bmc helix

Head in the Cloud: BMC Helix SaaS Security Overview and Approach

Table of Contents

Introduction

Time is of the essence in the digital economy. The modern business is more dependent than ever on technology with zero tolerance for outages and delays. Facing rising service demands, modern organizations struggle in a sea of legacy tools to manage increasingly complex, dynamic, and distributed IT environments. Fortunately, SaaS can help solve these challenges by building and scaling IT infrastructure to meet these needs and is expected to grow to a $116 billion-dollar market this year.

Companies are experiencing a tech tsunami with trends like multi-cloud, multi-device (IoT), multi-channel, DevOps and Big Data, creating enormous complexities in their IT landscapes. Organizations are gaining competitive advantage in the market by embracing cognitive automation technologies like AI/ML, virtual agents, chatbots, and RPA to transform their IT service and operations management tools from being reactive to proactive, predictive and preventive.

Since 1999, to SaaS or not to SaaS has been the question on every decision makers mind. In 2020, breaking down silos and giving access to innovation continues to be top of mind for all leaders. The speed of market changes requires a rethinking of processes that don't serve growth initiatives. Rewiring expectations starts with a hard look at how operations and services are managed end-to-end and giving teams flexibility to radically shift how they collaborate.

The sunk cost fallacy of legacy technology continues to be a productivity killer – end users are tired of not being able to take advantage of new innovations and often view ITSM and ITOM teams as laggards. In a recent survey, only 47% of employees felt like their org understood what technology they needed to be productive. As both teams try to merge policies and process, one driver remains key. A great customer experience, internally and externally.

Employees want to work for businesses that give them the tools to be successful at their jobs and they know that collaboration is the key to accomplishing great things. Digital transformation has moved beyond a buzzword and into the IT cost center. The new enterprise is SaaS powered.

Business Challenge	SaaS Outcomes
Scalability: whether it's the normal progression of a growing business or the need to accommodate huge capacity jumps, your infrastructure needs elasticity to rapidly increase or decrease compute power and storage needs on demand.	• BMC's services offer vertical and horizontal scaling of the infrastructure to meet performance requirements and consumption demands. • It facilitates multiple systems to talk to each other, giving you the freedom to scale-on-demand.
Cost: when you manage an on-prem data center, it's up to you to keep everything up to date. Enterprises end up spending a lot in terms of resources and time to upgrade software and hardware to remain current.	• With cloud, your organization can focus on its core business and delivering customer value, not on managing software and infrastructure.
Security: with security threats drastically increasing in scale and severity, protecting your business without disrupting innovation and growth seems impossible.	• Saas affords companies the opportunnity to re-engineer, automate, and strenghten their security to reduce the level of risk they face today. • Public cloud providers also offer vast resources for protecting against threats—more than nearly any single company could invest in.
Compliance: in an increasingly regulated world, applying consistent methodology to tackling risks cross business units and keeping pace via solutions that can apply speed and accuracy is top of mind for the corporate agenda.	• SaaS-based tools and services are already industry standard compliant, helping remove some of the burden of compliance from your enterprise IT teams. • Solutions that automate compliance checking and remediation can further increase efficiency and productivity, allowing organizations to maintain audit readiness and shift skilled resources to other projects.
Time to Value: digital business needs span a multitude of use cases and applying data to decisions, especially as the rate of data ingestion grows, remains a huge challenge. How fast your team can turn data into actionable insights can mean the difference between surviving or thriving.	• Moving to SaaS means enabling faster upgrades and access to innovations for your users. This means your organization saves time and money, but also realizes revenue faster.
Flexibility: a key growth driver is user access to business services while they're on the go, no matter the location. Fueled by constant improvements in the services they consume in their daily lives, the workforce expect the same from their employer.	• Mobility gives you and your employees the flexibility to work from any location. Cloud computing enables you to monitor the operations in your business effectively.

BMC Helix Overview

The public cloud has reimagined the way we do business and allowed us to rapidly embrace change down to how we iterate and learn. With this transformation, come hundreds, if not thousands, of accounts; similar, but not identical, cloud services across multiple platforms; and business apps and microservices updated at a dizzying frequency, consuming thousands of cloud resources, each one of which must be properly configured to be secure and remain compliant.

As AI and automation become foundational to service management, IT organizations must evolve to meet new expectations for service delivery. The next stage embraces and integrates these technologies to create a new intelligent enterprise.

