BGP Network Security Audit Checklist

Organization: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Audit Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Auditor: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Audit Scope: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Pre-Audit Planning & Documentation

## Scope Definition

* [ ] Autonomous systems within audit scope identified and documented
* [ ] External BGP relationships inventory completed
* [ ] Internal BGP topology mapped and verified
* [ ] Compliance frameworks requiring network controls identified (SOC 2, PCI DSS, NIST, etc.)
* [ ] Audit evidence collection requirements established
* [ ] Technical resources and expertise availability confirmed

## Stakeholder Coordination

* [ ] Network operations team interviewed and available
* [ ] Security team representatives identified and engaged
* [ ] Compliance officers briefed on BGP audit scope
* [ ] Vendor/service provider contacts documented
* [ ] Historical incident records and documentation collected

# Phase 1: BGP Infrastructure Assessment

## BGP Topology and Relationships

* [ ] All BGP peer relationships documented with business justification
* [ ] Network topology diagrams current and accurate
* [ ] Trust boundaries between autonomous systems clearly defined
* [ ] Legacy or forgotten BGP sessions identified
* [ ] Peer relationship change control processes documented

Findings: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Risk Level: [ ] Critical [ ] High [ ] Medium [ ] Low

## Route Advertisement Analysis

* [ ] Current route advertisements match documented routing policies
* [ ] No internal/management subnets advertised publicly
* [ ] Route aggregation policies properly implemented
* [ ] Route specificity appropriate for security requirements
* [ ] Historical route advertisement patterns analyzed for anomalies

Critical Finding - Route Leaks Detected:

* [ ] Internal routes advertised to external peers: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* [ ] Over-specific route advertisements identified: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* [ ] Unauthorized route announcements discovered: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Findings: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Risk Level: [ ] Critical [ ] High [ ] Medium [ ] Low

# Phase 2: Authentication and Session Security

## BGP Session Authentication

* [ ] All BGP sessions use authentication (no clear-text sessions)
* [ ] MD5 authentication passwords meet organizational complexity requirements
* [ ] Authentication keys unique per session (no shared keys across multiple peers)
* [ ] Key rotation schedule defined and followed
* [ ] Authentication failure logging enabled and monitored

Critical Findings - Authentication Weaknesses:

* [ ] Unauthenticated BGP sessions identified: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* [ ] Weak/default passwords detected: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* [ ] Shared authentication keys found: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* [ ] Overdue key rotations identified: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Findings: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Risk Level: [ ] Critical [ ] High [ ] Medium [ ] Low

## Route Origin Validation (RPKI)

* [ ] RPKI validation infrastructure deployed and operational
* [ ] Route Origin Authorizations (ROAs) created for all owned prefixes
* [ ] RPKI certificate chain validation working properly
* [ ] RPKI validation failures monitored and alerted
* [ ] Procedures exist for handling RPKI invalid routes

RPKI Implementation Status:

* [ ] Fully implemented with monitoring
* [ ] Partially implemented - needs completion
* [ ] Planning phase only
* [ ] Not implemented - immediate risk

Findings: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Risk Level: [ ] Critical [ ] High [ ] Medium [ ] Low

# Phase 3: BGP Security Monitoring and Detection

## Real-Time Monitoring Capabilities

* [ ] All organization-owned prefixes monitored for unauthorized announcements
* [ ] Route hijacking detection system deployed and operational
* [ ] Route leak detection capabilities implemented
* [ ] BGP monitoring integrated with SIEM/security operations
* [ ] Historical BGP data retained for forensic analysis

Monitoring Coverage Assessment:

* [ ] 100% of owned prefixes covered
* [ ] 75-99% coverage with gaps identified
* [ ] 50-74% coverage - significant gaps exist
* [ ] <50% coverage - inadequate monitoring

Findings: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Risk Level: [ ] Critical [ ] High [ ] Medium [ ] Low

