Sociology & Cultural Research Review (SCRR)
Available Online: https://scrrjournal.com
Print ISSN: 3007-3103 Online ISSN: 3007-3111
Platform & Workflow by: Open Journal Systems

Operationalizing the AYAZ KHAN Model: Institutional Guidance for Courts, Investigators, Prosecutors, Regulators, and Prevention Bodies in Pakistan

Mr. Ayaz Khan
Ph.D (Law) Research Scholar, Department of Law, Abdul Wali Khan University Mardan, Khyber Pakhtunkhwa, Pakistan
ayazkhan.law@awkum.edu.pk
Muhammad Kashif Irshad
Additional Director General, Khyber Pakhtunkhwa Centre of Excellence on Countering Violent Extremism, Pakistan
kashifkhankhail@hotmail.com

ABSTRACT
Pakistan's growing exposure to digitally mediated extremism requires institutional responses that are coordinated, lawful, and practically implementable. Building on a broader socio-legal doctoral study, this article translates the AYAZ KHAN Model into an institutional guidance framework for future application by investigators, prosecutors, courts, policy bodies, regulators, and rehabilitation actors. The article argues that model effectiveness depends less on rhetorical endorsement than on operational design: clear statutory drafting, differentiated thresholds, validated assessment protocols, digital evidence standards, inter-agency case routing, judicial oversight, and structured rehabilitation pathways. It sets out a practical roadmap for implementation through legislative reform, institutional restructuring, phased capacity building, monitoring, and cross-border cooperation. The article also allocates institution-specific responsibilities to the Federal Investigation Agency, Counter Terrorism Departments, prosecutors, the judiciary, NACTA, a proposed Digital Radicalization Prevention Authority, police, and community-based prevention systems. Rather than treating digital radicalisation as a single-security problem, the article shows how institutions can apply the model in future through a graduated architecture that preserves legality while improving prevention and operational coherence.
The central claim is that institutional guidance must be anchored in due process, transparent standards, and measurable implementation benchmarks if Pakistan is to build a sustainable response to online extremism.

***Keywords**: Digital Radicalisation, Institutional Coordination, Pakistan, Digital Evidence, Rehabilitation, Online Extremism*

Introduction

The future value of any legal model lies in whether institutions can apply it consistently. Pakistan's challenge with digital radicalisation is therefore not only conceptual but administrative and operational. Even the most carefully designed framework will fail if investigators cannot route cases properly, prosecutors cannot convert digital traces into admissible proof, courts cannot assess technical evidence, policy institutions cannot coordinate prevention, and rehabilitation systems remain detached from criminal-justice decision-making. This article

addresses that implementation problem by translating the AYAZ KHAN Model into institutional guidance for future use.

The need for such guidance is acute. Digital radicalisation now unfolds across open platforms, private messaging systems, cross-border infrastructures, and rapidly changing recommendation environments. At the same time, Pakistan's legal institutions continue to operate through fragmented statutory tools and separate organizational mandates. Rights groups have criticized legal vagueness and procedural weakness in cyber regulation, while NACTA has highlighted the importance of prevention and whole-
of-society engagement (Center for Justice, 2023; Digital Rights Foundation, 2025; NACTA, n.d.-a). Yet there remains no practical implementation architecture that aligns these concerns.

This article therefore asks how institutions can practically seek guidance from and apply the AYAZ KHAN Model in future. It proceeds in six parts. First, it restates the model as an implementation framework rather than a theoretical one. Second, it outlines legislative and regulatory reforms needed to operationalize the model. Third, it allocates institution-specific responsibilities. Fourth, it proposes implementation pathways for assessment, evidence, and zoned response. Fifth, it identifies training, monitoring, and international-cooperation needs. Sixth, it concludes with a phased roadmap for future application.

From Normative Model to Operational Framework

The AYAZ KHAN Model consists of eight integrated elements, but institutions need to treat them as workflow disciplines rather than abstract principles. Assessment identifies and structures risk information. Yardsticks of legal threshold classify conduct by seriousness and proximity. Authentication and attribution ensure digital proof is reliable. Zoned intervention links assessed risk and legal thresholds to proportionate state responses. Knowledge-led coordination provides shared procedures and case continuity. Human-rights safeguards and accountability mechanisms control discretion. Rehabilitation and reintegration ensure the framework is not reduced to prosecution alone.

