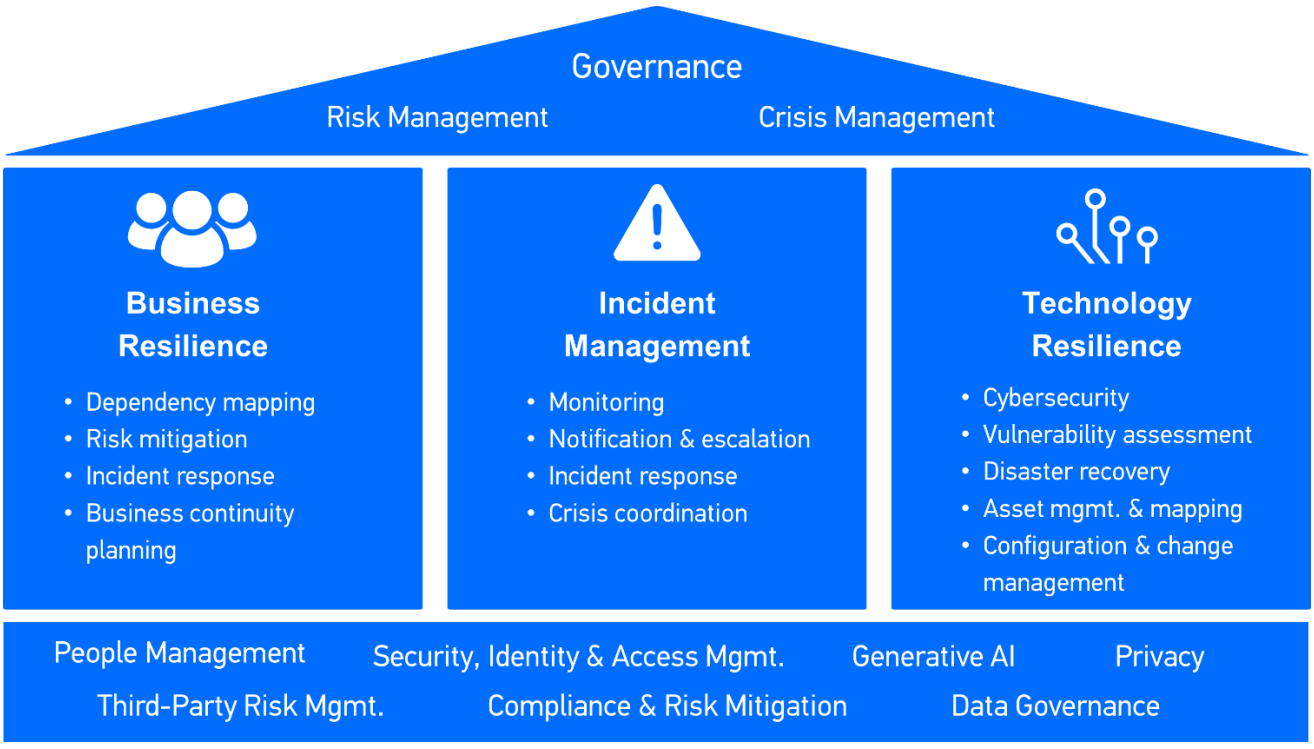
DIRECTV BUSINESS CONTINUITY MANAGEMENT SYSTEM

EXECUTIVE OVERVIEW

Events such as natural disasters, pandemics, cyber incidents, or critical technology failures can disrupt normal business operations. DIRECTV maintains an enterprise-wide Business Continuity Management System (BCMS) designed to ensure operational resilience and continuity of critical services during disruptive events. This system enables DIRECTV to continue providing high-quality video services to customers during periods of uncertainty.

DIRECTV's BCMS is aligned with ISO 22301, the international standard for business continuity management, and is designed to support the resilience of people, processes, technology, and third-party dependencies.



Governance and Leadership Commitment

DIRECTV has established a multi-tiered governance framework to provide oversight, direction, and accountability for business continuity activities. This framework includes Oversight, Risk Management, and Crisis Management functions that define policies, standards, and expectations across the enterprise.

Business Continuity Planning (BCP) is led by a designated Leader who coordinates with stakeholders across the business units to ensure continuity plans are documented, maintained, and aligned with enterprise standards. Executive oversight is provided by DIRECTV's Executive Committee, which serves as the governing body responsible for strategic direction, sponsorship, and support of the BCMS.