## Alert Management and Response

* [ ] BGP security alerts properly classified and prioritized
* [ ] Escalation procedures defined for different BGP incident types
* [ ] 24/7 availability of BGP expertise for incident response
* [ ] Alert tuning implemented to minimize false positives
* [ ] Response time objectives defined for BGP security incidents

Alerting Effectiveness:

* [ ] False positive rate <5% - well tuned
* [ ] False positive rate 5-15% - needs improvement
* [ ] False positive rate >15% - poorly tuned/alert fatigue risk

Findings: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Risk Level: [ ] Critical [ ] High [ ] Medium [ ] Low

# Phase 4: Incident Response and Business Continuity

## BGP Incident Response Procedures

* [ ] Documented procedures exist for BGP hijacking scenarios
* [ ] Route leak incident response playbooks available
* [ ] Coordination procedures with ISPs and peering partners defined
* [ ] Emergency contact information current and accessible
* [ ] Post-incident review procedures established

## Business Continuity Planning

* [ ] BGP attack scenarios included in business continuity plans
* [ ] Alternative connectivity options identified and tested
* [ ] Communication templates for BGP incidents prepared
* [ ] Regulatory notification procedures for BGP-related data breaches defined
* [ ] Customer communication plans for BGP service disruptions ready

Findings: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Risk Level: [ ] Critical [ ] High [ ] Medium [ ] Low

# Phase 5: Historical Analysis and Trend Assessment

## BGP Change Analysis

* [ ] Historical BGP routing changes documented and analyzed
* [ ] Baseline measurements established for normal BGP behavior
* [ ] AS path length changes tracked and evaluated
* [ ] Route flapping incidents identified and investigated
* [ ] Performance correlation with BGP changes analyzed

## Security Incident History

* [ ] Previous BGP hijacking incidents documented
* [ ] Route leak events and impact assessed
* [ ] Lessons learned from past incidents incorporated into procedures
* [ ] Trend analysis completed for recurring BGP issues
* [ ] Root cause analysis performed for major BGP incidents

Historical Risk Indicators:

* [ ] No significant BGP incidents in past 12 months
* [ ] 1-2 minor incidents with quick resolution
* [ ] 3-5 incidents indicating systemic issues
* [ ] >5 incidents or major service impact - high risk pattern

Findings: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Risk Level: [ ] Critical [ ] High [ ] Medium [ ] Low

# Phase 6: Compliance and Regulatory Assessment

## SOC 2 Compliance Mapping

* [ ] BGP security controls mapped to SOC 2 Common Criteria
* [ ] Logical access controls include BGP authentication requirements
* [ ] System monitoring covers BGP security events
* [ ] Change management processes include BGP configuration changes
* [ ] Availability monitoring includes route hijacking detection

## PCI DSS Network Segmentation

* [ ] Cardholder data environment networks not publicly routable via BGP
* [ ] BGP monitoring covers payment processing network routes
* [ ] Network segmentation validation includes BGP route analysis
* [ ] BGP security controls documented for PCI DSS compliance
* [ ] BGP attack scenarios included in penetration testing scope

## Other Regulatory Requirements

* [ ] Data localization requirements considered in BGP routing policies
* [ ] Industry-specific network security requirements addressed
* [ ] International data transfer restrictions reflected in routing configurations
* [ ] Regulatory reporting requirements for network incidents include BGP events

Compliance Gaps Identified:

* [ ] Critical compliance violations requiring immediate remediation
* [ ] Minor gaps that should be addressed in next compliance cycle
* [ ] Documentation deficiencies affecting audit evidence

Findings: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Risk Level: [ ] Critical [ ] High [ ] Medium [ ] Low

# Risk Assessment and Overall Scoring

## Vulnerability Risk Matrix

Critical Vulnerabilities (Score 9-10):

* [ ] No BGP authentication on external sessions
* [ ] Public route leaks exposing sensitive systems
* [ ] No BGP monitoring capability
* [ ] Multiple recent hijacking incidents

High Vulnerabilities (Score 7-8):