For implementation purposes, these elements can be read as a sequence of institutional questions. What is the nature of the online conduct? How reliable is the evidence? What threshold has been crossed? Which agency leads? What level of intervention is justified? What review mechanisms apply? Does the case permit diversion or require prosecution? This sequence is important because it prevents agencies from beginning with their preferred organizational tool rather than the legal character of the conduct itself.

Institutional guidance must also reflect a basic lesson from comparative practice: digital-radicalisation governance works poorly when powers expand faster than standards. The EU's DSA, the UK's online-safety architecture, and Australia's eSafety system all show that online-harm regulation increasingly depends on explicit duties, documented processes, and review structures rather than informal discretion alone (eSafety Commissioner, n.d.; European Union, 2022; Online Safety Act 2023, 2023). Pakistan's future application of the model should proceed from the same premise.

Empirical and Documentary Basis for Institutional Guidance

The institutional guidance offered here is derived from a wider doctoral study that combined doctrinal analysis with qualitative interviews across Pakistan's criminal-justice and policy landscape. Twenty-three respondents were purposively selected from the judiciary, prosecution services, police and counterterrorism bodies, the FIA, academia, policy institutions, defense

practice, and rehabilitation-oriented settings. This design matters because institutional guidance cannot be credibly written from legislation alone; it must reflect how agencies actually understand thresholds, evidence, and operational constraints.

The broader study found that institutions often recognized the same problem while describing it in incompatible languages. Investigators focused on patterns of escalation, platform migration, and operational timing. Prosecutors focused on admissibility and provability. Judges focused on legality, attribution, and constitutional restraint. Prevention actors focused on vulnerability and non-penal engagement. The AYAZ KHAN Model was derived to stabilize these institutional differences without erasing them. The implementation guidance in this article therefore aims to convert those differences into a common operating architecture.

The documentary base also included comparative legal materials and official policy sources, including Pakistan's cyber and counterterrorism laws, NACTA prevention materials, rights-based critiques of PECA, and international regulatory models. These sources support the practical recommendations made below, especially on institutional coordination, digital-evidence governance, and the need for reviewable preventive structures.

Legislative and Regulatory Guidance

The first practical requirement is legislative consolidation. Pakistan should not attempt to operationalize the model solely through administrative circulars or ad hoc inter-agency arrangements. A dedicated Digital Radicalization Prevention Act would be the clearest vehicle for implementation. Such legislation should define objectives, clarify core terms, establish institutional mandates, create assessment and review procedures, set evidentiary standards, and embed rehabilitation pathways.

Drafting should follow six principles. First, precision: the law must distinguish protected expression, ideological advocacy, unlawful incitement, facilitation, recruitment, and terrorism-linked conduct. Second, proportionality: responses should correspond to the model's graduated thresholds. Third, procedural safeguards: coercive measures should require clear authorization, review, and challenge rights. Fourth, institutional clarity: statutes must define the roles of the FIA, CTDs, prosecutors, courts, police, NACTA, and any new coordinating body. Fifth, rehabilitation integration: diversion and reintegration should have an explicit legal basis. Sixth, international cooperation: the framework should address cross-border evidence, platform engagement, and digital-financing risks (FATF, 2021).

Existing law should also be amended. PECA should be revised to improve definitional clarity and incorporate explicit digital-evidence provisions. ATA should clarify its digital application and permit structured rehabilitation where legally appropriate. The Qanun-e-Shahadat Order and criminal procedure rules should be updated to address authentication, metadata, expert testimony, and digital chain of custody. Without these amendments, the model will remain conceptually attractive but procedurally underpowered.

Institution-Specific Roles and Future Guidance

Future application of the model depends on role clarity. The FIA Cyber Crime Wing should serve as the primary technical gateway for digital detection, forensic preservation, platform liaison, and cross-border evidence requests. Its function under the model is not to monopolize all cases but to anchor the authentication and attribution component. FIA units should therefore develop specialist capability in extremist-content analysis, encrypted-platform investigation, metadata preservation, and mutual legal-assistance procedures.

