I’m developing a website using Pycharm and Flask.   
  
This is what I have so far:  
  
flask\_app/  
│── app.py  
│── templates/  
│ ├── base.html  
│ ├── home.htmla  
│ ├── sign\_in.html  
│ ├── dashboard.html  
│ ├── assessment.html  
│ ├── results\_admin.html  
│ ├── results\_user.html  
│ ├── library.html  
│ ├── breach\_info.html  
│ ├── risks\_bp.html  
│ ├── org\_manager.html  
│ ├── sys\_manager.html  
│ └── checklist.html

Also, I have static/css/style.css  
/\* Reset and Base Styles \*/  
\* {  
 margin: 0;  
 padding: 0;  
 box-sizing: border-box;  
}  
  
body {  
 font-family: 'Roboto', sans-serif;  
 line-height: 1.6;  
 background-color: #d1d5da;  
 color: #000000; /\* Ensure text is visible \*/  
 display: flex;  
 flex-direction: column;  
 min-height: 100vh;  
}  
  
body.authenticated {  
 /\* No additional styling needed for authenticated state \*/  
}  
  
body.unauthenticated main {  
 margin-left: 0;  
}  
  
/\* Header \*/  
header {  
 background-color: #2c3e50;  
 color: white;  
 padding: 1rem 2rem;  
 width: 100%;  
 display: flex;  
 justify-content: space-between;  
 align-items: center;  
 box-shadow: 0 2px 5px rgba(0, 0, 0, 0.1);  
 position: relative;  
 z-index: 10;  
}  
  
.logo {  
 font-size: 1.5rem;  
 font-weight: 700;  
}  
  
nav a {  
 color: white;  
 text-decoration: none;  
 margin-left: 1.5rem;  
 font-weight: 400;  
 transition: color 0.3s;  
}  
  
nav a:hover {  
 color: #3498db;  
}  
  
/\* Sidebar \*/  
.sidebar {  
 width: 250px;  
 background-color: #e8eaec;  
 padding: 1rem;  
 border-right: 1px solid #ddd;  
 box-shadow: 0 2px 10px rgba(0, 0, 0, 0.05);  
 min-height: calc(50vh - 10px);  
 max-height: 600px; /\* Adjusted to extend slightly below Org Manager \*/  
 position: absolute;  
 top: 60px;  
 left: 0;  
 overflow-y: auto;  
 align-items: center;  
}  
  
.sidebar h2 {  
 font-size: 2rem;  
 color: #2c3e50;  
 margin-bottom: 2rem;  
 margin-top: 1rem;  
 text-align: center;  
 border-bottom: 2px solid #2c3e50; /\* Add a dark line under "Navigation" \*/  
}  
  
.sidebar ul {  
 list-style-type: none;  
}  
  
.sidebar ul li {  
 margin-bottom: 0.8rem;  
}  
  
.sidebar ul li a {  
 color: #000000;  
 text-decoration: none;  
 font-weight: 500;  
 transition: color 0.3s;  
}  
  
.sidebar ul li a:hover {  
 color: #2980b9;  
 text-decoration: underline;  
}  
  
/\* Submenu \*/  
.has-submenu {  
 position: relative;  
}  
  
.submenu {  
 list-style-type: none;  
 padding-left: 1rem;  
 display: block;  
}  
  
.submenu li a {  
 font-size: 0.9rem;  
 color: #7f8c8d;  
}  
  
.submenu li a:hover {  
 color: #3498db;  
}  
  
/\* Main Content \*/  
main {  
 margin-left: 260px;  
 padding: 2rem 1rem;  
 flex: 1 0 auto;  
}  
  
.main-content {  
 max-width: 1200px;  
 margin: 0 auto;  
 min-height: calc(100vh - 120px);  
 display: flex;  
 flex-direction: column;  
}  
  
/\* Home Page Specific Styles \*/  
.welcome-text {  
 color: black;  
 font-size: 1.5rem;  
 margin-bottom: 1rem;  
}  
  
.bottom-content {  
 margin-top: auto;  
 padding-top: 2rem;  
}  
  
/\* Sign-In Box \*/  
.sign-in-box {  
 background-color: #ffffff;  
 padding: 2rem;  
 border: 1px solid #ddd;  
 border-radius: 8px;  
 box-shadow: 0 2px 10px rgba(0, 0, 0, 0.1);  
 width: 100%;  
 max-width: 500px;  
 text-align: center;  
 position: relative;  
 margin: 0 auto;  
}  
  
h1 {  
 color: #2c3e50;  
 font-size: 2rem;  
 margin-bottom: 1rem;  
}  
  
p {  
 margin-bottom: 1rem;  
 color: #7f8c8d;  
}  
  
/\* Form Styles \*/  
.form-group {  
 margin-bottom: 1.5rem;  
 text-align: left;  
 display: block;  
}  
  
.form-group label {  
 display: flex;  
 align-items: flex-start; /\* Align items to the top for better text alignment \*/  
 gap: 1.5rem;  
 width: 100%;  
 margin-bottom: 0;  
 font-weight: 400;  
 color: #333;  
 padding-top: 0.2rem; /\* Fine-tune alignment with checkbox/radio \*/  
}  
  
.form-group input[type="checkbox"],  
.form-group input[type="radio"] {  
 margin: 0;  
 -webkit-appearance: none;  
 -moz-appearance: none;  
 appearance: none;  
 width: 1.2rem; /\* Consistent size for both radio and checkbox \*/  
 height: 1.2rem;  
 min-width: 1.2rem; /\* Prevent shrinking \*/  
 min-height: 1.2rem; /\* Prevent shrinking \*/  
 border: 2px solid #333;  
 border-radius: 0; /\* Square shape for both \*/  
 background-color: #fff;  
 cursor: pointer;  
 position: relative;  
}  
  
.form-group input[type="radio"]:checked,  
.form-group input[type="checkbox"]:checked {  
 background-color: #3498db;  
 border-color: #3498db;  
}  
  
.form-group input[type="radio"]:checked::after,  
.form-group input[type="checkbox"]:checked::after {  
 content: '\2713'; /\* Checkmark \*/  
 display: block;  
 color: #fff;  
 font-size: 0.8rem;  
 text-align: center;  
 line-height: 1.2rem;  
 position: absolute;  
 top: 0;  
 left: 0;  
 width: 100%;  
 height: 100%;  
}  
  
.form-group input[type="text"],  
.form-group input[type="email"],  
.form-group input[type="password"] {  
 width: 100%;  
 padding: 0.75rem;  
 border: 1px solid #ddd;  
 border-radius: 4px;  
 font-size: 1rem;  
 height: 48px;  
 box-sizing: border-box;  
}  
  
.form-group select {  
 width: 100%;  
 padding: 0.75rem;  
 border: 1px solid #ddd;  
 border-radius: 4px;  
 font-size: 1rem;  
 height: 48px;  
 box-sizing: border-box;  
}  
  
.form-actions {  
 margin-top: 2rem;  
 display: flex;  
 justify-content: space-between;  
 align-items: center;  
 padding-bottom: 2rem;  
 position: relative;  
 z-index: 5;  
}  
  
button {  
 background-color: #3498db;  
 color: white;  
 padding: 0.75rem 1.5rem;  
 border: none;  
 border-radius: 4px;  
 cursor: pointer;  
 font-size: 1rem;  
 transition: background-color 0.3s;  
}  
  
button:hover {  
 background-color: #2980b9;  
}  
  
.forgot-password {  
 color: #3498db;  
 text-decoration: none;  
 font-size: 0.9rem;  
}  
  
.forgot-password:hover {  
 text-decoration: underline;  
}  
  
/\* Error Message \*/  
.error-message {  
 color: #e74c3c;  
 background-color: #f2dede;  
 padding: 0.5rem;  
 border-left: 4px solid #e74c3c;  
 margin-top: 1rem;  
 font-size: 0.9rem;  
}  
  
/\* Disclaimer Style \*/  
.disclaimer {  
 font-size: 0.9rem;  
 color: #7f8c8d;  
 margin-top: 1rem;  
 padding: 0.5rem;  
 background-color: #ecf0f1;  
 border-left: 4px solid #e74c3c;  
}  
  
/\* Flash Messages \*/  
.flash-messages {  
 background-color: #b0b7bc;  
 color: #000000 !important;  
 padding: 1rem;  
 margin-bottom: 1rem;  
 border-radius: 4px;  
 text-align: center;  
 opacity: 1;  
 transition: opacity 1s ease-out;  
}  
  
.flash-messages p {  
 color: #000000 !important;  
 margin: 0;  
 font-weight: bold;  
}  
  
/\* Footer \*/  
footer {  
 text-align: center;  
 padding: 1rem;  
 background-color: #2c3e50;  
 color: #ffffff;  
 width: 100%;  
 position: relative;  
 bottom: 0;  
 z-index: 1;  
}  
  
/\* Responsive Design \*/  
@media (max-width: 768px) {  
 header {  
 flex-direction: column;  
 text-align: center;  
 }  
  
 .sidebar {  
 width: 100%;  
 position: static;  
 min-height: auto;  
 max-height: none;  
 top: 0;  
 border-right: none;  
 border-bottom: 1px solid #ddd;  
 }  
  
 main {  
 margin-left: 0;  
 }  
  
 .main-content {  
 padding: 1rem;  
 }  
  
 nav {  
 margin-top: 1rem;  
 }  
  
 nav a {  
 margin: 0 0.75rem;  
 }  
  
 .form-actions {  
 flex-direction: column;  
 gap: 0.5rem;  
 }  
  
 .forgot-password {  
 margin-top: 0.5rem;  
 }  
  
 .sign-in-box {  
 margin: 1rem 0;  
 position: static;  
 transform: none;  
 width: 90%;  
 max-width: none;  
 }  
}  
  
/\* Instructions Section \*/  
.instructions {  
 background-color: #2c3e50;  
 padding: 1rem;  
 border: 1px solid #ddd;  
 border-radius: 4px;  
 margin-bottom: 2rem;  
}  
  
.instructions h2 {  
 font-size: 1.5rem;  
 color: #white;  
 margin-bottom: 0.5rem;  
}  
  
