and recovery roles. The executive sponsor of the ISCP is the Chief Product Officer.

Please refer to the Latest ServiceNow Information System Contingency Plan - Test Report here:
https://community.servicenow.com/community?id=community_article&sys_id=e7fca6a5dbd0dbc01dcaf3231f961992"

Are formal business continuity procedures developed and documented?

While ServiceNow's Information System Contingency Plan covers the ongoing operations of the cloud environment, ServiceNow has a formally documented Corporate Business Continuity Plan (BCP) which describes the procedures to recover and sustain its business operations. The annual Business Impact Analysis (BIA) includes the identification of critical resources and an assessment of potential disruption impacts, allowable availability thresholds, and recovery priorities. When combined, the operational risks provide ServiceNow with a comprehensive assessment of its business continuity posture. Due to the sensitivity of content, ServiceNow's BIA is not shared externally.

Semi-annual tabletop exercises are performed to validate the health of the BCP capabilities. ServiceNow's BCP controls are validated on an annual basis during its ISO 27001 assessment.

ServiceNow's BCP is reviewed at least annually by senior management and is available electronically to all employees involved in response and recovery. Key ServiceNow personnel receive training in the form of detailed, hands-on business continuity recovery drills and exercises. The executive sponsor of the BCP is the Chief Financial Officer.

For more details:
Please refer to the (10914) Information System Contingency Plan (ISCP) here:
https://community.servicenow.com/community?id=community_article&sys_id=aa4c22a1dbd0dbc01dcaf3231f9619a2
Please refer to the Latest ServiceNow Information System Contingency Plan - Test Report here:
https://community.servicenow.com/community?id=community_article&sys_id=e7fca6a5dbd0dbc01dcaf3231f961992
Please refer to the (POL0020158) Corporate Business Continuity SOP here:
https://community.servicenow.com/community?id=community_article&sys_id=0dbcaa25dbd0dbc01dcaf3231f961962"

Do formal business continuity procedures include the continuity of Information security activities and processes (e.g., intrusion detection, vulnerability management, log collection)?

As part of ServiceNow's High Availability offering, in the event that a primary colocation data center becomes unavailable, the secondary colocation data center will resume the functions with live data.

For more details:
Please refer to the Advance High Availability (AHA) whitepaper here:
https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/white-paper/wp-sn-advanced-high-availability-architecture.pdf"

Do formal business continuity procedures include the continuity of IT operations activities and processes (e.g., network operations, data center operations, help desk)?

ServiceNow has documented Corporate Business Continuity SOP for continuity of operational activities and processes including IT. ServiceNow has customer support offices located around the globe to provide 24/7, follow-the-sun support for ServiceNow's customers. Major support locations are San Diego, CA; Orlando, FL; London, United Kingdom; Amsterdam, Netherlands; Sydney, Australia. Incidents and problems reported by customers, are recorded and tracked in HI, ServiceNow's customer facing internal instance of our product.

Does the overall management of critical response and recovery include roles and responsibilities for those who invoke and execute the plan?

ServiceNow Control:
ISCP documentation includes the roles and responsibilities for those who invoke and execute the plans.

For more details:
Please refer to the (10914) Information System Contingency Plan (ISCP) here:
https://community.servicenow.com/community?id=community_article&sys_id=aa4c22 a1dbd0dbc01dcaf3231f9619a2

Please refer to the Latest ServiceNow Information System Contingency Plan - Test Report here:
https://community.servicenow.com/community?id=community_article&sys_id=e7fca6a 5dbd0dbc01dcaf3231f961992

Does the overall management of critical response and recovery include alternate and diverse means of communications in the event standard communication channels are unavailable?

"ServiceNow Control:
ISCP documentation includes Appendix F Alternate Site And Telecommunications. Additionally, section 3.2 Notification covers multiple communication channels to be used for internal communication and notification to customers.

For more details:
Please refer to the (10914) Information System Contingency Plan (ISCP) here:
https://community.servicenow.com/community?id=community_article&sys_id=aa4c22 a1dbd0dbc01dcaf3231f9619a2 "

Is there a periodic (at least annual) review of your Business Resiliency procedures?

ServiceNow has a formally documented Information System Contingency Plan (ISCP) which describes the recovery resources, procedures, and priorities necessary to provide seamless customer access in the event a disaster takes place that impacts customer data at the data center(s). The ISCP is dependent on ServiceNow's Advanced High Availability (AHA) data center architecture which provides replication and redundancy. ServiceNow's data centers are arranged in pairs. All customer production data is stored in both data centers in a pair and kept in sync using asynchronous database replication. Subproduction instances are only located in a single data center and are not replicated between data centers. Both data centers in a pair are active at all times and have identical processing capabilities; each data center has the ability to

support the combined production load of the pair. Each data center has multiple ISPs coming into every data center cage, redundant network paths throughout the network, redundant disks in RAID arrays, redundant power suppliers, and many other hardware and configurations designed to remove single points of failure from the architecture. In the event of a disaster, ServiceNow activates a failover process that transfers customer operations to the alternate data center in the pair. From this perspective, ServiceNow is providing customers with business continuity as opposed to disaster recovery.

Is a critical vendor Dependency Chart or list made available to clients?

For more details:
Please refer to the Data Center Certifications here:
https://community.servicenow.com/community?id=community_topic&sys_id=94495e2d dbd897c068c1fb651f9619eb

Do contracts with Critical Service Providers include a penalty or remediation clause for breach of availability and continuity SLAs?

Contracts with colocation data centers include penalties for breach of availability and continuity SLAs. Penalties include indemnification for damages, service credits for downtime, termination right, and continued obligation for resolution.

Please rank your financial resiliency plan that is in place to weather this event within the next 3 months of disruption.

As per our current assessment, there is no impact to ServiceNow's operations and employees. ServiceNow' is closely monitoring the situation.

Are products/services reliant upon any non-US personnel or facilities?

ServiceNow has customer support offices located around the globe to provide 24/7, follow-the-sun support for ServiceNow's customers. In the unlikely event that one region is unable to operate, another region will take over to ensure consistent, world-class customer support for every customer.

Further, U.S. Federal Government customers will continue to be supported **only** by our U.S. Government Customer Support team.

More information is available in https://hi.service-now.com/kb_view.do?sysparm_article=KB0597854

Do you have a pandemic policy?

ServiceNow has documented business continuity plans which are updated annually and address scenarios such as pandemic response. these plans are up to date to manage pandemic situations and include asset dependencies (office, people, critical third-party dependencies etc.).

Our crisis management plan address cross-functional response to pandemic along with external (government, regulators, media, etc.) and internal communications protocol.

a. If yes, is it being executed?

ServiceNow has not activated any of the business continuity plans yet. However, our emergency and continuity teams are well informed and on standby for the situation. We will keep this FAQ updated if anything changes

For more information

www.servicenow.com