Business Continuity Capabilities

DIRECTV's BCMS integrates multiple resilience capabilities to ensure preparedness and effective response to disruptive incidents, including:

- Business Resilience – identification and protection of critical business services and supporting processes
- Incident Management – coordinated response to operational disruptions to stabilize and restore services
- Technology Resilience – disaster recovery and technology continuity capabilities supporting critical systems

These capabilities are supported by foundational management processes that enable consistent implementation across the organization

Risk Assessment and Annual Review

As part of its Enterprise Risk Management (ERM) program, DIRECTV conducts an annual assessment of business continuity and disaster recovery risks. Senior leaders evaluate the potential impact and likelihood of disruptive events and determine whether additional mitigation or management actions are required.

The results of this assessment inform leadership priorities and continuity initiatives for the upcoming year. Where risks are identified as significant, deeper analysis and targeted mitigation actions are incorporated into DIRECTV's business continuity activities.

Continuous Improvement

DIRECTV maintains a strong culture of continuous improvement and routinely validates its readiness through structured testing and review activities. Cross-business unit tabletop exercises are conducted to test response capabilities, validate roles and responsibilities, and identify improvement opportunities.

Following significant incidents or exercises, After-Event Reviews are performed to capture lessons learned. Improvement opportunities are documented, prioritized, and incorporated into implementation plans that are reviewed with senior leadership to drive enterprise-level resilience enhancements.

Commitment to Customers and Partners

DIRECTV is committed to maintaining the availability of critical services and minimizing disruption to customers and partners during adverse events. Through its ISO 22301-aligned BCMS, DIRECTV continuously strengthens its ability to respond to, recover from, and adapt to disruptive incidents.

BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) GOVERNANCE

Governance and Oversight

DIRECTV maintains a multitiered BCMS governance structure that provides enterprise-wide oversight, accountability, and alignment. Governance begins at the Executive Committee and Senior Leadership level, where business continuity priorities, policies, and standards are established. These expectations are communicated across the organization to enable consistent adoption and execution at the operational level.

To ensure alignment, effectiveness, and continuous improvement, governance activities are reviewed on a regular cadence across leadership and working teams, including:

- Executive level reviews to identify enterprise-level risks and set strategic priorities
- Cross-business unit exercises to validate readiness and response capabilities
- Leadership reviews to ensure alignment on focus areas and preparedness objectives
- Operational working sessions to support scenario planning and plan maintenance

This structure ensures continuity objectives remain aligned with business priorities and evolving risk conditions.

Enterprise Risk Management (ERM)

Business continuity is integrated into DIRECTV's broader ERM framework. On an annual basis, senior leaders participate in an ERM assessment that evaluates risks relevant to their respective business units. Risks are assessed based on potential impact (including financial, operational, regulatory, strategic, and reputational considerations) and likelihood.

Risk assessment results are consolidated and reviewed with the Executive Committee to identify top enterprise risks. For newly ascending or emerging high-priority risks, deeper analysis is conducted to confirm contributing factors and define appropriate mitigation strategies, such as risk acceptance, avoidance, reduction, or sharing. Action plans and controls are developed to address material residual risks and strengthen enterprise resilience.

Crisis Management

Crisis Management provides the governance framework for responding to high impact, low probability events that may threaten DIRECTV's people, operations, customers, or reputation. The crisis management process is tightly integrated with Incident Management to ensure that potential crisis level events are identified and escalated quickly by teams closest to the incident.

When crisis criteria are met, a cross-functional senior leadership team is convened to assess the situation and determine the appropriate response strategy. Where required, the Executive Committee is engaged to support enterprise-level decisions. A dedicated coordination function oversees execution of the response plan across internal teams and external stakeholders to ensure timely, consistent, and effective action.

Corporate Communications

Corporate Communications is a critical component of DIRECTV's BCMS governance, enabling clear, timely, and coordinated communication before, during, and after disruptive events. Communications support preparedness by developing crisis communication plans, defining escalation paths, and maintaining pre-approved messaging aligned with business continuity and crisis response objectives.

In the event of an incident or crisis, Corporate Communications works closely with Crisis Management and Incident Response teams to deliver consistent updates to employees, customers, partners, and external stakeholders. Effective communication supports informed decision-making, protects trust and reputation, and reinforces confidence in DIRECTV's ability to maintain continuity of service during periods of uncertainty.

BUSINESS RESILIENCE

Business Resilience focuses on ensuring DIRECTV can continue delivering its most critical services during disruptive events by proactively identifying what matters most to the business and preparing continuity strategies in advance. This capability emphasizes understanding critical value streams, prioritizing essential processes, and enabling flexible operating models to reduce customer and business impact when disruptions occur.