.instructions ul {  
 list-style-type: disc;  
 padding-left: 1.5rem;  
}  
  
.instructions li {  
 margin-bottom: 0.5rem;  
 color: #bac1c7  
}  
  
/\* Question Styling \*/  
.question {  
 margin-bottom: 4rem; /\* Increased for more vertical spacing \*/  
}  
  
.question p {  
 font-weight: 700;  
 color: #2c3e50;  
 font-size: 1.5rem;  
}  
  
/\* Question Styling \*/  
.question p strong {  
 color: #2c3e50 !important; /\* Add !important to ensure it takes precedence \*/  
}  
  
.question .form-group {  
 margin-left: 0;  
}  
/\* Question Container Styling \*/  
.question-container {  
 background-color: #ffffff;  
 border: 1px solid #ddd;  
 border-radius: 8px;  
 box-shadow: 0 2px 10px rgba(0, 0, 0, 0.1);  
 margin-bottom: 1rem;  
 padding: 1rem; /\* Reduced padding to minimize extra space \*/  
 color: #333;  
 display: flex;  
 flex-direction: column;  
 justify-content: center; /\* Center content vertically \*/  
 align-items: flex-start; /\* Align content to the left \*/  
 min-height: 10rem; /\* Ensure a minimum height for better centering \*/  
}  
  
.question-container .question p {  
 color: #2c3e50;  
 font-size: 1.5rem;  
 margin: 5; /\* Remove margin to let flexbox handle spacing \*/  
}  
  
.question-options {  
 display: flex;  
 flex-direction: column;  
 gap: 1rem;  
 width: 100%; /\* Ensure options take full width \*/  
}  
  
.question-options .form-group {  
 display: flex;  
 align-items: center; /\* Vertically center the checkbox and label \*/  
}  
  
.question-options .form-group label {  
 color: #333;  
 font-size: 1rem;  
 line-height: 1.5rem;  
 margin: 0;  
}  
  
.question-options .form-group input[type="radio"],  
.question-options .form-group input[type="checkbox"] {  
 margin-right: 0.5rem;  
}  
  
/\* Responsive Adjustments \*/  
@media (max-width: 768px) {  
 .question-container {  
 padding: 0.3rem;  
 min-height: 8rem; /\* Adjust min-height for smaller screens \*/  
 }  
  
 .question-container .question p {  
 font-size: 1.3rem;  
 }  
  
 .question-options .form-group label {  
 font-size: 0.9rem;  
 line-height: 1.2;  
 }  
  
 .question-options {  
 gap: 0.4rem;  
 }  
}  
  
/\* Results Button \*/  
.results-button {  
 background-color: #7f8c8d;  
 color: white;  
 padding: 0.75rem 1.5rem;  
 border-radius: 4px;  
 text-decoration: none;  
 font-size: 1rem;  
 transition: background-color 0.3s;  
 display: inline-block; /\* Change from block to inline-block \*/  
 margin-top: 2rem;  
 width: 200px; /\* Set a specific width, adjust as needed \*/  
 text-align: center; /\* Ensure text is centered within the button \*/  
}  
  
.results-button:hover {  
 background-color: #6c757d;  
}  
  
/\* Active Sidebar Item \*/  
.sidebar ul li a.active {  
 background-color: #2c3e50;  
 color: white;  
 padding: 0.5rem;  
 border-radius: 4px;  
 display: block;  
}  
  
.sidebar ul li a.active:hover {  
 color: white;  
 text-decoration: none;  
}  
  
/\* Dashboard Styles \*/  
.dashboard-container {  
 display: flex;  
 flex-wrap: wrap;  
 gap: 2rem;  
 margin-top: 2rem;  
}  
  
/\* Dashboard Styles \*/  
.compliance-score {  
 background-color: #ffffff;  
 padding: 2rem;  
 border: 1px solid #ddd;  
 border-radius: 8px;  
 text-align: center;  
 width: 370px;  
 height: 180px;  
 display: flex;  
 flex-direction: column;  
 justify-content: space-around; /\* Adjusted for better vertical centering \*/  
}  
  
.compliance-score h2 {  
 font-size: 1.5rem; /\* Slightly larger for better readability \*/  
 color: #2c3e50;  
 margin-bottom: 0.5rem; /\* Reduced to minimize vertical space \*/  
 white-space: nowrap; /\* Prevent text wrapping \*/  
}  
  
.score-box {  
 font-size: 2rem; /\* Increased for better proportionality \*/  
 font-weight: 700;  
 color: #2c3e50;  
 padding: 0.5rem; /\* Adjusted for larger text \*/  
 border-radius: 4px;  
 margin-top: 0.5rem; /\* Adjusted for spacing \*/  
}  
  
.action-buttons {  
 display: flex;  
 flex-wrap: wrap;  
 gap: 1rem;  
 margin-top: 1rem;  
}  
  
.action-button {  
 background-color: #2c3e50;  
 color: white;  
 padding: 0.75rem 1.5rem;  
 border-radius: 4px;  
 text-decoration: none;  
 font-size: 1rem;  
 text-align: center;  
 transition: background-color 0.3s;  
}  
  
.action-button:hover {  
 background-color: #2980b9;  
}  
  
/\* Separator Line \*/  
.separator {  
 border: 0;  
 height: 1px;  
 background: #ddd;  
 margin: 2rem 0;  
}  
  
/\* Checklist Styles \*/  
.checklist-container {  
 display: flex;  
 flex-wrap: nowrap; /\* Changed from wrap to ensure side-by-side layout \*/  
 gap: 2rem;  
 margin-top: 2rem;  
 align-items: flex-start; /\* Align items at the top \*/  
}  
  
.checklist {  
 background-color: #ffffff;  
 padding: 1.5rem;  
 border: 1px solid #ddd;  
 border-radius: 8px;  
 width: 1500px; /\* Widened checklist \*/  
 flex-grow: 1; /\* Allow checklist to grow but respect width \*/  
}  
  
.checklist h2 {  
 font-size: 1.5rem;  
 color: #2c3e50;  
 margin-bottom: 1rem;  
}  
  
.checklist .form-group {  
 margin-bottom: 1.5rem; /\* Increased for more vertical spacing \*/  
}  
  
/\* To-Do List Table Styles \*/  
.to-do-table {  
 width: 100%;  
 border-collapse: collapse;  
 margin-top: 1rem;  
 background-color: #ffffff; /\* Ensure table background contrasts with text \*/  
}  
  
.to-do-table th, .to-do-table td {  
 padding: 0.75rem;  
 text-align: left;  
 border-bottom: 1px solid #ddd;  
 color: #333; /\* Set text color to a dark shade for visibility \*/  
}  
  
.to-do-table th {  
 background-color: #ecf0f1;  
 font-weight: 700;  
}  
  
/\* Organization Manager Styles \*/  
.org-manager-container {  
 display: flex;  
 flex-wrap: wrap;  
 gap: 2rem;  
 margin-top: 2rem;  
}  
  
.admin-manager {  
 background-color: #ffffff;  
 padding: 1.5rem;  
 border: 1px solid #ddd;  
 border-radius: 8px;  
 width: 100%;  
 max-width: 600px;  
}  
  
.admin-manager h2 {  
 font-size: 1.5rem;  
 color: #2c3e50;  
 margin-bottom: 0.5rem;  
}  
  
.admin-manager table {  
 width: 100%;  
 border-collapse: collapse;  
 margin-bottom: 1rem;  
}  
  
.admin-manager th, .admin-manager td {  
 padding: 0.5rem;  
 text-align: left;  
 border-bottom: 1px solid #ddd;  
}  
  
.admin-manager th {  
 background-color: #2c3e50;  
 font-weight: 700;  
 color: white; /\* Ensure header text is readable against the dark background \*/  
}  
  
.admin-manager td {  
 color: black; /\* Set table cell text to black \*/  
}  
  
.admin-manager select {  
 padding: 0.5rem;  
 border: 1px solid #ddd;  
 border-radius: 4px;  
 font-size: 1rem;  
}  
  
/\* Create User Box Styles \*/  
.create-user-box {  
 background-color: #ffffff;  
 padding: 2rem;  
 border: 1px solid #ddd;  
 border-radius: 8px;  
 box-shadow: 0 2px 10px rgba(0, 0, 0, 0.1);  
 width: 100%;  
 max-width: 500px;  
 text-align: center;  
 margin-left: 2rem;  
}  
  
.create-user-box h2 {  
 font-size: 1.5rem;  
 color: #2c3e50;  
 margin-bottom: 1rem;  
}  
  
.create-user-box .form-group {  
 display: flex;  
 flex-direction: column;  
 align-items: flex-start;  
 margin-bottom: 1rem;  
}  
  
.create-user-box .form-group label {  
 margin-bottom: 0.25rem;  
 font-weight: 400;  
 color: #333;  
 text-align: left;  
 width: 100%;  
}  
  
.create-user-box .form-group input,  
.create-user-box .form-group select {  
 width: 100%;  
 padding: 0.75rem;  
 border: 1px solid #ddd;  
 border-radius: 4px;  
 font-size: 1rem;  
 height: 48px;  
 box-sizing: border-box;  
 margin-bottom: 0.5rem;  
}  
  
.create-user-box .form-actions {  
 margin-top: 1rem;  
 display: flex;  
 justify-content: center;  
}  
  
.create-user-box button {  
 background-color: #3498db;  
 color: white;  
 padding: 0.75rem 1.5rem;  
 border: none;  
 border-radius: 4px;  
 cursor: pointer;  
 font-size: 1rem;  
 transition: background-color 0.3s;  
 width: 100px;  
}  
  
.create-user-box button:hover {  
 background-color: #2980b9;  
}  
  
/\* System Manager Styles \*/  
.sys-manager-container {  
 display: flex;  
 flex-wrap: wrap;  
 gap: 2rem;  
 margin-top: 2rem;  
}  
  