* [ ] Weak BGP authentication (default/shared passwords)
* [ ] Limited monitoring coverage (<75% of prefixes)
* [ ] No RPKI implementation
* [ ] Inadequate incident response procedures

Medium Vulnerabilities (Score 4-6):

* [ ] Authentication gaps on some sessions
* [ ] Partial RPKI deployment
* [ ] Monitoring with significant false positives
* [ ] Documented procedures but limited testing

Low Vulnerabilities (Score 1-3):

* [ ] Strong authentication with minor implementation gaps
* [ ] Comprehensive monitoring with room for improvement
* [ ] Good procedures with regular testing and updates

Overall BGP Security Risk Score: \_\_\_\_\_ / 10

# Business Impact Assessment

## Financial Impact Estimation

* [ ] Service outage costs calculated: $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ per hour
* [ ] Incident response costs estimated: $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ per incident
* [ ] Regulatory fine exposure assessed: $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ potential
* [ ] Customer churn risk quantified: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_% revenue impact
* [ ] Reputation damage costs considered: $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ estimated

## Compliance Impact

* [ ] SOC 2 audit implications identified
* [ ] PCI DSS compliance gaps documented
* [ ] Industry-specific regulatory impacts assessed
* [ ] Contract violation risks with customers/partners evaluated

Total Estimated Annual Risk Exposure: $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Remediation Recommendations and Priorities

## Immediate Actions Required (0-30 days)

* [ ] Enable authentication on all unauthenticated BGP sessions
* [ ] Stop advertising internal routes publicly
* [ ] Implement basic BGP monitoring for owned prefixes
* [ ] Document emergency contact procedures

## Short-term Improvements (1-6 months)

* [ ] Deploy comprehensive BGP monitoring system
* [ ] Implement RPKI validation infrastructure
* [ ] Develop BGP incident response procedures
* [ ] Conduct BGP security awareness training

## Medium-term Strategic Actions (6-18 months)

* [ ] Complete RPKI ROA creation for all prefixes
* [ ] Integrate BGP monitoring with SIEM systems
* [ ] Establish formal change control for BGP configurations
* [ ] Conduct regular BGP security assessments

## Long-term Architecture Considerations (12+ months)

* [ ] Evaluate modern networking alternatives to BGP
* [ ] Assess identity-based networking solutions
* [ ] Consider strategic architecture changes to eliminate BGP risks
* [ ] Develop comprehensive network security program

# Strategic Decision Framework

## Current State Assessment

BGP Security Maturity Level:

* [ ] Advanced: Comprehensive controls, monitoring, and response capabilities
* [ ] Developing: Basic controls in place with improvement needed
* [ ] Initial: Limited BGP security measures implemented
* [ ] Ad-hoc: No systematic approach to BGP security

## Resource Requirements for BGP Security

Estimated Annual Investment Required:

* [ ] Personnel costs: $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (specialized expertise)
* [ ] Technology costs: $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (monitoring tools, RPKI infrastructure)
* [ ] Training costs: $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (ongoing education and certification)
* [ ] Operational costs: $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (incident response, coordination)

Total Annual BGP Security Investment: $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Alternative Architecture Consideration

* [ ] Current BGP complexity acceptable given security requirements
* [ ] BGP security investment justified by business requirements
* [ ] Exploring alternatives to reduce complexity and eliminate risks
* [ ] Ready to consider identity-based networking to eliminate BGP vulnerabilities

# Audit Conclusion

Overall Assessment: [ ] Satisfactory [ ] Needs Improvement [ ] Unsatisfactory

Key Findings Summary:

Critical Actions Required:

Strategic Recommendation:

[ ] Invest in comprehensive BGP security tools and processes

[ ] Eliminate BGP risks through modern networking architecture

Auditor Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Next Audit Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This checklist can be used standalone or as a supplement to comprehensive network security audit procedures. For organizations seeking to eliminate BGP vulnerabilities rather than manage them, consider evaluation of modern networking alternatives like [noBGP](https://www.nobgp.com/).