BMC Helix is the first and only end-to-end service and operations SaaS platform integrated with 360-degree intelligence. It delivers fast, accurate, cost-effective cognitive service management for the complex demands of your multi-cloud, multi-device, and multi-channel environments. Our approach empowers the Cognitive Enterprise with:

- Choice of cloud with containers: leverage the power of containers and run your cloud of choice.
- Omni-channel service experience: a seamless multi-channel, multi-device experience for users.
- AI platform-agnostic flexibility: integrate with your preferred AI platform.

Culture of Responsibility

Security Approach

At BMC, security is a journey rather than an end goal or a final state. Our practices are always evolving, and we adapt our tools and techniques to encompass new technologies and protect against new kinds of threats. We know that IT operations and security professionals are continuously overwhelmed with the number of tasks and sheer volume of work they face every day, and solutions for task and process automation have become a necessity. Our goal is to deliver modern solutions that integrate easily within your ecosystem, provide easy-to-use interfaces and utilize modern technologies such as containers and microservices.

We know that cloud and container security is challenging because of the supercharged velocity of change. Qualified security talent is scarce, and so automation is all the more important to keep enterprise IT propelling the business forward is a secure and compliant manner. For enterprises adopting new technology, the importance of ensuring compliance cannot be overlooked. For most organizations, that means making sure security measures are met, being aware of potential challenges, and of course, staying on top of industry trends in compliance.

We know that you cannot manage what you cannot measure. We have thousands of cloud resources changing every day in our development cloud accounts as developers continuously push new functionality to production. We are constantly striving to increase our agile velocity without compromising on security. We build with the end in mind, benchmarking our security posture and looking for ways to fix high risk vulnerabilities.

With all this in mind, we've built the BMC Helix platform to provide visibility and control into the security initiatives necessary to protect data across borders. We continually evaluate the challenges associated with the complexity of distributed IT environments and keep an eye towards features critical for success and growth.

Cloud environments are subject to rapid change, and traditional tools are unable to keep pace. We've built automation into our end-to-end platform to enable you to operate with speed, visibility and control, while remaining audit ready.

Operational Approach

BMC understands that the confidentiality, integrity and availability of your operational information are vital to your organization. We use a multi-layered approach to protect your data, constantly monitoring and improving applications, systems, and processes. The BMC Security Operations Center (SOC) and Network Operations Center (NOC) teams work 24 hours a day, seven days a week, and 365 days a year to ensure the continuous and secure operation of your service.

The NOC makes extensive use of BMC's world class monitoring and automation solutions. All customer environments are monitored 24 hours a day and seven days a week. The NOC frequently resolves potential incidents before they impact customers.

BMC Helix Data Handling Policy

Our commitment to data privacy, integrity, and security is published here. We manage sensitive customer data by using the following guidelines:

- Customers retain ownership of their data at all times.
- Strong physical security mechanisms are in place at all BMC Helix facilities based on SSAE 18 (or equivalent) certified data centers. See Service locations for additional details.
- All external solution traffic over the web is secured using encryption.
- You are allocated a dedicated or shared environment depending on the services purchased. Environments leverage virtualization and/or containerization for the user interface and application server components.
- Your database is dedicated to your data (data is not mixed among customers or environments).
- The infrastructure and applications are configured to account for security standards using a hardening process to reduce security vulnerabilities.
- Monitoring is in place to alert you of any suspected or actual data breaches.
- Periodic penetration tests are performed to identify any potential or actual security issues.
- The operational and support organizations employ the separation of duties security principle to ensure that only the resources required to support the solution have access to specific data.
- Periodic internal and external security audits are run on the systems to identify any vulnerabilities.

Data Privacy Overview

Safeguarding the privacy and security of personal information is a top priority for BMC in our data driven economy. In July 2015, BMC became the world's first IT management provider to get its Data Privacy Binding Corporate Rules Policy (BCRs) approved by the European data protection authorities, both as a Controller and a Processor. BCRs are considered to be the platinum standard for compliance in data privacy and personal data protection worldwide. BMC's BCRs apply to all personal information of past, current and potential BMC employees, customers, resellers, suppliers, service providers and other third parties.

All BMC entities, employees and third-party providers comply with and respect the BCRs which govern the collection, use, access, storage and transfer of personal data among BMC entities and third-party sub-processors worldwide.

