National Association of Workforce Boards

SKILLS ECONOMY TOOLKIT

ACTION GUIDE:
SKILLS DATA GOVERNANCE

Introduction

A skills economy depends on trusted, transparent, and interoperable quality data. When skills information is inconsistent, siloed, or unverifiable, the entire system breaks down, employers can't trust credentials, workers can't demonstrate competencies, and training providers can't align to market needs.

Data governance for skills data provides the structure, standards, and processes to ensure skills data is accurate, accessible, and actionable across your ecosystem. This guide will help you establish governance frameworks that enable skills data transparency and portability.

Why Data Governance Matters

Data governance is what transforms disconnected credentials into a functioning skills economy. Without it, badges can't be verified, skills can't transfer between systems, and employers can't trust what they see.

Strong data governance requires three things: clear policies that define who can access and share data; technical standards that ensure different systems can communicate with each other; and stakeholder buy-in so partners actually follow the rules they helped create.

The best workforce development boards start small, perhaps just governing badge data with three partners, and expand as they learn. When governance works, it's invisible: *credentials flow seamlessly, privacy stays protected, and everyone trusts the system.*

In summary, data governance matters for:

- **Trust:** Verified, quality data builds confidence in skills-based systems
- **Interoperability:** Common standards enable data sharing across platforms
- **Portability:** Workers can move credentials between employers and systems
- **Privacy:** Proper governance protects individual data rights
- **Value:** High-quality data enables better matching, planning, and outcomes

In this action guide, we walk you through establishing your governance structure and building trust by sharing high-quality data and information grounded in informed consent and privacy-preserving protocols.

Step 1: Establish Your Governance Structure

Effective data governance requires clear roles, responsibilities, and decision-making processes. Start by creating a governance structure appropriate to your ecosystem's complexity.

Core Governance Roles

Role	Responsibilities	Who Fills This Role
Data Steward	Sets data standards, policies, and quality requirements across the ecosystem	WDB leadership or designated data governance committee
Data Custodian	Manages technical infrastructure, ensures data security, and system integrity	IT director or technology partner managing platforms
Data Owner	Creates and maintains specific data sets, ensures accuracy and timeliness	Employers, training providers, credential issuers
Data User	Accesses and uses data for decision-making, matching, or analysis	Workforce centers, employers, job seekers, analysts
Compliance Officer	Ensures adherence to privacy laws, regulations, and ethical standards	Legal counsel or privacy officer
Holder	Is personally linked to the data. They may upload, manage, share, and use the skills ecosystem in good faith.	The individual person to whom the data represents, such as a learner or worker.

🔴 ***Action Item:*** *Use the Governance Roles and Responsibilities Matrix (Tool 1) to assign these roles in your organization.*

Step 2: Define Data Standards and Policies

Data standards ensure consistency and enable interoperability. It is important to establish clear policies for how skills data should be structured, classified, and shared throughout the skills data ecosystem.

Essential Data Standards

Standard Type	What to Define
Taxonomy Standards	Which skills frameworks will you use? (e.g., O*NET, ESCO, industry-specific taxonomies). How will you map between them?
Data Formats	What technical formats for credentials? (e.g., Open Badges, Verifiable Credentials, CTDL). Required metadata fields?
Quality Thresholds	Minimum data completeness (e.g., 90% of required fields). Accuracy targets, update frequency requirements.
Access Controls	Who can view, edit, or share which data? Role-based permissions, consent requirements for personal data.
Verification Methods	How will skills be validated? Assessment standards, issuer credibility criteria, and digital signature requirements.
Retention Policies	How long to keep data? Archiving procedures and deletion protocols for inactive credentials or outdated skills.

🔴 ***Action Item:*** *Use the Data Standards Definition Template (Tool 2) to document your standards and policies.*

Step 3: Implement Data Quality Management

High-quality data is accurate, complete, timely, and consistent. Establish processes to measure and maintain data quality across your ecosystem.

Six Dimensions of Data Quality

Dimension	What It Means	How to Measure
Accuracy	Data correctly represents the real-world skill or credential	Verification checks, audit samples, and error rates
Completeness	All required fields are populated with valid values	% of required fields populated, null value tracking
Consistency	Same data values across different systems and sources	Cross-system validation, duplicate detection
Timeliness	Data is current and updated at appropriate intervals	Last updated timestamps, freshness metrics
Validity	Data conforms to defined formats, ranges, and rules	Format validation, range checks, referential integrity
Uniqueness	No unnecessary duplication of records or credentials	Duplicate detection algorithms, unique identifiers

🔴 ***Action Item:*** *Use the Data Quality Scorecard (Tool 3) to assess and track your data quality metrics.*

Step 4: Protect Privacy and Security

Skills data often includes personally identifiable information (PII). Strong privacy and security practices build trust and ensure regulatory compliance.