.create-org-box {  
 background-color: #ffffff;  
 padding: 2rem;  
 border: 1px solid #ddd;  
 border-radius: 8px;  
 box-shadow: 0 2px 10px rgba(0, 0, 0, 0.1);  
 width: 100%;  
 max-width: 400px;  
 text-align: center;  
}  
  
.create-org-box .form-group input,  
.create-org-box .form-group select {  
 height: 48px;  
}  
  
/\* Breach Info Page Specific Styles \*/  
.breach-container {  
 background-color: #ffffff;  
 border: 1px solid #ddd;  
 border-radius: 8px;  
 box-shadow: 0 2px 10px rgba(0, 0, 0, 0.1);  
 margin-bottom: 2rem;  
 padding: 1.5rem;  
 transition: transform 0.2s ease-in-out;  
}  
  
.breach-container:hover {  
 transform: translateY(-5px);  
}  
  
.breach-title {  
 color: #2c3e50;  
 font-size: 1.8rem;  
 margin-bottom: 1rem;  
 border-bottom: 2px solid #3498db;  
 padding-bottom: 0.5rem;  
}  
  
.breach-details {  
 padding: 1rem;  
}  
  
.breach-details h4 {  
 color: #3498db;  
 font-size: 1.3rem;  
 margin-bottom: 0.5rem;  
}  
  
.breach-details ul {  
 list-style-type: disc;  
 padding-left: 2rem;  
 margin-bottom: 1rem;  
}  
  
.breach-details li {  
 margin-bottom: 0.5rem;  
 color: #333;  
}  
  
.intro-text {  
 font-size: 1.1rem;  
 color: #7f8c8d;  
 margin-bottom: 2rem;  
 line-height: 1.8;  
}  
  
/\* Graph Container Styles \*/  
.graph-container {  
 background-color: #ffffff;  
 border: 1px solid #ddd;  
 border-radius: 8px;  
 box-shadow: 0 2px 10px rgba(0, 0, 0, 0.1);  
 margin-bottom: 2rem;  
 padding: 1.5rem;  
 text-align: center;  
}  
  
.graph-title {  
 color: #2c3e50;  
 font-size: 1.5rem;  
 margin-bottom: 1rem;  
}  
  
.graph-image {  
 max-width: 100%;  
 height: auto;  
 border: 1px solid #ddd;  
 border-radius: 4px;  
 margin-bottom: 1rem;  
}  
  
.graph-caption {  
 font-size: 0.95rem;  
 color: #7f8c8d;  
 line-height: 1.6;  
 margin: 0 auto;  
 max-width: 800px;  
}  
  
/\* Responsive Adjustments \*/  
@media (max-width: 768px) {  
 .breach-container {  
 padding: 1rem;  
 }  
  
 .breach-title {  
 font-size: 1.5rem;  
 }  
  
 .breach-details h4 {  
 font-size: 1.1rem;  
 }  
  
 .graph-container {  
 padding: 1rem;  
 }  
  
 .graph-title {  
 font-size: 1.3rem;  
 }  
  
 .graph-caption {  
 font-size: 0.9rem;  
 }  
}  
/\* Library Page Specific Styles \*/  
.toc-container {  
 background-color: #f9f9f9;  
 border: 1px solid #ddd;  
 border-radius: 8px;  
 padding: 1.5rem;  
 margin-bottom: 2rem;  
}  
  
.toc-container h3 {  
 color: #2c3e50;  
 font-size: 1.5rem;  
 margin-bottom: 1rem;  
 border-bottom: 2px solid #3498db;  
 padding-bottom: 0.5rem;  
}  
  
.toc-list {  
 list-style-type: none;  
 padding: 0;  
}  
  
.toc-list li {  
 margin-bottom: 0.5rem;  
}  
  
.toc-list a {  
 color: #3498db;  
 text-decoration: none;  
 font-size: 1.1rem;  
 transition: color 0.3s ease;  
}  
  
.toc-list a:hover {  
 color: #2c3e50;  
 text-decoration: underline;  
}  
  
.section-container {  
 background-color: #ffffff;  
 border: 1px solid #ddd;  
 border-radius: 8px;  
 box-shadow: 0 2px 10px rgba(0, 0, 0, 0.1);  
 margin-bottom: 2rem;  
 padding: 1.5rem;  
}  
  
.section-container h2 {  
 color: #2c3e50;  
 font-size: 1.8rem;  
 margin-bottom: 1rem;  
 border-bottom: 2px solid #3498db;  
 padding-bottom: 0.5rem;  
}  
  
.section-container p {  
 font-size: 1rem;  
 color: #333;  
 line-height: 1.8;  
 margin-bottom: 1rem;  
}  
  
.recital-list {  
 padding-left: 2rem;  
 margin-bottom: 1rem;  
}  
  
.recital-list li {  
 margin-bottom: 1rem;  
 color: #333;  
 line-height: 1.8;  
}  
  
/\* Responsive Adjustments \*/  
@media (max-width: 768px) {  
 .toc-container {  
 padding: 1rem;  
 }  
  
 .toc-container h3 {  
 font-size: 1.3rem;  
 }  
  
 .toc-list a {  
 font-size: 1rem;  
 }  
  
 .section-container {  
 padding: 1rem;  
 }  
  
 .section-container h2 {  
 font-size: 1.5rem;  
 }  
  
 .section-container p {  
 font-size: 0.95rem;  
 }  
}  
/\* Main Content (already in your style.css, included for completeness) \*/  
.main-content {  
 padding: 20px;  
 max-width: 1200px;  
 margin: 0 auto;  
 color: #d3d3d3;  
}  
  
/\* Section Styling \*/  
.section {  
 margin-bottom: 40px;  
}  
  
.section h2 {  
 font-size: 1.8em;  
 color: #2c3e50;  
 border-bottom: 2px solid #1e90ff;  
 padding-bottom: 10px;  
 margin-bottom: 20px;  
}  
  
/\* Accordion Styling \*/  
/\* Accordion Styling \*/  
.accordion {  
 margin-bottom: 20px;  
}  
  
.accordion-item {  
 margin-bottom: 10px;  
}  
  
.accordion-header {  
 background-color: #2c3e50; /\* Keep the dark header for contrast \*/  
 color: #ffffff;  
 padding: 15px;  
 width: 100%;  
 text-align: left;  
 border: none;  
 border-radius: 5px;  
 cursor: pointer;  
 font-size: 1.2em;  
 transition: background-color 0.3s;  
}  
  
.accordion-header:hover {  
 background-color: #2980b9;  
}  
  
.accordion-content {  
 display: none;  
 background-color: #ffffff; /\* White background to match breach-container \*/  
 border: 1px solid #ddd; /\* Add border for consistency \*/  
 border-radius: 0 0 5px 5px; /\* Rounded corners at the bottom \*/  
 box-shadow: 0 2px 10px rgba(0, 0, 0, 0.1); /\* Add shadow to match breach-container \*/  
 padding: 1.5rem; /\* Match padding of breach-container \*/  
 color: #333; /\* Dark text for readability on white background \*/  
}  
  
.accordion-content p {  
 margin: 10px 0;  
 color: #333; /\* Ensure text is readable \*/  
 line-height: 1.8; /\* Match breach-details line height \*/  
}  
  
.accordion-content ul {  
 list-style-type: disc; /\* Match breach-details \*/  
 padding-left: 2rem; /\* Match breach-details \*/  
 margin: 10px 0 1rem 0; /\* Match breach-details \*/  
}  
  
.accordion-content li {  
 margin-bottom: 0.5rem; /\* Match breach-details \*/  
 color: #333; /\* Match breach-details \*/  
}  
  
.accordion-content strong {  
 color: #1e90ff; /\* Keep the blue highlight for strong tags \*/  
}  
  
/\* Table Styling Inside Accordion \*/  
.accordion-content table {  
 background-color: #ffffff; /\* Ensure table background is white \*/  
 width: 100%;  
 border-collapse: collapse;  
 margin-top: 1rem;  
}  
  
.accordion-content table th,  
.accordion-content table td {  
 padding: 0.75rem;  
 text-align: left;  
 border-bottom: 1px solid #ddd;  
 color: #333; /\* Dark text for readability \*/  
}  
  
.accordion-content table th {  
 background-color: #ecf0f1; /\* Light gray for table headers \*/  
 font-weight: 700;  
}  
  
/\* Accordion Controls (Expand All/Close All Buttons) \*/  
.accordion-controls {  
 margin-bottom: 20px;  
 display: flex;  
 gap: 10px;  
}  
  
.accordion-control-button {  
 background-color: #1e90ff;  
 color: #ffffff;  
 padding: 10px 20px;  
 border: none;  
 border-radius: 5px;  
 cursor: pointer;  
 font-size: 1em;  
 transition: background-color 0.3s;  
}  
  
.accordion-control-button:hover {  
 background-color: #4682b4;  
}  
  
/\* Responsive Adjustments \*/  
@media (max-width: 768px) {  
 .accordion-header {  
 font-size: 1em;  
 padding: 10px;  
 }  
  
 .accordion-content {  
 padding: 1rem; /\* Reduce padding on smaller screens \*/  
 }  
  
 .accordion-controls {  
 flex-direction: column;  
 gap: 5px;  
 }  
  
 .accordion-control-button {  
 padding: 8px 15px;  
 font-size: 0.9em;  
 }  
  
 .accordion-content table th,  
 .accordion-content table td {  
 padding: 0.5rem; /\* Reduce padding for smaller screens \*/  
 }  
}  
  
/\* Intro Text \*/  
.intro-text {  
 font-size: 1.1em;  
 color: #d3d3d3;  
 margin-bottom: 30px;  
}  
  
/\* Results Button (already in your style.css, included for completeness) \*/  
.results-button {  
 display: inline-block;  
 background-color: #1e90ff;  
 color: #ffffff;  
 padding: 10px 20px;  
 text-decoration: none;  
 border-radius: 5px;  
 margin-top: 20px;  
 transition: background-color 0.3s;  
}  
  
.results-button:hover {  
 background-color: #4682b4;  
}  
  
/\* Responsive Adjustments \*/  
@media (max-width: 768px) {  
 .section h2 {  
 font-size: 1.5em;  
 }  
  