Critical Process Identification and Dependency Mapping

DIRECTV's Business Architecture capability provides the foundation for Business Resilience by establishing a shared understanding of enterprise business capabilities and how they support strategic objectives. A baseline capability map serves as a common taxonomy that connects business services, applications, and operational processes across the organization.

Using this baseline, DIRECTV performs Dependency Mapping to identify and prioritize the most critical end-to-end processes that deliver value to customers and support revenue-generating activities. This approach enables the organization to focus resilience planning on the processes and services with the greatest operational, financial, and reputational impact, rather than treating all processes equally. Insights from Dependency Mapping inform continuity strategies, dependency awareness, and investment prioritization.

Business Continuity Planning (BCP)

DIRECTV's BCP is aligned with ISO 22301 and is designed to sustain operations during significant disruptions such as cyber incidents, natural disasters, or third-party failures. Continuity strategies address people, processes, and technology, and are tailored to support the continuation of critical business services identified through value stream and impact analysis.

Close coordination with the Video Outage Management (VOM) team provides early operational signals, validates whether issues are real, and assesses customer and business impact. This impact awareness ensures that escalation and response decisions are grounded in business relevance and aligned with continuity priorities before formal incident activation. Should it be needed, DIRECTV has alternative communication and collaboration tools in place for internal operations during disruptions.

Furthermore, DIRECTV operates using a combination of internal teams and strategic partners. This diversified operating model strengthens resilience by allowing resources, workloads, and customer interactions to be shifted when normal operations are disrupted. If a strategic partner experiences an outage or work stoppage, DIRECTV can reroute work or leverage alternate teams to maintain service continuity.

Workforce Safety and Readiness – DIRECTV SAFE

Protecting employees is a foundational element of Business Resilience. The DIRECTV SAFE (Safety Alerts for Employees) program is designed to monitor weather-related and emergency safety risks affecting employees across the enterprise and to enable rapid accountability of our employees' well-being during disruptive events.

DIRECTV SAFE leverages third-party monitoring and established escalation criteria to identify events that may impact employee safety. When an event meets SAFE alert thresholds, employees in affected areas receive notifications through multiple channels, including text messages, automated phone calls, and email. Employees are prompted to report their status, enabling the organization to quickly account for its workforce and identify individuals who may need assistance.

The DIRECTV SAFE program supports leadership decision-making during disruptive events, enables timely engagement of support resources, and helps ensure employee safety while business continuity actions are executed. SAFE activities are closely coordinated with Business Continuity, Incident Management, and Crisis Management teams when broader operational or enterprise-level response is required.

INCIDENT MANAGEMENT

Incident Management is the execution arm of DIRECTV's resilience framework, responsible for the rapid identification, escalation, coordination, and resolution of disruptions that materially impact customers, agents, or business operations. While Business Resilience defines what must be protected and prioritized, Incident Management focuses on how the organization responds in real time to stabilize operations and restore services.

Incident Detection and Escalation

DIRECTV's Incident Management ecosystem integrates operational monitoring and business impact validation to ensure early visibility into emerging issues. Capabilities such as Video Outage Management identify potential service disruptions through multiple intake channels and validate impact severity using business-aligned criteria.

When predefined thresholds are met, incidents are escalated into a structured Major Incident Management process, ensuring timely engagement of technical teams, operational leaders, and executive stakeholders. This integration ensures that only validated, material incidents trigger enterprise-level response, reducing noise while maintaining speed and accuracy.

Major Incident Management Operating Model

Once activated, Major Incident Management follows a disciplined operating model designed to support rapid coordination and recovery. This model includes formal response bridges, technical and management escalations, severity confirmation, stakeholder communications, service restoration validation, and scheduling of root cause analysis.

Defined service level expectations govern response behaviors, including rapid alerting, on-call acknowledgement, timely initiation of response bridges, regular status updates, and early leadership engagement for high-severity events. This structure ensures accountability, transparency, and executive awareness throughout the incident lifecycle.

Governance, Metrics, and Continuous Improvement

Each major incident is tracked using standardized attributes such as severity, duration, impacted services, and business impact. These data support trend analysis, Key Performance Indicators (KPI) reporting, and identification of systemic risks. After-Event Reviews and root cause analyses are performed to capture lessons learned and provide feedback into both Incident Management improvements and Business Resilience planning, strengthening future preparedness and reducing repeat events.

How Business Resilience and Incident Management Work Together

Business Resilience and Incident Management are intentionally interconnected. Business Resilience defines critical services, continuity priorities, and acceptable impact thresholds, while Incident Management operationalizes those priorities during live events.