Counter Terrorism Departments should lead on cases that meet higher threshold indicators involving incitement, facilitation, recruitment, financing, or operational linkage. Their digital units should work from shared handover protocols with the FIA so that cyber-origin cases do not lose evidentiary continuity when they transition into terrorism-oriented investigation. This is especially important where a case begins with online propaganda exposure and later reveals recruitment or attack preparation.

Prosecution services should establish specialist teams in major jurisdictions to handle model-based cases. Their future guidance role is to translate assessed conduct into legally sustainable charges and to police overreach internally. Prosecutors should ask whether the evidence actually supports the relevant threshold, whether digital attribution is defensible, whether non-penal referral is available, and whether constitutional standards can be met in court.

The judiciary should remain the principal guardian of the model's legality. Courts should require the state to demonstrate threshold crossing, evidentiary integrity, proportionality, and procedural fairness at each coercive stage. Judicial academies should develop bench books on digital evidence, encrypted communications, platform architecture, and threshold analysis so that judges are not forced to improvise technical reasoning case by case.

NACTA should focus on strategic policy, research, community engagement, and oversight of prevention and rehabilitation programming. It should not absorb investigative functions that belong elsewhere. Instead, NACTA's institutional guidance role is to support prevention metrics, inter-agency learning, national-level trend analysis, and evidence-based policy adaptation.

Police, universities, schools, prison authorities, and community organizations also have future roles. They should function as referral and early-warning nodes rather than coercive substitutes. Under the model, not every concern moves directly into criminal process. Some require referral into assessment, counseling, family engagement, educational support, or monitored disengagement pathways.

Table 1 ***Illustrative Institutional Responsibilities Under the AYAZ KHAN Model***

Institution	Lead Functions	Key Safeguards/Outputs
FIA Cyber Crime Wing	Digital detection, platform liaison, preservation, metadata and forensic extraction	Standardized forensic protocols and lawful cross-border evidence requests
Counter Terrorism Departments	Lead on Y3-Y4 investigations, online recruitment/facilitation inquiries, coordinated operational response	Case-routing rules, warrant discipline, and evidentiary continuity
Prosecution services	Threshold review, charge selection, expert-evidence management, appellate strategy	Written charging rationale and internal overreach checks
Judiciary	Review warrants, assess thresholds, test digital-	Bench books, review hearings, and published jurisprudential guidance

	evidence integrity, protect fair-trial rights	
NACTA / coordinating authority	Policy analysis, prevention oversight, data synthesis, rehabilitation quality assurance	Monitoring indicators, public reporting, and inter-agency learning
Rehabilitation providers	Counseling, mentoring, reintegration planning, monitored disengagement	Eligibility criteria, voluntariness standards, and outcome evaluation

Assessment Protocols and Case Routing

Practical implementation begins with structured assessment. The model envisages three stages: initial screening, structured professional judgment, and comprehensive case review. Future institutional guidance should formalize each stage. Initial screening should be based on legally authorized criteria and should avoid open-ended fishing. Structured professional judgment should be carried out by trained assessors using documented indicators rather than personal intuition. Comprehensive review should be multidisciplinary for significant cases and should consider context, escalation patterns, and alternative interventions.

Case routing should follow threshold logic. Y1 cases involving private extremist belief without actionable expression do not justify intervention beyond lawful intelligence retention where authorized. Y2 cases involving ideological advocacy, glorification, or non-imminent extremist expression may justify monitoring, civil remedies, platform action, or preventive engagement. Y3 cases involving facilitation, direct incitement, recruitment, or material support should transition to formal criminal process. Y4 cases involving operational preparation or participation justify full counterterrorism response. The practical strength of this routing structure is that it gives institutions a common language for decision-making.

Institutional guidance should also address reversibility. Radicalisation is dynamic, and assessed risk can escalate or de-escalate. Therefore case review should be periodic. A case initially placed in a preventive zone may require escalation if evidence of recruitment or operational linkage emerges. Conversely, successful disengagement may justify step-down, diversion, or structured closure. Without periodic review, the model risks becoming static and punitive.