 .accordion-header {  
 font-size: 1em;  
 padding: 10px;  
 }  
  
 .accordion-content {  
 padding: 15px;  
 }  
  
 .accordion-controls {  
 flex-direction: column;  
 gap: 5px;  
 }  
  
 .accordion-control-button {  
 padding: 8px 15px;  
 font-size: 0.9em;  
 }  
  
 .intro-text {  
 font-size: 1em;  
 }  
  
 .results-button {  
 padding: 8px 15px;  
 font-size: 0.9em;  
 }  
}  
/\* PDF Section \*/  
.pdf-section {  
 margin-bottom: 40px;  
}  
  
.pdf-section h2 {  
 font-size: 1.8em;  
 color: #ffffff;  
 border-bottom: 2px solid #1e90ff;  
 padding-bottom: 10px;  
 margin-bottom: 20px;  
}  
  
/\* PDF Container \*/  
.pdf-container {  
 background-color: #1a1a1a; /\* Dark background to match your theme \*/  
 padding: 10px;  
 border-radius: 5px;  
 box-shadow: 0 2px 5px rgba(0, 0, 0, 0.3);  
}  
  
/\* PDF Viewer \*/  
.pdf-viewer {  
 width: 100%;  
 height: 80vh; /\* Use viewport height to make it larger and responsive \*/  
 min-height: 600px; /\* Ensure a minimum height for smaller screens \*/  
 border: none;  
 border-radius: 5px;  
}  
  
/\* Responsive Adjustments \*/  
@media (max-width: 768px) {  
 .pdf-section h2 {  
 font-size: 1.5em;  
 }  
  
 .pdf-viewer {  
 height: 60vh; /\* Slightly smaller on mobile \*/  
 min-height: 400px;  
 }  
}  
/\* Header Styles \*/  
header {  
 background-color: #2c3e50;  
 padding: 0; /\* Remove padding to fit within 20px height \*/  
 height: 70px; /\* Set fixed height to 20px \*/  
 display: flex;  
 justify-content: space-between;  
 align-items: center;  
 overflow: hidden; /\* Hide any overflow from the logo or nav \*/  
}  
  
.header-logo {  
 height: 300px; /\* Scale the logo to fill the header height \*/  
 width: auto; /\* Maintain aspect ratio \*/  
 object-fit: contain; /\* Ensures the logo fits within the height without cropping \*/  
 max-width: 300px; /\* Limit max width to prevent excessive stretching \*/  
}  
  
header nav {  
 display: flex;  
 align-items: center;  
 height: 100%; /\* Ensure nav fits within the 20px height \*/  
}  
  
header nav a {  
 color: #ecf0f1;  
 text-decoration: none;  
 margin-left: 1rem; /\* Reduce margin for tight space \*/  
 margin-right: 2rem;  
 font-size: 1rem; /\* Smaller font size to fit within 20px height \*/  
 white-space: nowrap; /\* Prevent text wrapping \*/  
}  
  
/\* Responsive Adjustments (optional, adjust as needed) \*/  
@media (max-width: 768px) {  
 header nav a {  
 font-size: 0.6rem; /\* Even smaller on mobile \*/  
 margin-left: 0.3rem;  
 }  
}  
  
/\* Ensure the main content area doesn't constrain the PDF viewer \*/  
.main-content {  
 padding: 20px;  
 max-width: 100%; /\* Allow the content to take full width \*/  
 margin: 0 auto;  
 color: #d3d3d3;  
}  
  
/\* Style for the introductory paragraph \*/  
.main-content p {  
 font-size: 1.1em;  
 color: #2c3e50;  
 margin-bottom: 20px;  
}  
  
.main-content p strong {  
 color: #1e90ff; /\* Highlight GDPR in blue \*/  
}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
assessment.html  
{% extends "base.html" %}  
{% block title %}Assessment - DPAT{% endblock %}  
{% block content %}  
<div class="main-content">  
 <h1>Begin Compliance Assessment</h1>  
 <p>This exam evaluates your organization's Data Practices using the GDPR Requirements.</p>  
  
 <!-- Instructions Section -->  
 <div class="instructions">  
 <h2>Instructions</h2>  
 <ul>  
 <li>This exam consists of 20 questions.</li>  
 <li>Please select the most appropriate answer.</li>  
 <li>For scenario-based questions, choose all applicable responses.</li>  
 <li>Once you have answered the questions, submit the responses.</li>  
 </ul>  
 </div>  
  