General Data Protection Regulation (GDPR)

On May 25, 2018, the European General Data Protection Regulation (GDPR) entered into force and modified the legislation underlying BMC's BCRs. As advised by the EU Regulators, BMC has updated its BCRs to reflect the relevant changes and notified the updated version to the French Data Protection Authority ("CNIL"), who initially approved our BCRs in 2015. The most significant changes include Accountability, Transparency, Individual Privacy Rights and Privacy by Design.

Data Protection

Malware protection

BMC utilizes McAfee Endpoint Security on all servers, workstations, and email gateways for core threat prevention, endpoint detection and incident response. Protection includes virus scanning, and spyware and adware detection. McAfee agents are updated daily and managed centrally using a centralized policy server. Viruses and malware alerts are reported to the Security Information and Event Management (SIEM) system and assessed weekly as part of the Security Operations Control reporting procedure. All customer servers contain the McAfee agent and have no anti-malware exceptions.

Incoming data files are scanned automatically when sent via email. Scanning is also performed on-access as part of the standard security policy.

SaaS Media Protection policy

BMC's SaaS Media Protection policy addresses practices that control the use of data on removable media and mobile devices. BMC restricts access to customer information to those with a legitimate need to know and requires restrictions and device configuration to limit types of portable media.

Data Encryption

Data at Rest for BMC Helix ITSM services

BMC provides two options for encryption of data at rest:

1. The entire database can be encrypted at rest upon request.

2. You may encrypt only certain character fields. This option utilizes AES 128-bit encryption.

Data at Rest for BMC Helix Custom Applications-based services

Data at rest for BMC Helix Custom Applications-based services is encrypted by default in all environments. Encryption is implemented using PostgreSQL encryption at the file system level.

Data in Transit

Data in transit over the public internet utilizes encryption technologies such as HTTPS/SSL, TLS, AES and IPSec. Between the BMC Helix Client Gateway and the customer's server gateway, IP-based restrictions are utilized coupled with a pre-shared key.

Email Encryption

To guarantee message privacy as email messages transit the public internet mail infrastructure, BMC supports email encryption based on Transport Layer Security (TLS) and Secure Sockets Layer (SSL).

Data in Transport

BMC's media protection policy governs any type of media transport and covers the protection and control of all media with sensitive information used during transport outside of controlled areas. The transport of media is controlled and secured by strict chain-of-custody procedures.

Confidentiality

BMC ensures that all personnel granted access to customer systems have committed themselves to protecting customer data by executing written confidentiality obligations. The obligation to treat customer data pursuant to such confidentiality obligations survives the termination of employment. Applying the principle of least privilege, customer data is made available only to personnel that require access to such data for the performance of BMC's contractual obligation to you.