Digital Evidence Standards for Future Application

No part of the model is more critical in practice than digital evidence. Future implementation should therefore prioritize a national digital-evidence protocol. That protocol should specify procedures for lawful seizure, forensic imaging, metadata preservation, hash verification, translation, contextual analysis, and secure storage. It should also distinguish between intelligence leads and court-ready evidence.

Screenshots should never be treated as self-sufficient proof when attribution is disputed. Investigators should seek device extraction, server-side confirmation where available, witness linkage, account-behaviour patterns, and expert interpretation. Encrypted-platform cases should be approached through layered methods: device forensics, subscriber information, financial trails, open-source correlation, and legally obtained cross-platform data. Pakistan's future framework must recognize that technical difficulty cannot justify evidentiary shortcuts.

Specialist forensic laboratories and certification systems are therefore essential. Judges and prosecutors need confidence that experts follow standardized methods. Defense counsel needs

a basis on which to challenge or test digital claims. A rights-compatible model requires both technical capability and adversarial fairness. This is why digital evidence reform should be treated as core implementation, not a later technical add-on.

Illustrative Institutional Workflows

A future-ready model benefits from concrete workflow examples. Consider a university student whose public posts increasingly endorse martyrdom narratives, who joins a medium-sized Telegram channel sharing extremist sermon clips, and who begins reposting material with ambiguous praise for armed struggle. Under the model, a referral from university administration or lawful cyber-monitoring would not automatically trigger prosecution. Instead, the case would move first into structured assessment. If the assessment places the conduct in Y2, the response could include preventive engagement, digital-literacy intervention, family contact where appropriate, and time-limited monitoring subject to review. Only if the evidence later showed recruitment, direct incitement, or movement toward operational activity would the case escalate to Y3 or Y4.

Now consider a second case involving an encrypted messaging administrator who manages multiple channels distributing attack glorification, logistical advice, and explicit invitations to join a proscribed organization. Here the workflow is different. The FIA's role would be immediate evidence preservation and attribution work; the CTD would assume lead investigative responsibility once facilitation indicators are established; prosecutors would assess charge framing under ATA and PECA-linked provisions; and the court would be asked to scrutinize warrants, attribution, and the link between the digital activity and terrorism-related conduct. The value of the model is that the institutional transition is planned rather than improvised.

A third scenario concerns a prison-release case. An individual previously convicted in a terrorism-related matter returns to online spaces but appears to be consuming extremist content without yet engaging others. Under current practice, authorities may respond either with broad suspicion or with no meaningful structure at all. Under the model, post-release online behaviour can be assessed using documented indicators and tied to conditional rehabilitation and reintegration planning. If the conduct remains at Y1 or low Y2, the response should remain supervisory and rehabilitative. If the person begins reconnecting with recruitment channels or coordinating with known extremist accounts, the case can be escalated transparently. This protects both public safety and due process.

These workflows illustrate a larger institutional point. Future application of the model should be organized around case pathways, not agency silos. Each pathway should specify initiating triggers, evidentiary checkpoints, threshold classification, lead and supporting institutions, review deadlines, and closure criteria. Such workflows can be codified in standing operating procedures, prosecution manuals, judicial bench books, and inter-agency memoranda. They also make training more practical because personnel can learn through decision trees and case simulations rather than abstract legal categories alone.

The same logic applies to platform engagement. Where extremist content is hosted on open platforms, the model should distinguish evidence preservation from content-removal requests, and both from user-focused intervention. Where content appears on encrypted platforms, institutions should rely on device-side forensics, subscriber information where lawfully available, financial links, and cross-platform corroboration rather than demanding impossible levels of

platform access. Institutional guidance becomes effective when it tells agencies not only what ideals to follow, but what steps to take in recurring factual situations.

Capacity Building, Financing, and Administrative Sequencing

Institutional application requires money, technology, and administrative sequencing. Reform often fails because states adopt broad mandates without resourcing the personnel and infrastructure necessary to carry them out. Pakistan's future application of the model should therefore begin with a national implementation budget covering forensic laboratories, specialist software, secure evidence storage, training modules, case-management systems, and rehabilitation partnerships. Financing should be treated as a rule-of-law investment, not merely a security expense, because weak evidence and poor coordination impose costs across the entire justice system.