- Business Resilience provides the lens for impact and prioritization
- Incident Management provides the mechanism for response and recovery
- Feedback from incidents continuously informs resilience planning

Together, these capabilities enable DIRECTV to respond quickly, communicate clearly, recover effectively, and continuously strengthen its ability to protect customers, revenue, and brand trust during disruptive events.

TECHNOLOGY RESILIENCE

Technology Resilience ensures that DIRECTV's critical technology platforms, infrastructure, and data are protected, recoverable, and capable of supporting essential business services during disruptive events. This capability focuses on preventing technology failures where possible, detecting and responding to issues quickly, and restoring services in a controlled and prioritized manner when disruptions occur.

Technology Resilience is fully integrated with Business Continuity, Incident Management, and Crisis Management to ensure technology recovery efforts are aligned with business priorities and customer impact.

Cybersecurity Operations

DIRECTV's Cybersecurity program underpins the company's Business Continuity approach. Security controls follow the DIRECTV Official Security Standard (DOSS), which is aligned with ISO/IEC 27001:2022 and the NIST Cybersecurity Framework 2.0. Cyber resilience is strengthened through continuous monitoring, vulnerability identification and patch management, secure by design practices, and regular testing and exercises.

Security operations are tightly integrated with Business Continuity and Disaster Recovery to ensure that critical services are prioritized for restoration during technology disruptions. In the event of a major security or technology incident, DIRECTV's Incident Response Protocol enables rapid containment, coordinated stakeholder communication, and compliance-aware decision-making. Lessons learned from incidents are systematically incorporated back into security controls and resilience plans to continuously reduce risk.

To support end-to-end service continuity, DIRECTV extends security expectations to its suppliers through the Supplier Information Security Requirements (SISR). These requirements mandate comparable safeguards, including access control, encryption, logging, and timely remediation, to help manage third-party risk and strengthen ecosystem resilience.

IT Disaster Recovery Program

Disaster Recovery (DR) is a core component of DIRECTV's Information Technology Resilience capability and is designed to protect all or part of the company's technology operations in the event of a disruptive incident. The DR program supports recovery from cyber incidents, data loss, power outages, natural disasters, and other technology-related disruptions, with the goal of minimizing business impact and restoring services in a predictable manner.

Key components of DIRECTV's Disaster Recovery program include:

- Asset and Application Identification
  Technology assets, applications, and tools deployed in the DIRECTV environment are identified and recorded in configuration management repositories, with unique identifiers assigned to support ownership, dependency awareness, and recovery planning.

- Business Impact Analysis (BIA)
  Application and asset owners complete BIAs to define Recovery Time Objectives (RTOs) and Recovery

Point Objectives (RPOs). BIAs also capture interdependencies, functional criticality, and business impact, enabling prioritization and sequencing of recovery activities.

- Recovery Strategy and Planning
  Disaster Recovery (DR) strategies are selected based on business criticality, architectural design, and recovery objectives. Documented DR plans outline recovery architectures, procedures, and responsibilities required to restore services during a disruptive event.

- Testing and Exercising
  DR plans are validated through functional and tabletop exercises to assess readiness, identify gaps, and improve response effectiveness.

- Maintenance and Continuous Improvement
  DR plans and test results are maintained, reviewed, and updated regularly. Lessons learned from exercises and real incidents are incorporated to strengthen recovery capabilities over time.

Video Engineering Disaster Recovery Program

Disaster Recovery is a foundational responsibility within DIRECTV Engineering, supporting the delivery of reliable satellite and streaming services. Engineering recovery efforts are focused on sustaining operations and restoring services following infrastructure failures, cyber incidents, power outages, or natural disasters, while enabling safe and coordinated response across Engineering teams.

DIRECTV Engineering operates a hybrid technology environment that includes on-premises facilities and public cloud platforms. Services supporting satellite and streaming operations are hosted across multiple geographically distributed locations, including data centers as well as cloud environments such as AWS. Recovery approaches are tailored to the design and resiliency characteristics of each service rather than relying on a single uniform model.

Core elements of the Engineering Disaster Recovery approach include:

- Architectural Resiliency
  Where feasible, services are designed with inherent resiliency. Cloud-based services leverage multi-Availability Zone deployments to tolerate localized failures. Select services maintain regional redundancy through cold standby or redeployment capabilities. Satellite services typically operate from designated primary sites, with geographic diversity incorporated where practical.

- Service Ownership and Documentation
  Engineering teams maintain clear ownership of services and infrastructure components. Runbooks document recovery procedures, deployment steps, and troubleshooting guidance to support effective response during disruptive events.