 <!-- Assessment Form -->  
 <form method="POST" action="{{ url\_for('assessment') }}">  
 <h2>Part I: Multiple Choice Questions</h2>  
 <div class="question-container">  
 <div class="question">  
 <p><strong>1.</strong> How does your organization handle the collection of personal data from EU residents?</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q1" value="a" required>  
 We collect personal data without a clear, documented purpose.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q1" value="b">  
 We collect personal data for specific, documented purposes and based on explicit consent.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q1" value="c">  
 We collect personal data only for internal use and without consent.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q1" value="d">  
 We do not process personal data of EU residents.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>2.</strong> How does your organization ensure that personal data is only accessible by authorized individuals?</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q2" value="a" required>  
 We rely on basic access control, allowing broad access to data.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q2" value="b">  
 We implement strict access control policies and regularly review access permissions.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q2" value="c">  
 We allow employees unrestricted access to personal data if stored in the same database.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q2" value="d">  
 We have no specific access control policies in place.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>3.</strong> How does your organization manage data retention and deletion under GDPR?</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q3" value="a" required>  
 We store personal data indefinitely unless explicitly requested by the data subject.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q3" value="b">  
 We store personal data only for as long as necessary and securely delete it when no longer needed.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q3" value="c">  
 We keep data for as long as possible for future business purposes.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q3" value="d">  
 We have no formal data retention policy.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>4.</strong> How does your organization handle obtaining consent from data subjects?</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q4" value="a" required>  
 We collect personal data without seeking explicit consent.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q4" value="b">  
 We collect personal data only after obtaining clear, informed consent and allow individuals to withdraw consent.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q4" value="c">  
 We assume that individuals implicitly consent when they use our services.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q4" value="d">  
 We collect personal data only when required by law.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>5.</strong> How does your organization protect personal data during transmission?</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q5" value="a" required>  
 We use no encryption for data transmission.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q5" value="b">  
 We use basic security protocols like HTTP, without encryption.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q5" value="c">  
 We use encryption for sensitive data during transmission but not for all data.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q5" value="d">  
 We use HTTPS and implement encryption for all personal data transmissions.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>6.</strong> What is your organization’s approach to handling data breaches?</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q6" value="a" required>  
 We have no formal breach notification process in place.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q6" value="b">  
 We notify affected individuals and report to relevant authorities within 72 hours of a breach.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q6" value="c">  
 We notify individuals only if the breach is deemed significant.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q6" value="d">  
 We do not notify anyone about data breaches.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>7.</strong> Does your organization conduct Data Protection Impact Assessments (DPIAs) for new data processing activities?</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q7" value="a" required>  
 We only conduct DPIAs for high-risk activities.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q7" value="b">  
 We do not conduct DPIAs unless legally required.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q7" value="c">  
 We conduct DPIAs for all new data processing activities.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q7" value="d">  
 We conduct DPIAs only when prompted by the regulatory authority.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>8.</strong> How does your organization ensure the accuracy of personal data?</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q8" value="a" required>  
 We do not have procedures for checking the accuracy of personal data.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q8" value="b">  
 We update personal data only when the individual requests an update.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q8" value="c">  
 We regularly review and update personal data to ensure its accuracy.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q8" value="d">  
 We store personal data as provided by the individual and make no updates.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>9.</strong> How does your organization handle requests from individuals to access or delete their personal data under GDPR?</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q9" value="a" required>  
 We do not have a formal process to handle these requests.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q9" value="b">  
 We respond to requests within 30 days, confirming the status of the request.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q9" value="c">  
 We only respond to requests made in writing or by email.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q9" value="d">  
 We automatically reject requests if the individual’s identity cannot be verified.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>10.</strong> How does your organization ensure third-party vendors comply with GDPR when processing personal data?</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q10" value="a" required>  
 We assume third-party vendors are compliant without formal agreements.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q10" value="b">  
 We have formal contracts in place that include GDPR-specific clauses.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q10" value="c">  
 We do not monitor third-party vendors for GDPR compliance.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="radio" name="q10" value="d">  
 We only work with vendors located within the EU.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <h2>Part II: Multiple-Answer Questions</h2>  
 <div class="question-container">  
 <div class="question">  
 <p><strong>11.</strong> Which of the following practices does your organization follow to ensure compliance with the GDPR principle of "data minimization"? (Select all that apply.)</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q11" value="a">  
 We collect only the minimum amount of personal data necessary for our business purpose.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q11" value="b">  
 We store personal data indefinitely to ensure we have it available if needed.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q11" value="c">  
 We regularly review and limit the data we collect to prevent unnecessary storage.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q11" value="d">  
 We request extensive personal information from customers to better understand their preferences.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>12.</strong> Which of the following security measures has your organization implemented to protect personal data? (Select all that apply.)</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q12" value="a">  
 Encryption of personal data at rest and during transmission.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q12" value="b">  
 Regular security audits and vulnerability testing of IT systems.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q12" value="c">  
 Restricting physical access to data storage locations.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q12" value="d">  
 Allowing all employees full access to personal data without restrictions.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>13.</strong> Which actions does your organization take to comply with the GDPR’s "Right to Erasure" (Right to be Forgotten)? (Select all that apply.)</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q13" value="a">  
 We permanently delete personal data upon request when no legitimate business reason exists for its retention.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q13" value="b">  
 We assess whether data can be erased unless it's required for legal reasons.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q13" value="c">  
 We store personal data indefinitely and only provide a reason for deletion if requested by the individual.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q13" value="d">  
 We inform the data subject of the actions we take in response to their request.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>14.</strong> When transferring personal data to third parties outside the EU, which of the following safeguards does your organization use to ensure GDPR compliance? (Select all that apply.)</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q14" value="a">  
 We use Standard Contractual Clauses (SCCs) to secure the data transfer.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q14" value="b">  
 We rely on verbal agreements and assume that the third party is GDPR-compliant.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q14" value="c">  
 We assess the data protection laws of the recipient country before transferring data.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q14" value="d">  
 We ensure the third-party provider has signed a Data Processing Agreement (DPA) with GDPR clauses.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>15.</strong> How does your organization handle consent management for personal data processing? (Select all that apply.)</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q15" value="a">  
 We collect explicit consent for each type of data processing activity.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q15" value="b">  
 We use pre-ticked boxes to obtain consent during registration.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q15" value="c">  
 We allow individuals to withdraw consent at any time.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q15" value="d">  
 We collect consent only once and do not provide individuals with an option to withdraw.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <h2>Part III: Scenario-Based Questions</h2>  
 <div class="question-container">  
 <div class="question">  
 <p><strong>16.</strong> Scenario: Your company has launched a new marketing campaign that involves collecting email addresses and phone numbers from potential customers for promotional purposes. The marketing team has not yet consulted with the data protection officer (DPO). What actions should your organization take to ensure GDPR compliance for this campaign? (Select all that apply.)</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q16" value="a">  
 Review the purpose of data collection to ensure it is documented and clear.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q16" value="b">  
 Obtain explicit consent from individuals before collecting their personal data.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q16" value="c">  
 Inform individuals about how their data will be used and their rights under GDPR.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q16" value="d">  
 Begin the campaign immediately without any consultation with the DPO as consent is implied.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>17.</strong> Scenario: A data breach occurs when an employee accidentally sends a document containing sensitive personal data (e.g., health data) to the wrong email address. The email was not encrypted. What immediate actions should your organization take following this breach? (Select all that apply.)</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q17" value="a">  
 Inform affected individuals and relevant supervisory authorities within 72 hours.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q17" value="b">  
 Investigate the cause of the breach and mitigate any future risks.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q17" value="c">  
 Document the breach and any actions taken to address it.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>18.</strong> Scenario: A customer requests to have their personal data deleted because they no longer want to receive marketing communications. The data includes their name, email, and past purchase history. How should your organization respond to this request? (Select all that apply.)</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q18" value="a">  
 Confirm the request within 30 days and delete all personal data, unless legally required to retain it.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q18" value="b">  
 Deny the request if the data is necessary for fulfilling contractual obligations.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q18" value="c">  
 Ask the customer to provide proof of identity before processing the request.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q18" value="d">  
 Store the customer’s data indefinitely unless they explicitly withdraw consent.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>19.</strong> Scenario: Your organization is preparing to outsource customer support services to a third-party provider in the US. The provider will have access to personal data, including customer contact details and purchase history. What actions must your organization take to ensure compliance with GDPR? (Select all that apply.)</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q19" value="a">  
 Execute a Data Processing Agreement (DPA) with the third-party provider.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q19" value="b">  
 Transfer the data without taking any specific measures, assuming the provider is compliant with GDPR.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q19" value="c">  
 Ensure that the provider implements adequate safeguards, such as Standard Contractual Clauses (SCCs).  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q19" value="d">  
 Transfer personal data without assessing the provider’s data protection measures.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="question-container">  
 <div class="question">  
 <p><strong>20.</strong> Scenario: Your company is conducting an audit of its data security practices and has found that certain personal data stored on employee laptops is not encrypted. This includes sensitive data like employee addresses and social security numbers. What should your organization do to address this issue? (Select all that apply.)</p>  
 <div class="question-options">  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q20" value="a">  
 Immediately encrypt all personal data on employee laptops.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q20" value="b">  
 Implement encryption on all devices used for storing or accessing personal data.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q20" value="c">  
 Nothing can be done, as encryption is not legally required for personal data on laptops.  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="q20" value="d">  
 Update company policies to mandate encryption for all personal data.  
 </label>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <div class="form-actions">  
 <button type="submit">Submit</button>  
 </div>  
 </form>  
</div>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
base.html  
<!DOCTYPE html>  
<html lang="en">  
<head>  
 <meta charset="UTF-8">  
 <meta name="viewport" content="width=device-width, initial-scale=1.0">  
 <title>{% block title %}Data Privacy and Analysis Tool - DPAT{% endblock %}</title>  
 <link rel="stylesheet" href="{{ url\_for('static', filename='css/style.css') }}">  
 <link href="https://fonts.googleapis.com/css2?family=Roboto:wght@400;700&display=swap" rel="stylesheet">  
 <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/flatpickr/dist/flatpickr.min.css">  
 <script src="https://cdn.jsdelivr.net/npm/flatpickr"></script>  
</head>  
<body class="{% if current\_user.is\_authenticated %}authenticated{% else %}unauthenticated{% endif %}">  
 <header>  
 <img src="{{ url\_for('static', filename='images/dpat\_header\_logo.png') }}" alt="DPAT Logo" class="header-logo">  
 <nav>  
 <a href="{{ url\_for('home') }}">Home</a>  
 <a href="{{ url\_for('dashboard') }}">Dashboard</a>  
 <a href="{{ url\_for('logout') }}">Logout</a>  
 </nav>  
</header>  
 {% if current\_user.is\_authenticated %}  
 <div class="sidebar">  
 <h2>Navigation</h2>  
 <ul>  
 {% if current\_user.email == 'sysadmin@dpat.org' %}  
 <li><a href="{{ url\_for('sys\_manager') }}" class="{% if request.endpoint == 'sys\_manager' %}active{% endif %}">System Manager</a></li>  
 {% else %}  
 <li><a href="{{ url\_for('home') }}" class="{% if request.endpoint == 'home' %}active{% endif %}">Home</a></li>  
 <li><a href="{{ url\_for('dashboard') }}" class="{% if request.endpoint == 'dashboard' %}active{% endif %}">Dashboard</a></li>  
 <li class="has-submenu">  
 <a href="{{ url\_for('assessment') }}" class="{% if request.endpoint == 'assessment' %}active{% endif %}">Assessment</a>  
 <ul class="submenu">  
 <li><a href="{{ url\_for('results\_user') }}" class="{% if request.endpoint == 'results\_user' %}active{% endif %}">– Results</a></li>  
 {% if current\_user.is\_authenticated and current\_user.role == 'admin' %}  
 <li><a href="{{ url\_for('results\_admin') }}" class="{% if request.endpoint == 'results\_admin' %}active{% endif %}">– Admin Results</a></li>  
 {% endif %}  
 </ul>  
 </li>  
 <li class="has-submenu">  
 <a href="{{ url\_for('checklist') }}" class="{% if request.endpoint == 'checklist' %}active{% endif %}">Compliance Checklist</a>  
 <ul class="submenu">  
 <li><a href="{{ url\_for('to\_do\_list') }}" class="{% if request.endpoint == 'to\_do\_list' %}active{% endif %}">– To-Do List</a></li>  
 </ul>  
 </li>  
 <li class="has-submenu">  
 <a href="{{ url\_for('library') }}" class="{% if request.endpoint == 'library' %}active{% endif %}">Compliance Library</a>  
 </li>  
 <li class="has-submenu">  
 <a href="{{ url\_for('breach\_info') }}" class="{% if request.endpoint == 'breach\_info' %}active{% endif %}">Breach Information</a>  
 <ul class="submenu">  
 <li><a href="{{ url\_for('risks\_bp') }}" class="{% if request.endpoint == 'risks\_bp' %}active{% endif %}">– BI Graphical Analysis</a></li>  
 <li><a href="{{ url\_for('consequences\_bp') }}" class="{% if request.endpoint == 'consequences\_bp' %}active{% endif %}">– Consequences and BP</a></li>  
 </ul>  
 </li>  
 {% if current\_user.is\_authenticated and current\_user.role == 'admin' %}  
 <li><a href="{{ url\_for('org\_manager') }}" class="{% if request.endpoint == 'org\_manager' %}active{% endif %}">Organization Manager</a></li>  
 {% endif %}  
 {% endif %}  
 </ul>  
 </div>  
 {% endif %}  
 <main>  
 {% block content %}{% endblock %}  
 </main>  
 <footer>  
 <p>© 2025 Data Privacy and Analysis Tool (DPAT). All rights reserved.</p>  
 </footer>  
</body>  
</html>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
breach\_info.html  
{% extends "base.html" %}  
{% block title %}Breach Information - DPAT{% endblock %}  
{% block content %}  
<div class="main-content">  
 <h1>Breach Information</h1>  
 <p class="intro-text">Learn about data breaches and how to handle them. Below is a detailed analysis of some of the largest data breaches since 2010, along with their consequences and financial impacts.</p>  
  
 <!-- Breach Details -->  
 <h2>Largest Data Breaches Since 2010 (Chronological Order)</h2>  
  
 <div class="breach-container">  
 <h3 class="breach-title">Breach 1: Sony PlayStation Network – April 2011</h3>  
 <div class="breach-details">  
 <h4>Key Details:</h4>  
 <ul>  
 <li>77 million accounts compromised (names, addresses, email addresses, birthdates, PSN login credentials, purchase history)</li>  
 <li>Credit card information potentially exposed (Sony claims it was encrypted)</li>  
 </ul>  
 <h4>Impact & Consequences:</h4>  
 <ul>  
 <li>23-day shutdown of PlayStation Network</li>  
 <li>Legal fees, security upgrades, compensation ($171 million)</li>  
 <li>Lawsuits for negligence in protecting user data</li>  
 <li>Loss of customer trust</li>  
 <li>Regulatory scrutiny</li>  
 <li>Reputational damage</li>  
 </ul>  
 </div>  
 </div>  
  
 <div class="breach-container">  
 <h3 class="breach-title">Breach 2: Yahoo – August 2013 & November 2014</h3>  
 <div class="breach-details">  
 <h4>Key Details:</h4>  
 <ul>  
 <li>Both breaches combined compromised 3.5 billion accounts (names, email addresses, birthdays, hashed passwords, security questions)</li>  
 <li>2013 breach not publicly disclosed until September of 2016</li>  
 <li>2014 breach not publicly disclosed until December of 2016</li>  
 </ul>  
 <h4>Impact & Consequences:</h4>  
 <ul>  
 <li>Reduced acquisition offer from Verizon ($350 million)</li>  
 <li>Settlements, fines ($153.5 million)</li>  
 <li>Loss of customer trust</li>  
 <li>Regulatory scrutiny</li>  
 <li>Reputational damage</li>  
 <li>Security upgrades</li>  
 </ul>  
 </div>  
 </div>  
  