Administrative sequencing should also be explicit. In the first year, the priority should be legal reform, interim protocols, and the designation of lead agencies. In years two and three, the focus should shift to specialist staffing, pilot jurisdictions, certified training, and data systems. Only after these foundations are in place should full national-scale zoned intervention and comprehensive rehabilitation pathways be activated. This sequencing reduces the risk that agencies will improvise under political pressure before standards and safeguards exist.

Capacity building must be tailored. Investigators need technical training in extraction, metadata analysis, open-source correlation, and lawful online operations. Prosecutors need case-construction workshops using real or simulated digital files. Judges need intensive short-course formats with bench materials and recurring updates as platforms and tactics evolve. Prevention practitioners need training in referral ethics, safeguarding, and documentation. Senior administrators need management training on coordination, oversight, and performance review. A single training package will not suffice because the model's demands differ by institutional role.

Administrative culture is another often neglected dimension. The model requires agencies to share information without collapsing accountability, to document decisions they may previously have taken informally, and to accept review by courts and supervisory bodies. That may require deliberate change-management strategies: leadership directives, shared templates, incentives for cooperation, and regular inter-agency case conferences. Without cultural adaptation, even well-drafted procedures may remain unused.

Judicial and Prosecutorial Decision Support

For the model to work in practice, judges and prosecutors need decision-support tools rather than general exhortations. A judicial bench guide should set out threshold questions in sequence: What is the alleged conduct? What legal category is asserted? What evidence links the conduct to the respondent or accused? What technical basis supports authenticity? What degree of risk is alleged? What warrant, restriction, or prosecution is being requested? What safeguards apply? Structured questions of this kind reduce the risk that courts will rely on broad security narratives rather than the specific legal basis of the application before them.

Prosecutorial manuals should perform a similar function. Before authorizing charges, prosecutors should complete a threshold-and-evidence memorandum summarizing the relevant yardstick, the digital-evidence chain, corroborative material, platform-specific issues, potential constitutional concerns, and reasons why a non-penal route is inadequate. Such internal documentation would strengthen accountability, improve appellate resilience, and create a body of best practice over time.

These tools also promote consistency across jurisdictions. Without them, one province or court may treat a pattern of conduct as mere extremist expression while another treats a similar pattern as criminal facilitation. Consistency does not require uniform outcomes in all cases, but it does require common reasoning structures. Decision-support materials are therefore a practical extension of the model's knowledge-led coordination component.

Zoned Intervention and Procedural Safeguards

The model's zoned response component should guide agencies away from a one-size-fits-all strategy. Zone 1 should prioritize observation, lawful referrals, family and community engagement, and digital-literacy or counseling interventions. Zone 2 should permit disruption, targeted restrictions, or intensified investigation under reviewable procedures where the risk is significant but the criminal threshold is not yet fully met. Zone 3 should be reserved for prosecutable conduct. The zones are not merely descriptive; they are safeguards against both paralysis and overreach.

Every zone should carry review obligations. Zone 1 measures should be documented and time-limited. Zone 2 actions should require higher authorization and defined challenge mechanisms. Zone 3 prosecutions should trigger full constitutional protections and strict evidentiary scrutiny. This graduated architecture operationalizes procedural justice: state power expands only as legal justification strengthens (Ashworth & Zedner, 2014; Tyler, 2003).

Future institutional guidance should also prohibit category drift, whereby lower-zone concerns are informally treated as if they were prosecutable conduct. Such drift is common in security settings and is precisely what the model is designed to prevent. The threshold should govern the response, not the level of institutional anxiety.

Rehabilitation, Reintegration, and Community Interface

Practical application of the model requires institutions to understand rehabilitation as a security and justice function rather than a charitable afterthought. Some individuals exposed to extremist ecosystems can be redirected through structured interventions involving counseling, mentoring, religious dialogue, educational support, vocational planning, or supervised reintegration. The model therefore expects formal referral pathways between criminal-justice institutions and rehabilitation providers.