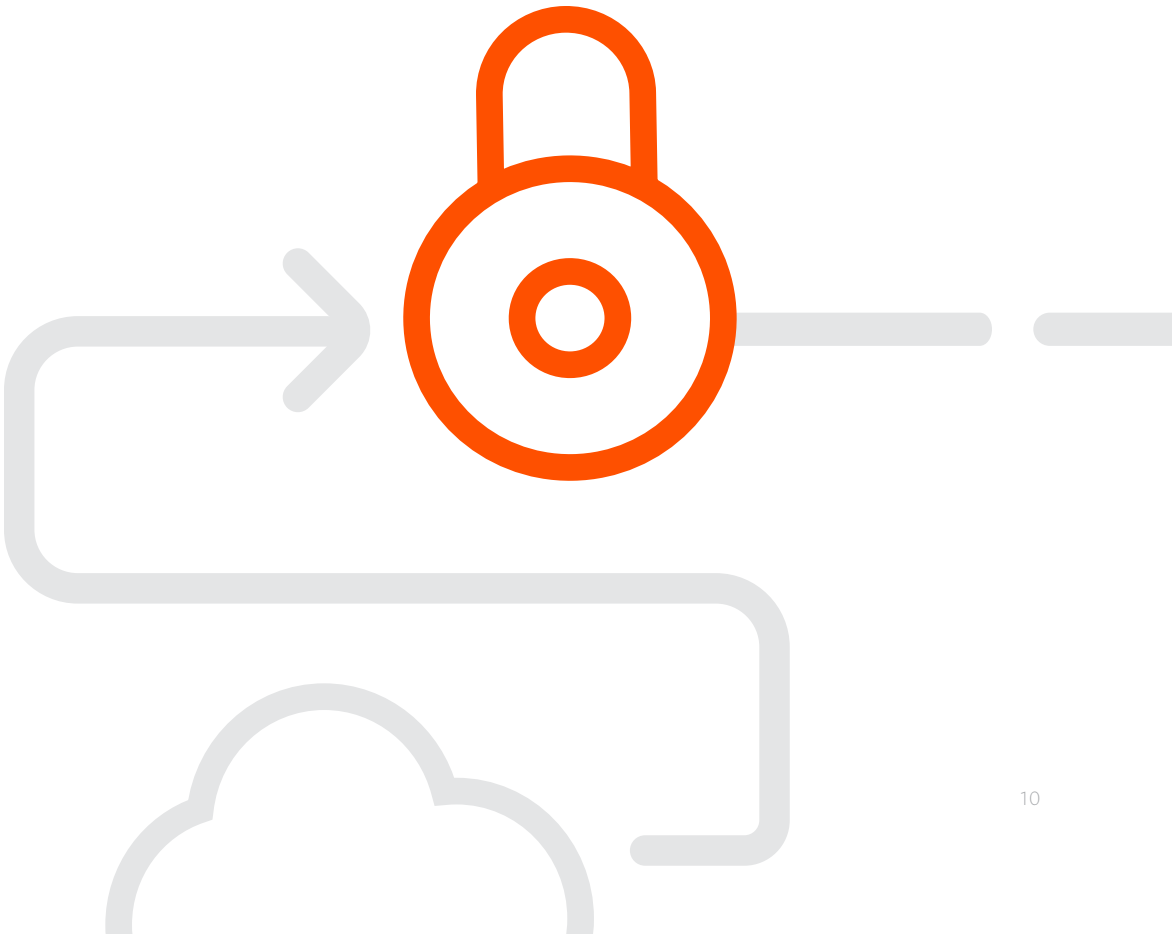
Technical Protection Measures

Access control to data center facilities and assets to prevent unauthorized persons from gaining access to customer systems and data are controlled by the following measures:

- Access to customer data is restricted to BMC authorized personnel only and controlled via identity management systems.
- BMC utilizes stringent user password creation, encryption and management processes.
- BMC's data center facilities are provided by industry-recognized providers and include:
- Multiple compliance certifications
- 24-hour security
- Restricted, multi-factor access requirements

User Password Controls

BMC user accounts that provide access to customer systems are created using strict password controls to prevent unauthorized use with controls in place to manage algorithms; password creation, transit and storage; and access restrictions amongst others.



Culture of Resiliency

Forty years ago, we couldn't have imagined how a global pandemic could force the world, and the enterprise, to its knees. Building a culture of resilience is key to enabling robust organizations that can withstand threats that can't be imagined or even prepared for. Imbuing resiliency in your workforce is more than just a buzzword, it requires a cultural shift. In the age of analytics, remaining flexible and able to pivot as needed is still as critical as the opportunities to predict and prepare for events that could disrupt the business. Adaptive capacity and empathy remain the bedrock of resiliency required of a workforce that may need to pivot at a moment's notice.

Compliance doesn't sleep during a crisis, neither do bad actors. The ability to successfully implement adaptive cybersecurity starts with ensuring the integrity of business-critical data and that it is collected, stored, and used with a zero-trust framework.

Purpose

Information systems are vital to the mission for BMC and its business functions. It is therefore critical that the services provided by BMC are able to operate effectively without excessive interruption. BMC's Information Systems Contingency plan (ISCP) establishes comprehensive procedures to recover BMC Helix services quickly and effectively following a service disruption. We have extensive guidelines and procedures for notification and activation, recovery and reconstitution prior to the occurrence of a service disruption.

Compliance

BMC's ISCP supports the requirements for the Federal Risk and Authorization Management Program (FedRAMP). The ISCP denotes interim measures to recover services following an unprecedented emergency or system disruption. Interim measures include the relocation of production systems and services to an alternate site. Unless otherwise agreed in advance, alternate sites will always reside within the same country as the primary site.

Scope

In accordance with Federal Information Processing Standards (FIPS) 199, BMC follows guidelines on determining potential impact to organizational operations and assets, and individuals through a formula that examines three security objectives: confidentiality, integrity, and availability. The procedures in the ISCP have been developed for a moderate-impact system and are designed to recover BMC Helix services within the RTO targets specified below.