 <div class="breach-container">  
 <h3 class="breach-title">Breach 3: Adobe – October 2013</h3>  
 <div class="breach-details">  
 <h4>Key Details:</h4>  
 <ul>  
 <li>153 million accounts compromised (email addresses, encrypted passwords, password hints, partial payment data)</li>  
 </ul>  
 <h4>Impact & Consequences:</h4>  
 <ul>  
 <li>Lawsuits, settlements ($1.1 million settlement)</li>  
 <li>Loss of customer trust</li>  
 <li>Regulatory scrutiny</li>  
 <li>Reputational damage</li>  
 <li>Security upgrades</li>  
 </ul>  
 </div>  
 </div>  
  
 <div class="breach-container">  
 <h3 class="breach-title">Breach 4: Target – December 2013</h3>  
 <div class="breach-details">  
 <h4>Key Details:</h4>  
 <ul>  
 <li>Credit and debit card information from 40 million customers exposed</li>  
 <li>Personal data from 70 million additional individuals exposed (names, addresses, phone numbers, email addresses)</li>  
 </ul>  
 <h4>Impact & Consequences:</h4>  
 <ul>  
 <li>Settlements, legal fees, security upgrades ($292 million)</li>  
 <li>Loss of customer trust</li>  
 <li>Regulatory scrutiny</li>  
 <li>Reputational damage</li>  
 </ul>  
 </div>  
 </div>  
  
 <div class="breach-container">  
 <h3 class="breach-title">Breach 5: Marriott – June 2014</h3>  
 <div class="breach-details">  
 <h4>Key Details:</h4>  
 <ul>  
 <li>Personal data from 500 million guests compromised (names, phone numbers, email addresses, passport numbers, arrival and departure dates, and encrypted payment card details)</li>  
 </ul>  
 <h4>Impact & Consequences:</h4>  
 <ul>  
 <li>Regulatory lawsuits, fines ($23.8 million)</li>  
 <li>Loss of customer trust</li>  
 <li>Regulatory scrutiny</li>  
 <li>Reputational damage</li>  
 <li>Security Upgrades</li>  
 </ul>  
 </div>  
 </div>  
  
 <div class="breach-container">  
 <h3 class="breach-title">Breach 6: Uber – November 2016</h3>  
 <div class="breach-details">  
 <h4>Key Details:</h4>  
 <ul>  
 <li>Data from 57 million users compromised (names, email addresses, phone numbers)</li>  
 <li>600,000 US drivers had their license numbers exposed (along with their user data)</li>  
 <li>Uber failed to disclose the breach for over a year</li>  
 </ul>  
 <h4>Impact & Consequences:</h4>  
 <ul>  
 <li>Settlement ($148 million)</li>  
 <li>Uber’s former CSO was charged by the US Department of Justice for covering up the breach (convicted of obstruction of justice)</li>  
 <li>Loss of customer trust</li>  
 <li>Regulatory scrutiny</li>  
 <li>Reputational damage</li>  
 <li>Security upgrades</li>  
 </ul>  
 </div>  
 </div>  
  
 <div class="breach-container">  
 <h3 class="breach-title">Breach 7: Equifax – July 2017</h3>  
 <div class="breach-details">  
 <h4>Key Details:</h4>  
 <ul>  
 <li>147 million people had their data compromised (full names, social security numbers, birthdays, addresses, driver’s license numbers, credit card numbers, dispute documents)</li>  
 </ul>  
 <h4>Impact & Consequences:</h4>  
 <ul>  
 <li>Lawsuits, settlements ($700 million)</li>  
 <li>Security upgrades, breach response ($1.4 billion)</li>  
 <li>CEO resignation</li>  
 <li>Loss of customer trust</li>  
 <li>Regulatory scrutiny</li>  
 <li>Reputational damage</li>  
 </ul>  
 </div>  
 </div>  
  
 <div class="breach-container">  
 <h3 class="breach-title">Breach 8: Facebook – April 2019</h3>  
 <div class="breach-details">  
 <h4>Key Details:</h4>  
 <ul>  
 <li>Unsecured databases exposed sensitive data from 540 million user accounts (user IDs, account names, comments, likes, reactions, friends lists, interests, check-ins, activity logs)</li>  
 <li>In rare cases, plaintext Facebook passwords were exposed (22,000 users)</li>  
 </ul>  
 <h4>Impact & Consequences:</h4>  
 <ul>  
 <li>Loss of customer trust</li>  
 <li>Regulatory scrutiny</li>  
 <li>Reputational damage</li>  
 <li>Security upgrades</li>  
 </ul>  
 </div>  
 </div>  
  
 <div class="breach-container">  
 <h3 class="breach-title">Breach 9: Capital One – July 2019</h3>  
 <div class="breach-details">  
 <h4>Key Details:</h4>  
 <ul>  
 <li>106 million accounts compromised (names, addresses, phone numbers, email addresses, birthdays, credit scores, transaction data)</li>  
 <li>Exposed 80,000 bank account numbers, 140,000 US Social Security numbers, and 1 million Canadian Social Insurance numbers</li>  
 </ul>  
 <h4>Impact & Consequences:</h4>  
 <ul>  
 <li>Fines, settlements, lawsuits, security upgrades ($300-500 million)</li>  
 <li>Loss of customer trust</li>  
 <li>Regulatory scrutiny</li>  
 <li>Reputational damage</li>  
 </ul>  
 </div>  
 </div>  
  
 <div class="breach-container">  
 <h3 class="breach-title">Breach 10: T-Mobile – August 2021</h3>  
 <div class="breach-details">  
 <h4>Key Details:</h4>  
 <ul>  
 <li>Data from 76.6 million customers compromised (names, birthdays, social security numbers, driver’s license and ID numbers, phone numbers, T-Mobile account details, T-Mobile account PINs)</li>  
 </ul>  
 <h4>Impact & Consequences:</h4>  
 <ul>  
 <li>Settlements ($350 million and T-Mobile required to provide free credit monitoring to all affected individuals)</li>  
 <li>Security upgrades ($150 million)</li>  
 <li>Loss of customer trust</li>  
 <li>Regulatory scrutiny</li>  
 <li>Reputational damage</li>  
 </ul>  
 </div>  
 </div>  
</div>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
change\_user.html

{% extends "base.html" %}  
{% block title %}Change User Role - DPAT{% endblock %}  
{% block content %}  
<div class="main-content">  
 <h1>Change User Role</h1>  
 <p>Adjust role for {{ user.email }}</p>  
 <form method="POST">  
 <label for="role">Role:</label>  
 <select id="role" name="role">  
 <option value="user" {% if user.role == 'user' %}selected{% endif %}>User</option>  
 <option value="admin" {% if user.role == 'admin' %}selected{% endif %}>Admin</option>  
 </select>  
 <button type="submit">Save</button>  
 </form>  
</div>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
checklist.html  
{% extends "base.html" %}  
{% block title %}Compliance Checklist - DPAT{% endblock %}  
{% block content %}  
<div class="main-content">  
 {% if current\_user.role == 'admin' %}  
 <h1>Compliance Checklist</h1>  
 <div class="checklist-container">  
 <div class="checklist">  
 <h2>GDPR Compliance Checklist</h2>  
 <p2> Note -- Resubmitting this Checklist will reset the Compliance Score</p2>  
 <form id="checklist-form" method="POST" action="{{ url\_for('checklist') }}">  
 <!-- Lawful Basis for Processing -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="lawful\_basis\_identified" onchange="updateComplianceScore()">  
 Have we identified and documented the lawful basis for each type of data processing (e.g., consent, contract necessity, legitimate interests)?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="lawful\_basis\_demonstrated" onchange="updateComplianceScore()">  
 Are we able to demonstrate the lawful basis for processing personal data for all current and past activities?  
 </label>  
 </div>  
  
 <!-- Data Minimization -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="data\_minimization\_necessary" onchange="updateComplianceScore()">  
 Do we only collect the personal data necessary for the specified purpose(s)?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="data\_minimization\_review" onchange="updateComplianceScore()">  
 Are we regularly reviewing the data we hold to ensure we are not retaining unnecessary or excessive data?  
 </label>  
 </div>  
  
 <!-- Data Accuracy -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="data\_accuracy\_process" onchange="updateComplianceScore()">  
 Do we have processes in place to ensure that the personal data we hold is accurate and up-to-date?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="data\_accuracy\_correction" onchange="updateComplianceScore()">  
 Are there mechanisms to allow data subjects to correct inaccurate data?  
 </label>  
 </div>  
  
 <!-- Transparency and Information to Data Subjects -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="transparency\_notices" onchange="updateComplianceScore()">  
 Have we provided clear, easily accessible privacy notices that explain how personal data is processed?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="transparency\_details" onchange="updateComplianceScore()">  
 Do our privacy notices specify the purposes of data processing, the lawful basis, data retention periods, and the rights of data subjects?  
 </label>  
 </div>  
  
 <!-- Consent Management -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="consent\_freely\_given" onchange="updateComplianceScore()">  
 If we rely on consent for processing personal data, is it freely given, specific, informed, and unambiguous?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="consent\_management" onchange="updateComplianceScore()">  
 Have we implemented processes for obtaining, recording, and managing consent from data subjects?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="consent\_withdrawal" onchange="updateComplianceScore()">  
 Do we provide data subjects with an easy method to withdraw consent at any time?  
 </label>  
 </div>  
  
 <!-- Data Subject Rights -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="subject\_rights\_procedures" onchange="updateComplianceScore()">  
 Do we have clear procedures for handling data subject rights requests (e.g., right to access, rectification, erasure, portability, objection)?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="subject\_rights\_response" onchange="updateComplianceScore()">  
 Are we able to respond to data subject requests within the required one-month timeframe?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="subject\_rights\_verification" onchange="updateComplianceScore()">  
 Have we established a process for verifying the identity of individuals making data subject rights requests?  
 </label>  
 </div>  
  