Future guidance should establish standards for eligibility, voluntariness, program design, religious and psychological expertise, confidentiality, and outcome measurement. Rehabilitation should not become a coercive black box in which individuals are confined without due process. Nor should it function as a symbolic program with no measurable effect. What the model requires is evidence-based, reviewable, and culturally grounded reintegration practice.

Community engagement is equally important. Universities, local administrations, faith-based institutions, and families should be integrated carefully into non-penal pathways where appropriate. However, community engagement must not become a route for informal stigma or extra-legal punishment. Institutional guidance should therefore stress confidentiality, anti-discrimination, and documented referral criteria.

Capacity Building, Monitoring, and International Cooperation

Implementation will fail without sustained training. Investigators require advanced skills in platform analysis, digital forensics, and online undercover work within lawful boundaries. Prosecutors require expertise in charge selection, expert-evidence management, and appellate strategy. Judges require training in digital-proof assessment and platform architecture.

Prevention practitioners require competence in radicalisation indicators, safeguarding, and referral ethics. These are not optional improvements; they are preconditions for model fidelity.

Monitoring and evaluation should also be embedded from the outset. A future implementation authority should collect data on referrals, threshold classifications, case outcomes, diversion rates, acquittals based on evidentiary weakness, rehabilitation completion, recidivism indicators, and complaints concerning rights violations. These metrics would allow Pakistan to determine whether the model is actually improving coherence and fairness or simply adding administrative complexity.

International cooperation is now unavoidable. Extremist content, platform infrastructure, and financial pathways are frequently cross-border. Pakistan's future application of the model should therefore strengthen mutual legal-assistance capacity, platform engagement procedures, and cooperation consistent with FATF standards on virtual-asset risks and terrorist financing (FATF, 2021). Comparative frameworks such as the DSA and major online-safety regimes also offer useful models for platform transparency, notice systems, and systemic-risk thinking, though they must be adapted rather than copied wholesale (European Union, 2022).

Phased Roadmap for Future Application

A realistic implementation pathway is phased rather than immediate. In Phase 1, Pakistan should adopt core legislation, establish national protocols, and designate a coordinating authority or statutory body with clear limits. In Phase 2, specialist units, forensic capability, judicial training, and referral systems should be built in selected pilot jurisdictions. In Phase 3, the full assessment and zoned-intervention system should operate nationally with standardized metrics and independent review. In Phase 4, the framework should be revised in light of empirical experience, technological change, and constitutional jurisprudence.

This sequencing matters because institutional reform is cumulative. Over-ambitious implementation without training, technology, and review mechanisms may worsen inconsistency. A phased approach allows procedural learning, correction, and legitimacy-building. It also makes it possible to identify where the model is succeeding, where it is producing false positives, and where legal safeguards need strengthening.

Institutional Adoption Checklist

A practical checklist can help agencies determine whether they are genuinely applying the model. At minimum, an adopting institution should be able to answer yes to the following questions: Do we have a written threshold framework? Do we distinguish intelligence leads from admissible evidence? Do we know when our institution leads and when it supports? Do our staff receive specialized training relevant to their role? Are our coercive decisions documented and reviewable? Do we have referral pathways for non-penal cases? Do we collect performance data? If the answer to most of these questions is no, the institution has not yet operationalized the model in any meaningful sense.

This checklist should be incorporated into self-audits, external inspections, and annual implementation reviews. It can also guide donor support, technical assistance, and judicial scrutiny by making visible which parts of the architecture are functioning and which remain aspirational. In reform environments, that kind of structured honesty is often more useful than broad claims of implementation success.

Monitoring, Evaluation, and Public Legitimacy

Future application should be measured rather than presumed. A model-based monitoring framework should track at least eight indicators: number of assessments initiated, number of cases assigned to each threshold category, time taken to route cases across agencies, digital-evidence rejection rates in court, proportion of cases diverted to rehabilitation, number of complaints alleging overreach, recidivism or re-engagement indicators, and completion rates for training and certification. These metrics would tell policymakers whether the model is improving coherence or merely increasing paperwork.