Privacy Principles

To ensure trust throughout a skills economy and ecosystem, so that organizations adhere to privacy principles such as the following:

- **Consent:** Individuals control their own skills data and explicitly consent to sharing
- **Transparency:** Clear communication about what data is collected and how it's used
- **Minimal Collection:** Only collect data necessary for specified purposes
- **Purpose Limitation:** Use data only for stated purposes, not secondary uses
- **Data Portability:** Individuals can export and transfer their credentials
- **Right to Delete:** Individuals can request deletion of their data

Security Requirements

Any skills data shared across a skills ecosystem should also adhere to security protocols to protect it against harm during storage, transmission, and use. Here are some ways we ensure data security.

Security Layer	Implementation
Authentication	Multi-factor authentication for system access, strong password requirements, and single sign-on where appropriate
Encryption	Encrypt data at rest and in transit using industry standards (e.g., AES-256, TLS 1.3)
Access Controls	Role-based permissions, principle of least privilege, regular access reviews, and audits
Audit Logging	Track all data access and changes with timestamps and user IDs for accountability
Backup & Recovery	Regular automated backups, tested recovery procedures, and a disaster recovery plan

🔴 ***Action Item:*** *Use the Privacy and Security Checklist (Tool 4) to audit your current practices and identify gaps.*

Step 5: Enable Data Interoperability

For skills to be portable, data must move seamlessly between systems. To work towards interoperability, it is recommended to adopt open standards and establish data exchange agreements.

Key Interoperability Standards

Standard	Purpose	When to Use
Open Badges	Digital credentials with embedded metadata about skills and achievements	Training completions, micro-credentials, skill validations
CTDL (Credential Transparency Description Language)	Standardized descriptions of credentials, competencies, and pathways	Publishing to Credential Engine, creating credential registries
Comprehensive Learning and Employment Records (CLR)	Comprehensive records combining education, training, and work experience	Comprehensive worker skill profiles, career pathways
Verifiable Digital Credentials (W3C)	Cryptographically secure credentials that can be independently verified	High-security credentials, professional licenses, certifications

Data Governance Tools & Templates

Use these tools to establish and maintain effective data governance practices.

TOOL 1: Governance Roles & Responsibilities Matrix

Assign governance roles and document responsibilities.

Role	Person/Team	Key Activities	Decision Authority
Data Steward			
Data Custodian			
Data Owner			
Data User			
Compliance Officer			

TOOL 2: Data Standards Definition Template

Document your data standards and policies.

Skills Taxonomy Standard
Which taxonomy/framework: (e.g., O*NET, ESCO, custom)
Credential Format Standard
Technical format: (e.g., Open Badges, Verifiable Credentials)
Required Metadata Fields
List all required fields for credentials:
Data Quality Thresholds
Completeness requirement: ___% of required fields Accuracy target: ___% Maximum age of data: ___ days/months
Verification Requirements
How will skills/credentials be verified?

TOOL 3: Data Quality Scorecard

Assess data quality across six dimensions. Rate 1-5 (1=Poor, 5=Excellent).

Dimension	Assessment Question	Current Metric	Score
Accuracy	Are skills and credentials correctly represented?	Error rate: ___%	
Completeness	Are all required fields populated?	Completeness: ___%	
Consistency	Is data consistent across systems?	Duplicate rate: ___%	
Timeliness	Is the data current and up-to-date?	Avg age: ___ days	
Validity	Does data conform to standards?	Validation pass: ___%	
Uniqueness	Are there unnecessary duplicates?	Duplicate records: ___	
Total Score: ___/30 Overall Rating: ___			

TOOL 4: Privacy & Security Compliance Checklist

Ensure your data governance practices meet privacy and security requirements.

Requirement	Compliant?
Individuals must provide explicit consent before data collection	
Privacy policy clearly explains data use and sharing practices	
Users can access and download their own skills data	
Users can request the deletion of their personal data	
Multi-factor authentication is required for system access	
Data encrypted at rest and in transit	
Role-based access controls implemented	
All data access is logged with the holder ID and timestamp	
Regular security audits and vulnerability assessments are conducted	
Data backup and recovery procedures are tested quarterly	
Incident response plan documented and staff trained	
Vendor contracts include data protection requirements	
Annual privacy and security training for all staff	
Data retention and disposal policies established	
Compliance officer designated and empowered	

Next Steps

Establishing effective data governance is an ongoing process. Here's how to get started:

- **Assign governance roles** and establish clear responsibilities
- **Define data standards** for taxonomies, formats, and quality
- **Assess current data quality** and set improvement targets
- **Implement privacy protections** and security controls
- **Adopt interoperability standards** to enable data portability
- **Review and update** governance practices quarterly

Additional Resources

- **Action Guide:** Skills and Credentialing Taxonomies
- **Action Guide:** The Role of Technology in Skills Work
- **Credential Engine:** CTDL Technical Specifications
- **1EdTech (IMS Global):** Open Badges Specification
- **USCCF:** LER Implementation Toolkit

Questions, feedback, or looking for help setting up your skills data governance?
Contact the National Association of Workforce Boards
www.nawb.org