 <!-- Data Retention and Disposal -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="retention\_policy" onchange="updateComplianceScore()">  
 Do we have a documented data retention policy that specifies retention periods for personal data?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="retention\_disposal" onchange="updateComplianceScore()">  
 Are we regularly reviewing and securely disposing of data that is no longer required or that has reached its retention period?  
 </label>  
 </div>  
  
 <!-- Data Security Measures -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="security\_measures" onchange="updateComplianceScore()">  
 Do we have appropriate technical and organizational measures in place to protect personal data (e.g., encryption, access controls)?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="security\_training" onchange="updateComplianceScore()">  
 Are our employees trained on data security best practices, and do we have a process for reviewing and updating security measures regularly?  
 </label>  
 </div>  
  
 <!-- Data Breach Response -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="breach\_response\_plan" onchange="updateComplianceScore()">  
 Do we have an internal data breach response plan that includes procedures for identifying, containing, and reporting breaches?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="breach\_notification" onchange="updateComplianceScore()">  
 Have we implemented a system for notifying the relevant supervisory authority of data breaches within 72 hours, as required by GDPR?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="breach\_subject\_notification" onchange="updateComplianceScore()">  
 Are data subjects notified of breaches when necessary?  
 </label>  
 </div>  
  
 <!-- Third-Party Data Processors -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="third\_party\_contracts" onchange="updateComplianceScore()">  
 Do we have written contracts in place with third-party data processors outlining their GDPR obligations?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="third\_party\_audits" onchange="updateComplianceScore()">  
 Are we conducting due diligence and regular audits of third-party processors to ensure GDPR compliance?  
 </label>  
 </div>  
  
 <!-- Data Protection Impact Assessments (DPIAs) -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="dpia\_high\_risk" onchange="updateComplianceScore()">  
 Have we conducted DPIAs for high-risk processing activities, particularly when introducing new technologies or processing large volumes of sensitive data?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="dpia\_documented" onchange="updateComplianceScore()">  
 Are DPIAs documented, and do they include an assessment of the necessity and proportionality of the processing?  
 </label>  
 </div>  
  
 <!-- Accountability and Governance -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="dpo\_designated" onchange="updateComplianceScore()">  
 Do we have a designated Data Protection Officer (DPO) or another responsible person/team for ensuring GDPR compliance?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="processing\_records" onchange="updateComplianceScore()">  
 Are we maintaining proper documentation of our data processing activities, including data processing records?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="internal\_audits" onchange="updateComplianceScore()">  
 Are internal audits conducted regularly to assess compliance with GDPR?  
 </label>  
 </div>  
  
 <!-- International Data Transfers -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="data\_transfer\_safeguards" onchange="updateComplianceScore()">  
 If we transfer personal data outside the European Economic Area (EEA), have we implemented adequate safeguards (e.g., Standard Contractual Clauses, Binding Corporate Rules)?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="data\_transfer\_assessment" onchange="updateComplianceScore()">  
 Are we assessing the privacy and security standards of countries outside the EEA before transferring personal data?  
 </label>  
 </div>  
  
 <!-- Employee Training and Awareness -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="employee\_training" onchange="updateComplianceScore()">  
 Are all employees who handle personal data trained on GDPR principles and data protection practices?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="ongoing\_training" onchange="updateComplianceScore()">  
 Do we provide ongoing training and updates to ensure employees remain informed about data protection responsibilities?  
 </label>  
 </div>  
  
 <!-- Monitoring and Reporting -->  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="monitoring\_processes" onchange="updateComplianceScore()">  
 Do we have processes in place to monitor and report on compliance with GDPR internally?  
 </label>  
 </div>  
 <div class="form-group">  
 <label>  
 <input type="checkbox" name="checklist\_items" value="gdpr\_review" onchange="updateComplianceScore()">  
 Are we regularly reviewing our GDPR practices to ensure we stay aligned with evolving legal and regulatory requirements?  
 </label>  
 </div>  
  
 <button type="submit">Save/Generate To-Do List</button>  
 </form>  
 </div>  
 <div class="compliance-score">  
 <h2>Compliance Score</h2>  
 <div class="score-box" id="compliance-score">0%</div>  
 </div>  
 </div>  
 <p class="disclaimer">This checklist is visible only to admin users.</p>  
 {% else %}  
 <h1>Access Denied</h1>  
 <p>This page is restricted to admin users only. Please contact an administrator.</p>  
 {% endif %}  
</div>  
  
<script>  
 function updateComplianceScore() {  
 const checkboxes = document.querySelectorAll('input[name="checklist\_items"]');  
 const totalItems = checkboxes.length;  
 const checkedItems = Array.from(checkboxes).filter(checkbox => checkbox.checked).length;  
 const score = Math.round((checkedItems / totalItems) \* 100);  
 document.getElementById('compliance-score').textContent = `${score}%`;  
 }  
</script>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
consequences\_bp.html  
{% extends "base.html" %}  
{% block title %}Consequences & Best Practices - DPAT{% endblock %}  
{% block content %}  
<div class="main-content">  
 <h1>Consequences & Best Practices</h1>  
 <p class="intro-text">Understand the potential outcomes of data breaches and learn best practices to prevent them.</p>  
 <p class="intro-text">Click on each individual tab or use the access buttons to see the information.</p>  
 <!-- Data Breach Consequences -->  
 <div class="section" id="consequences">  
 <h2>Data Breach Consequences – Common Outcomes</h2>  
  
 <!-- Expand/Close All Buttons -->  
 <div class="accordion-controls">  
 <button class="accordion-control-button" onclick="expandAll()">Expand All</button>  
 <button class="accordion-control-button" onclick="closeAll()">Close All</button>  
 </div>  
  
 <div class="accordion">  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Loss of Trust</button>  
 <div class="accordion-content" id="loss-of-trust">  
 <p>A data breach can severely damage an organization's reputation, leading to a loss of trust among customers, partners, and stakeholders. When sensitive information is compromised, individuals may feel vulnerable and hesitant to continue engaging with the organization, fearing further security lapses. This erosion of trust can result in:</p>  
 <ul>  
 <li>Financial losses due to customer attrition.</li>  
 <li>Legal consequences as affected parties seek compensation.</li>  
 <li>Business moving to competitors.</li>  
 </ul>  
 <p>Moreover, regulatory bodies may impose fines and sanctions, further straining the organization's resources and credibility.</p>  
 <p><strong>GDPR Relevance:</strong> The General Data Protection Regulation (GDPR) establishes strict guidelines for data protection and holds organizations accountable for breaches. Companies must implement robust security measures and promptly notify authorities and affected individuals in the event of a breach. Failure to comply can lead to fines of up to 4% of annual global revenue or €20 million, whichever is higher, exacerbating the financial and reputational damage. GDPR emphasizes the need for proactive security measures to maintain trust.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Reputational Damage</button>  
 <div class="accordion-content" id="reputational-damage">  
 <p>Reputational damage following a data breach can have long-lasting consequences, including:</p>  
 <ul>  
 <li>Decreased customer retention and lost business opportunities.</li>  
 <li>Decline in brand value due to negative media coverage.</li>  
 <li>Impact on employee morale and investor confidence, potentially affecting stock prices.</li>  
 </ul>  
 <p>The cost of restoring reputation through public relations efforts, security improvements, and customer compensation can be substantial.</p>  
 <p><strong>GDPR Relevance:</strong> GDPR mandates transparency by requiring prompt disclosure of breaches, which can intensify public backlash if mishandled. Non-compliance can lead to significant fines, further harming credibility. Organizations that fail to comply may be perceived as negligent, worsening reputational harm.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Regulatory Scrutiny</button>  
 <div class="accordion-content" id="regulatory-scrutiny">  
 <p>Regulatory scrutiny following a data breach can lead to:</p>  
 <ul>  
 <li>Costly legal proceedings and mandatory audits.</li>  
 <li>Stricter compliance requirements and increased oversight.</li>  
 <li>Operational disruptions and loss of business relationships.</li>  
 </ul>  
 <p>Heightened regulatory attention can also damage the organization's credibility.</p>  
 <p><strong>GDPR Relevance:</strong> GDPR establishes clear legal obligations, with fines up to 4% of annual global revenue or €20 million for non-compliance. Regulatory bodies like the European Data Protection Board can investigate breaches and enforce corrective actions. Timely breach notifications are mandatory, increasing public and regulatory attention.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Lawsuits, Settlements, & Legal Fees</button>  
 <div class="accordion-content" id="lawsuits">  
 <p>Lawsuits and legal fees can impose a significant burden, including:</p>  
 <ul>  
 <li>Compensation for damages like identity theft or financial loss.</li>  
 <li>Substantial settlement costs from class-action lawsuits.</li>  
 <li>Prolonged negative media attention, further damaging reputation.</li>  
 </ul>  
 <p>Legal fees for defending claims and ensuring compliance can be overwhelming.</p>  
 <p><strong>GDPR Relevance:</strong> GDPR allows individuals to seek compensation for harm due to data breaches. Non-compliance can lead to regulatory penalties and strengthen the legal basis for lawsuits, amplifying financial and reputational damage.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Other Financial Penalties</button>  
 <div class="accordion-content" id="financial-penalties">  
 <p>Beyond regulatory fines, financial penalties include:</p>  
 <ul>  
 <li>Direct costs: forensic investigations, breach notifications, and customer compensation.</li>  
 <li>Loss of revenue as customers take business elsewhere.</li>  
 <li>Increased insurance premiums or payouts.</li>  
 <li>Costs of security upgrades to prevent future breaches.</li>  
 </ul>  
 <p><strong>GDPR Relevance:</strong> GDPR imposes fines up to 4% of global annual revenue or €20 million for non-compliance. Organizations must invest in robust security measures, or face higher costs post-breach.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Exposure of Sensitive Information</button>  
 <div class="accordion-content" id="exposure">  
 <p>Exposure of sensitive information can lead to:</p>  
 <ul>  
 <li>Identity theft, fraud, or cybercrimes for individuals.</li>  
 <li>Loss of competitive advantage due to leaked intellectual property.</li>  
 <li>Legal disputes and damaged business relationships.</li>  
 </ul>  
 <p><strong>GDPR Relevance:</strong> GDPR requires appropriate security measures to prevent unauthorized access and mandates breach notifications. Failure to protect data can result in significant fines and legal consequences.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Shutdowns</button>  
 <div class="accordion-content" id="shutdowns">  
 <p>Shutdowns following a breach can cause:</p>  
 <ul>  
 <li>Operational disruptions and lost revenue.</li>  
 <li>Missed business opportunities and delays in services.</li>  
 <li>Loss of customer and partner confidence.</li>  
 </ul>  
 <p><strong>GDPR Relevance:</strong> GDPR requires stringent security measures and timely breach notifications. Non-compliance can lead to sanctions, extending downtime and increasing scrutiny.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Loss of Intellectual Property</button>  
 <div class="accordion-content" id="ip-loss">  
 <p>Loss of intellectual property can result in:</p>  
 <ul>  
 <li>Competitors exploiting proprietary information.</li>  
 <li>Reduced revenue and weakened partnerships.</li>  
 <li>Legal disputes over unauthorized use.</li>  
 </ul>  
 <p><strong>GDPR Relevance:</strong> While GDPR focuses on personal data, its security principles apply to all sensitive information. Breaches involving PII can lead to additional fines and lawsuits.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Criminal Convictions & Resignations</button>  
 <div class="accordion-content" id="convictions">  
 <p>Convictions and resignations can lead to:</p>  
 <ul>  
 <li>Legal action against negligent executives or employees.</li>  
 <li>Leadership instability and reduced employee morale.</li>  
 <li>Challenges in recruiting new leadership.</li>  
 </ul>  
 <p><strong>GDPR Relevance:</strong> GDPR holds executives personally liable for non-compliance. Regulatory investigations can lead to legal consequences and forced resignations, intensifying public scrutiny.</p>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <!-- Data Breach Prevention – Best Practices -->  
 <div class="section" id="best-practices">  
 <h2>Data Breach Prevention – Best Practices</h2>  
  