The following sections provide details about BMC's disaster recovery services, an overview of the three phases of the ISCP, and a description of the roles and responsibilities of key personnel during contingency operations.

Disaster Recovery

Disaster Recovery is measured based on these objectives:

- **Recovery Point Objective (RPO):** the maximum loss of data before the disaster occurred. BMC offers a 15-minute RPO for all BMC Helix services.
- **Recovery Time Objective (RTO):** the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources and supported mission and business processes. BMC offers a four-hour RTO for all BMC Helix services.

Contingency phases

BMC's ISCP is designed to recover and reconstitute BMC Helix services using a three-phased approach. The approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions. The three recovery phases consist of activation and notification, recovery, and reconstitution.

Application Patches

BMC SaaS Operations manages all patching and maintenance of the underlying infrastructure for the BMC Helix services. This includes the installation of patches and service packs, and the application of upgrades. BMC provides periodic service packs for its BMC Helix solutions that may include a fix for known errors, or improved or incremental functionality; service packs are available to all customers. Hotfixes may be recommended by the BMC SaaS Service Desk and address known issues that are isolated to a specific customer.

Auditing

Third Party Audit

BMC completes a Type 2 Service Organization Control (SOC 2) examination annually. The examination is conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). The SOC 2 report is issued by an independent CPA firm and includes a qualified opinion on BMC's controls relative to the security, availability and confidentiality trust services principles and criteria of its BMC Helix services.

Culture of Readiness

Integrated Security Framework

For the most part, it can seem impossible to secure a highly elastic multi-cloud environment using traditional security strategies and solutions. At BMC, we have adopted an integrated security framework designed to operate effectively at the speed that networks currently require. Security technologies deployed across the network need to be able to share the threat information they gather, which is where tools like antivirus and antimalware, next-gen firewalls, and advanced protection are especially beneficial.

We also believe in leveraging automation with governance rules specifically for the cloud and a continuous risk treatment approach. We don't operate in silos; we embed technologies that provide a holistic view and capable of taking action on threats. With the speeds of cyberthreats, and the complexity of today's cybercriminals, time is truly of the essence and not even a second can be wasted. We've also built in SIEM (security, information, and event management) technologies to bolster advanced threat detection, prioritize indicators and automate collective responses.

BMC SaaS Operations Team

The BMC SaaS Operations team manages all operational aspects of the service, from activation to decommissioning. The following table describes key areas of responsibility:

Function	Description
Activation activities	Service activation focuses on the initial setup and configuration of your Helix environments so that you can begin using your service.
Lifecycle Requests	Operational and enhancement services included with your BMC Helix subscription are referred to as Lifecycle Requests. These services are fulfilled upon request by the BMC SaaS Operations team.
Customizations	BMC allows unlimited application customizations to your applications, assuming best-practice design is used. Ongoing maintenance of customizations is the responsibility of the customer.
Go-live assessment	Just before production cutover, the BMC SaaS Operations team conducts an extensive go-live assessment to evaluate production system parameters. Adjustments are made to the system if necessary.
Security	Led by its Security Operations Center (SOC), BMC uses a multilayered approach to protect your data, constantly monitoring and improving applications, systems, and processes.
Incident Response policy	Responding to incidents affecting your production system and restoring your service to normal levels is the number one priority of BMC SaaS Operations. Reporting on a service disruption involves an analysis of the issue, followed by a Request for Outage report.
Change management	The BMC Helix change management process involves close control of system changes throughout their lifecycle to ensure minimum disruption to supporting services.
Application patches	BMC manages all patching and maintenance of the underlying infrastructure of the BMC Helix services.
Application upgrades	BMC schedules and performs upgrades and patches per its published upgrade policy. Some services are upgraded per a schedule set by BMC SaaS Operations; others are by request.