- Recovery Planning and Execution
  Recovery strategies are defined based on service architecture, operational dependencies, and business criticality. During incidents, engineering teams execute established runbooks and coordination practices to restore services in a controlled and prioritized manner.

FOUNDATIONAL ENABLERS

Foundational Enablers provide the enterprise-wide capabilities, controls, and governance structures that allow DIRECTV's BCMS to operate consistently, securely, and at scale. These enablers support innovation, protect data, manage third-party risk, and ensure that resilience capabilities are sustainable and audit-ready.

Generative AI

DIRECTV's Generative AI (GenAI) initiative is designed to accelerate innovation, strengthen competitiveness, and unlock material value across the enterprise. The program focuses on three primary opportunity areas: differentiated customer experiences, new and optimized revenue streams, and modernized internal processes. Early use cases include virtual agents, personalized marketing, content intelligence, code generation, financial analysis, and HR automation—each aimed at improving customer satisfaction, reducing operational friction, and enabling faster, more informed decision-making.

To ensure safe, ethical, and effective adoption, DIRECTV has established a formal governance framework anchored by a centralized intake process and a cross-functional AI Strategy Steering Committee. This committee evaluates proposed use cases, conducts risk assessments, and ensures alignment with legal, privacy, security, and technical guardrails. All GenAI initiatives follow a structured lifecycle management approach, with enhanced scrutiny applied to medium and high-risk use cases. This framework balances speed and control—enabling innovation while protecting customer data, minimizing legal and reputational risk, and ensuring enterprise-wide consistency.

Data Governance

DIRECTV's Data Governance program strengthens the company's data protection and resilience posture by ensuring that access to data is intentional, time-bound, and aligned to a clear business purpose. The program reduces risk by standardizing data onboarding, offboarding, and access reviews across employees, vendors, and partners, helping to prevent unauthorized or lingering access.

Data Governance also enables DIRECTV to demonstrate effective controls through audit-ready evidence, reducing reliance on manual or reactive security measures. By establishing clear ownership, access controls, and accountability across the data lifecycle, the program supports operational resilience while enabling the responsible use of enterprise data.

Privacy

DIRECTV is committed to protecting personal and sensitive information by limiting collection to what is necessary, maintaining reasonable security measures, and preventing unauthorized access or disclosure, as required under applicable state privacy laws. We honor consumer rights to access, correct, delete, and obtain their data, and to opt out of targeted advertising, data sales, and profiling that may result in unfair, deceptive, or discriminatory outcomes. Sensitive personal information is processed only with appropriate consent or lawful purpose, supported by required assessments that evaluate risks and safeguards. We ensure transparent notices, prohibit coercive or misleading consent practices, and require third-party partners to apply strong privacy and security controls. Additionally, we have internal policies that are aligned with our

external Privacy Policy to maintain consistency and accountability across the organization. For more information, read the DIRECTV Privacy Policy.

Third-party Risk Management

As DIRECTV increasingly relies on third-party suppliers to support critical business operations, the company remains committed to protecting its data, customers, and brand. DIRECTV's Third-party Risk Management (TPRM) program is designed to safeguard the confidentiality, integrity, and availability of information while supporting regulatory compliance and operational resilience.

The TPRM program provides structured oversight of third-party relationships to ensure suppliers operate securely, responsibly, and in alignment with DIRECTV's corporate standards and regulatory expectations. The program emphasizes trust, risk reduction, and visibility to support informed decision-making across the vendor lifecycle.

Key TPRM activities include:

- Comprehensive onboarding assessments to evaluate the supplier's overall stability, risk profile, and potential brand / reputational impact, ensuring appropriate controls and monitoring are in place prior to engagement
- Annual attestations requiring suppliers with system/data access to confirm continued effectiveness of controls, including security posture
- Targeted audits initiated when elevated risk, changes in scope, or environmental factors are identified
- Structured offboarding processes to ensure secure termination of access, confirmation of data retention or destruction requirements, and disabling of credentials and system access

Through these controls, DIRECTV strengthens resilience across its extended ecosystem and reduces exposure to third-party related disruptions.

How Foundational Enablers Support the BCMS

Together, Generative AI Governance, Data Governance, Privacy by Design, and Third-party Risk Management form the foundation of DIRECTV's BCMS. These enablers ensure that innovation is responsible, data is protected, partners are accountable, and resilience capabilities are sustainable over time—supporting consistent execution across Governance, Business Resilience, Incident Management, and Technology Resilience.