Independent oversight is essential to public legitimacy. Annual reporting should summarize how many cases moved through each zone, what safeguards were used, how many warrants were sought and granted, how often digital evidence was excluded, and what remedial action followed rights violations or procedural failures. Such reporting need not disclose sensitive operational detail. It should, however, demonstrate that the system is reviewable and not functioning as an unobservable security apparatus.

Public legitimacy also depends on communication. If communities see the model only as an expanded form of surveillance, cooperation will decline. Institutions should therefore explain that the model differentiates risk, narrows coercive intervention to threshold-based cases, and provides non-penal pathways where possible. Community trust is especially important because many early-warning or referral opportunities arise outside formal security institutions. A rights-compatible public explanation of the model is therefore not peripheral messaging; it is part of operational success.

Implementation Risks and Safeguards

No implementation framework is risk free. The first risk is bureaucratic expansion without legal discipline. A new authority or coordination mechanism could become another layer of discretionary power unless its functions, limits, and reporting duties are clearly defined in law. The model therefore requires an explicit separation between coordination, investigation, prosecution, and adjudication roles.

The second risk is over-referral. Once institutions acquire a language of digital-radicalisation risk, there is a temptation to refer all troubling online conduct into security systems. Comparative experience warns against this. Over-referral wastes resources, stigmatizes low-risk individuals, and weakens the credibility of prevention systems. The model's threshold logic should therefore be treated as a gatekeeping device, not a formality.

The third risk is technological determinism. Institutions may assume that better software, more surveillance, or predictive tools can solve a problem that is in fact legal and social as much as technical. The model rejects that assumption. Assessment tools must be validated, reviewable, and subordinate to professional judgment and judicial control. Algorithmic opacity cannot become a substitute for legal reasoning.

The fourth risk is rights erosion through informal practice. Even a well-drafted law can be undermined if agencies keep poor records, rely on unverified screenshots, pressure individuals into opaque rehabilitation, or use administrative pressure where judicial authorization is required. Implementation guidance should therefore require documentation, periodic audits, complaint pathways, and public reporting on system performance.

A final risk is symbolic implementation. Pakistan has often adopted ambitious policy language without equivalent investment in training, case management, forensic capability, and evaluation. The model's future should therefore be tied to measurable benchmarks: trained personnel,

functioning laboratories, published protocols, appellate review statistics, rehabilitation outcomes, and cross-agency case-resolution data. Without such benchmarks, implementation may exist on paper but not in practice.

Sample Five-Year Adoption Pathway

In Year 1, the government should finalize drafting instructions, designate interim lead institutions, and issue temporary digital-evidence and case-routing protocols. In Year 2, pilot jurisdictions should begin operating with specialist prosecution support, trained judges, and certified forensic workflows. In Year 3, a formal rehabilitation referral network and threshold-based reporting dashboard should go live. In Year 4, the model should be extended to additional provinces, prison-release supervision, and university or community referral systems. In Year 5, a full independent review should assess fidelity, rights compliance, and measurable impact before expansion or revision.

This staged pathway matters because implementation is often derailed by pressure to announce completion long before institutions have absorbed new routines. A five-year pathway gives Pakistan a realistic horizon for training, staffing, evaluation, and legislative refinement. It also helps donors, policymakers, and oversight bodies assess progress against milestones rather than slogans.

Future institutional guidance should therefore treat implementation as a sequence of legally and administratively measurable steps. Success will not be proven by the existence of a model document, but by whether agencies can show that cases are being classified more consistently, evidence is being handled more reliably, coercive measures are more reviewable, and rehabilitation is more than an afterthought.

Conclusion

This article has shown how various institutions can seek guidance from and practically apply the AYAZ KHAN Model in future. The key lesson is that implementation must be institutionalized, not assumed. The model becomes real only when legislation clarifies thresholds, agencies share routing protocols, digital evidence standards are enforced, courts review coercive action rigorously, prevention systems are linked to law, and rehabilitation operates through transparent criteria.