Maintenance windows	Standard maintenance windows are published in advance and are typically outside of normal business hours for the region. Reminders are sent at least seven days before maintenance occurs for non-production systems and at least 21 days before maintenance occurs for production systems. Standard production monthly maintenance windows are a maximum of four hours in duration, with a goal of zero downtime. While most maintenance will not require downtime, infrastructure and shared service upgrades might require server restarts within this window.
Data handling	BMC data handling includes everything from data backup and retention schedules to archives to final data exports.
Auditing	BMC provides continual auditing of OS security logs and application logs, to proactively assess system activity.
Disaster recovery	The BMC Information Technology Contingency Plan addresses actions required by BMC in the event of a disaster that impacts a customer's primary service location. This plan is tested regularly. BMC offers two options for disaster recovery to suit a customer's individual recovery point and recovery time objectives.
Data extraction	Service decommissioning is provided when a customer's service terminates or expires. In such case, BMC SaaS Operations provides a data backup file in a comma-separated values (.csv) format or provides a database backup file before permanent deletion of the data occurs.

Data Centers and Architecture

BMC's Helix services are hosted from various regional locations. Each customer's service location is dependent on various factors such as environment type, proximity of the customer to the data location, and customer sector (public versus private).

Service Locations and Compliance

BMC is committed to offering its services from facilities that meet or exceed the rigorous standards and compliance requirements of our customers.

Service Location Features

Each BMC-controlled service location adheres to the following minimum standards:

Site characteristics	• Built to Tier III design specifications • Raised floor and/or overhead cable management systems
Security	• Security framework: based on the NIST SP 800-53 standards at a Moderate level • Guarded 24 hours a day, 7 days a week • Card access or biometrics access • Multilevel security card readers with battery backup • Closed-circuit television (CCTV) surveillance • Automated building monitoring system that oversees facility power, environment, and backup systems • Perimeter fence and gate controls
Communications	• FIPS 140-2 compliant cryptographic ciphers • Engineered with redundant network equipment, switches, links, and carriers, ensuring high availability and performance • Backbone speeds of the network are based on Gigabit Ethernet and 10-gigabit. Switches and routers have dual power supplies and failover LAN cards. • Redundant high-speed internet links with multiple carriers for primary sites • Redundant firewalls
Electrical and mechanical systems	• N+1 power infrastructure • Redundant grids • Mirrored, fully redundant uninterruptible power supply systems (UPS) • Redundant diesel generators • Redundant power distribution units • Redundant chillers, cooling towers or water pumps • Redundant packaged heating and air conditioning units • Multizone, dry-pipe sprinkler and smoke-detector system with VESDA; water-detection system • On-site emergency diesel fuel

Service Environment Details

Separate customer environments are provisioned for BMC Helix services. Application updates flow from the development / tailoring environment through QA before going live in production. These environments contain the most-recent generally available (GA) version of the products and out-of-the-box content (including services, templates, requests, catalogs and so on), pre-installed from a golden image.

Following the solution build and test, the environment is moved to QA so that the customer can perform the required user acceptance testing prior to going live. For services where a QA environment is not provided, user acceptance testing is performed in the development environment.

Environment	Purpose
Development / Tailoring	Creation of customer-specific integrations, workflow, and data configurations
Production	Operation of BMC Helix processes available to end users
Quality Assurance (QA)	Release, testing, and validation of custom application components prior to live operation

All environments are controlled, monitored, and managed by BMC SaaS Operations (including the underpinning application and infrastructure aspects of the BMC Helix services). Areas of focus include hosting, storage, network, application software, and the connectivity between the cloud and the customers' premises.

Additionally, the service includes the management of standard operational activities such as data and system backup and recovery.

Certifications and Standards

BMC has a variety of certifications, processes and controls in place for the Helix service:

- Binding Corporate Rules – intra-organizational transfers of personal data across borders
- Cloud Security Alliance assessment – publicly available self-assessment of BMC security controls
- FedRAMP Authority to Operate (ATO)
- GDPR – EU law on data protection and privacy
- ISO 14001 – environmental management
- NIST 800-53 – security controls for all U.S. federal information systems except those related to national security; All BMC security controls are based on this standard
- SOC2 TYPE II – 3rd party assessment of BMC's controls around Security, Availability and Confidentiality
- Third-party penetration tests – perimeter, network and application penetration tests

BMC Helix service locations typically have the following certifications (may vary by region):

- FedRAMP – see above
- ISAE 3402 – internal controls for financial reporting
- ISO 9001 – quality management system
- ISO 14001 – see above
- ISO 27001 – organizational information security risks
- ISO 50001 – energy management standard
- OHSAS 18001 – Occupational Health and Safety management systems
- PCI DSS – the Payment Card Industry Data Security Standard
- SSAE 18 SOC1 and SOC2 – auditing standard for service organizations
- Tier III Certification of Design Documents – facility engineering and architectural specifications

Conclusion

The future is one where technology will be firmly embedded in human lives, shaping how we work and live. By 2025, nearly two-thirds of enterprises will be prolific software producers with code deployed daily; over 90 percent of new apps will be cloud-native, 80 percent of code will be externally sourced, and there will be 1.6 times more developers. Technology will underpin every successful company and drive every business function, spanning customer relationships, business operations, and people management.