Pakistan's digital-radicalisation challenge cannot be solved by enforcement alone, nor by prevention rhetoric alone. It requires a coordinated architecture that links assessment, legality, evidence, proportionality, review, and reintegration. Properly implemented, the AYAZ KHAN Model offers that architecture. It gives institutions a common language for future action while preserving the constitutional disciplines that make security policy lawful, legitimate, and sustainable.

References

Anti-Terrorism Act, 1997 (Act XXVII of 1997) (Pakistan).

Aryaeinejad, K., & Scherer, T. L. (2024). The role of the internet and social media on radicalization: What research sponsored by the National Institute of Justice tells us (NCJ 305797). National Institute of Justice. https://www.ojp.gov/pdffiles1/nij/305797.pdf

Ashworth, A., & Zedner, L. (2014). Preventive justice. Oxford University Press.

Bandura, A. (1977). Social learning theory. Prentice Hall.

Borum, R. (2011a). Radicalization into violent extremism I: A review of social science theories. Journal of Strategic Security, 4(4), 7-36. https://doi.org/10.5038/1944-0472.4.4.1

Borum, R. (2011b). Radicalization into violent extremism II: A review of conceptual models and empirical research. Journal of Strategic Security, 4(4), 37-62. https://doi.org/10.5038/1944-0472.4.4.2

Center for Justice. (2023). Section 20 of Pakistan's Prevention of Electronic Crimes Act: Urgent reforms needed. Clooney Foundation for Justice.
https://cfj.org/wp-content/uploads/2023/10/Pakistan_PECA-Report_September-2023.pdf

Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. Studies in Conflict & Terrorism, 40(1), 77-98.
https://doi.org/10.1080/1057610X.2016.1157408

DataReportal. (2024). Digital 2024: Pakistan. https://datareportal.com/reports/digital-2024-pakistan

Digital Rights Foundation. (2025). The Prevention of Electronic Crimes (Amendment) Act, 2025: Analysis and recommendations.
https://digitalrightsfoundation.pk/wp-content/uploads/2025/01/The-Prevention-of-Electronic-Crimes-Amendment-Act-2025-DRF-Analysis-and-Recommendations.pdf

European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services (Digital Services Act). Official Journal of the European Union, L 277, 1-102.
https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

Financial Action Task Force. (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers.
https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

Institute for Economics & Peace. (2025). Global Terrorism Index 2025: Measuring the impact of terrorism. https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf

National Counter Terrorism Authority. (n.d.-a). Message from the National Coordinator. https://www.nacta.gov.pk/message-from-the-national-coordinator/

National Counter Terrorism Authority. (n.d.-b). NCVEP policy. https://nacta.gov.pk/functions/p-cve-wing/ce/ncvep-policy/

Neumann, P. R. (2013). The trouble with radicalization. International Affairs, 89(4), 873-893. https://doi.org/10.1111/1468-2346.12049

Online Safety Act 2023, c. 50 (UK). https://www.legislation.gov.uk/ukpga/2023/50/contents

Prevention of Electronic Crimes Act, 2016 (Act XL of 2016) (Pakistan). https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%3D-sg-jjjjjjjjjjjj

Scrivens, R., & Gaudette, T. (2024). Online terrorism and violent extremism. In Oxford Research Encyclopedia of Criminology and Criminal Justice. Oxford University Press. https://doi.org/10.1093/acrefore/9780190264079.013.795

Sohail, S. (2024). Exploiting encrypted networks: A CPM analysis of Telegram's role in extremist propaganda and radicalization by terrorist organisations. Pakistan Journal of Terrorism Research, 6(2), 45-68.
https://pjtr.nacta.gov.pk/index.php/Journals/article/view/140

Tyler, T. R. (2003). Procedural justice, legitimacy, and the effective rule of law. In M. Tonry (Ed.), Crime and justice: A review of research (Vol. 30, pp. 283-357). University of Chicago Press.

Warraich, S. K., Haider, A., & Mukhtar, A. (2023). Online radicalization in Pakistan: A case study of youth in South Punjab. Journal of Politics and International Studies, 9(1), 147-157. https://jpis.pu.edu.pk/45/article/view/137

eSafety Commissioner. (n.d.). What we do. https://www.esafety.gov.au/about-us/what-we-do