The evolution of security functions that can automatically sense, detect, react, and respond to access requests, authentication needs, and outside and inside threats, as well as meet regulatory requirements is necessary. BMC's Helix services combine AI-enabled solutions with a crowdsourcing environment, employs security-integrated DevOps (DevSecOps), uses cloud-native infrastructure and services, and adopts mature access and authentication practices with a zero-trust framework.

In addition to an innovation mindset, successful companies will have three common traits:

Agility	Customer centricity	Actionable insights
They create new operating models that integrate business, operations, and technology into standalone businesses-within-the-business domains. This approach allows organizations to run and reinvent themselves—they can be truly disruptive in one area while still supporting traditional businesses.	They leverage a connected economy to ensure they can meet and exceed customer expectations. By creating an ecosystem that uses technology to cater to every touchpoint of the customer journey, these organizations seem to anticipate their customers' requirements and deliver the goods and services	They know how to turn data into insights that drive actions which serve and anticipate customer needs. Organizations that know how to pull all the relevant information, capabilities, and people into the same place can act quickly and efficiently in making the right decisions.

Mastering these traits in a shifting landscape requires the evolution of companies to a state that supports the business today, while keeping the future in mind.

This is the path to an Autonomous Digital Enterprise (ADE).

Definitions

FedRAMP - Federal Risk and Authorization Management Program is a US federal agency-specific process for assessing and authorizing federal cloud computing products and services. FedRAMP consists of a subset of National Institute of Standards and Technology Special Publication (NIST SP) 800-53 security controls specifically selected to provide protection in cloud environments. BMC's FedRAMP certification is defined for the Federal Information Processing Standards (FIPS) 199 Moderate impact level.

ISAE 3402 - International Standard on Assurance Engagements No. 3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organizations and their auditors on the controls at a service organization that are likely to impact or be a part of the user organization's system of internal control over financial reporting.

ISO 9001 - International Organization for Standardization 9001 sets criteria for a quality management system. Based on a number of quality management principles, this certification assesses customer focus and helps ensure that customers get consistent, good quality products and services.

ISO 14001 - International Organization for Standardization 14001 certifies that a company's environmental policies, protocols and procedures meet a standard whereby impact to the environment is minimized.

ISO 27001 - International Organization for Standardization 27001 is a specification for an information security management system. This system is an approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

ISO 50001 - International Organization for Standardization 50001 specifies requirements for establishing, implementing and maintaining and improving an energy management system, whose purpose is to enable an organization to follow a systematic approach in achieving continual improvement of energy performance. It includes energy efficiency, energy use and consumption.

OHSAS 18001 - Occupational Health and Safety Management Systems is an international unified approach for the requirements of an occupational health and safety management system. It is a British Standard that exists to help organizations put in place demonstrably sound occupational health and safety performance.

PCI DSS - The Payment Card Industry Data Security Standard is a proprietary information security standard for organizations that handle branded credit cards from the major credit card companies. The standard was created to increase controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually.

SSAE 18 - Statement on Standards for Attestation Engagements (SSAE) No. 18, also referred to as a Service Organization Controls (SOC) 1 report, is an auditing standard for service organizations and serves as the authoritative guidance for reporting. It was drafted with the intention and purpose of updating the US service organization reporting standard so that it mirrors and complies with the international service organization reporting standard ISAE 3402. See also Third party audit for BMC's SSAE 18 SOC 2 Type II accreditation for the services.

Tier III Certification of Design Documents - As certified by Uptime Institute, tier certification is a performance-based evaluation of a data center's specific infrastructure. The first step in the certification process is the Tier Certification of Design Documents (TCDD) designation. To obtain the TCDD compliance level, Uptime Institute reviews all design documents, ensuring each subsystem among electrical, mechanical, monitoring and automation meet the fundamental concepts.

About BMC

From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise.

BMC—Run and Reinvent **www.bmc.com**

522721