 <!-- Expand/Close All Buttons -->  
 <div class="accordion-controls">  
 <button class="accordion-control-button" onclick="expandAll()">Expand All</button>  
 <button class="accordion-control-button" onclick="closeAll()">Close All</button>  
 </div>  
  
 <div class="accordion">  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Layered Security – Defense in Depth</button>  
 <div class="accordion-content" id="layered-security">  
 <p>Layered security employs multiple security measures to protect assets, including:</p>  
 <ul>  
 <li>Physical security, network security, and endpoint protection.</li>  
 <li>Access controls and data encryption.</li>  
 </ul>  
 <p>This approach ensures that if one control fails, others remain to limit the impact of an attack.</p>  
 <p><strong>GDPR Relevance:</strong> GDPR mandates appropriate technical safeguards to prevent breaches. Defense in depth aligns with these requirements by enhancing data protection through multiple layers.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Patch Management</button>  
 <div class="accordion-content" id="patch-management">  
 <p>Patch management involves regularly updating software to fix vulnerabilities, reducing the risk of:</p>  
 <ul>  
 <li>Unauthorized access and data theft.</li>  
 <li>System disruptions and downtime.</li>  
 </ul>  
 <p><strong>GDPR Relevance:</strong> GDPR requires keeping systems up to date to prevent breaches. Failure to apply patches can lead to non-compliance and penalties.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Vulnerability & Penetration Testing</button>  
 <div class="accordion-content" id="vulnerability-testing">  
 <p>Vulnerability and penetration testing identify weaknesses by:</p>  
 <ul>  
 <li>Scanning for known security flaws.</li>  
 <li>Simulating real-world attacks to test defenses.</li>  
 </ul>  
 <p>Regular testing strengthens security posture and reduces breach risks.</p>  
 <p><strong>GDPR Relevance:</strong> GDPR mandates proactive security measures. Regular testing helps organizations identify and fix weaknesses, ensuring compliance.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Employee Training & Awareness</button>  
 <div class="accordion-content" id="employee-training">  
 <p>Employee training reduces human error by educating staff on:</p>  
 <ul>  
 <li>Phishing threats and password management.</li>  
 <li>Data protection policies and security best practices.</li>  
 </ul>  
 <p><strong>GDPR Relevance:</strong> GDPR requires staff to understand data handling responsibilities. Training helps prevent accidental breaches and ensures compliance.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Access Controls</button>  
 <div class="accordion-content" id="access-controls">  
 <p>Access controls regulate who can access data, using:</p>  
 <ul>  
 <li>Role-based access control (RBAC) and multi-factor authentication (MFA).</li>  
 <li>Least privilege principles to limit exposure.</li>  
 </ul>  
 <p><strong>GDPR Relevance:</strong> GDPR requires protection against unauthorized access. Strict access controls reduce breach risks and ensure compliance.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Encryption of Sensitive Data</button>  
 <div class="accordion-content" id="encryption">  
 <p>Encryption transforms data into an unreadable format, protecting it:</p>  
 <ul>  
 <li>At rest (stored data) and in transit (transmitted data).</li>  
 <li>From unauthorized access, even if stolen.</li>  
 </ul>  
 <p><strong>GDPR Relevance:</strong> GDPR mandates technical safeguards like encryption. Encrypted data may not be reportable as a breach, reducing legal risks.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Data Minimization</button>  
 <div class="accordion-content" id="data-minimization">  
 <p>Data minimization limits data collection to what’s necessary, reducing:</p>  
 <ul>  
 <li>Risk of exposure in a breach.</li>  
 <li>Complexity in data management.</li>  
 </ul>  
 <p><strong>GDPR Relevance:</strong> GDPR requires data to be adequate, relevant, and limited. Data minimization aligns with this principle, mitigating breach risks.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Data Deletion Protocols</button>  
 <div class="accordion-content" id="data-deletion">  
 <p>Data deletion protocols securely remove unneeded data, using:</p>  
 <ul>  
 <li>Cryptographic wiping or physical destruction.</li>  
 <li>Processes to ensure data cannot be recovered.</li>  
 </ul>  
 <p><strong>GDPR Relevance:</strong> GDPR mandates data not be retained longer than necessary and supports the right to be forgotten. Secure deletion ensures compliance.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Incident Response Protocols</button>  
 <div class="accordion-content" id="incident-response">  
 <p>Incident response protocols ensure a swift response to breaches, including:</p>  
 <ul>  
 <li>Detecting, containing, and mitigating risks.</li>  
 <li>Investigating causes and notifying stakeholders.</li>  
 </ul>  
 <p><strong>GDPR Relevance:</strong> GDPR requires breach notifications within 72 hours. A strong response plan ensures compliance and minimizes damage.</p>  
 </div>  
 </div>  
  
 <div class="accordion-item">  
 <button class="accordion-header" onclick="toggleAccordion(this)">Continuous Logging and Monitoring</button>  
 <div class="accordion-content" id="logging-monitoring">  
 <p>Continuous logging and monitoring provide visibility into:</p>  
 <ul>  
 <li>Network traffic and user activities.</li>  
 <li>Potential threats and unusual behavior.</li>  
 </ul>  
 <p><strong>GDPR Relevance:</strong> GDPR requires technical measures to safeguard data. Monitoring detects threats in real-time, ensuring compliance.</p>  
 </div>  
 </div>  
 </div>  
 </div>  
  
 <a href="{{ url\_for('breach\_info') }}" class="results-button">Back to Breach Information</a>  
</div>  
  
<!-- JavaScript for Accordion -->  
<script>  
function toggleAccordion(button) {  
 const content = button.nextElementSibling;  
 const isOpen = content.style.display === "block";  
 // Close all other accordion items  
 document.querySelectorAll('.accordion-content').forEach(item => {  
 item.style.display = "none";  
 });  
 // Toggle the clicked item  
 content.style.display = isOpen ? "none" : "block";  
}  
  
function expandAll() {  
 document.querySelectorAll('.accordion-content').forEach(item => {  
 item.style.display = "block";  
 });  
}  
  
function closeAll() {  
 document.querySelectorAll('.accordion-content').forEach(item => {  
 item.style.display = "none";  
 });  
}  
</script>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
dashboard.html  
{% extends "base.html" %}  
{% block title %}Dashboard - DPAT{% endblock %}  
{% block content %}  
<div class="main-content">  
 {% if current\_user.role == 'admin' %}  
 <h1>Welcome, {{ current\_user.email }}</h1>  
 <div class="dashboard-container">  
 <!-- Compliance Score -->  
 <div class="compliance-score">  
 <h2>Compliance Score</h2>  
 <div class="score-box">{{ avg\_score }}%</div>  
 </div>  
  
 <!-- Date Set -->  
 <div class="compliance-score">  
 <h2>Date Set</h2>  
 <div class="score-box date-set" id="date-set">{{ goal\_date if goal\_date else 'Not Set' }}</div>  
 </div>  
  
 <!-- Days Remaining -->  
 <div class="compliance-score">  
 <h2>Days Remaining</h2>  
 <div class="score-box" id="days-remaining">{{ days\_remaining if days\_remaining else 'N/A' }}</div>  
 </div>  
 </div>  
  
 <!-- Separator Line -->  
 <hr class="separator">  
  
 <!-- Action Buttons -->  
 <div class="action-buttons">  
 <a href="{{ url\_for('org\_manager') }}" class="action-button">Manage User Accounts</a>  
 <a href="#" class="action-button" id="set-goal-date">Set Performance Goal</a>  
 <a href="{{ url\_for('results\_user') }}" class="action-button">See Compliance Results</a>  
 <a href="{{ url\_for('checklist') }}" class="action-button">See To-Do Report</a>  
 </div>  
  
 <p class="disclaimer">This dashboard is visible only to admin users.</p>  
 {% else %}  
 <h1>Access Denied</h1>  
 <p>This page is restricted to admin users only. Please contact an administrator.</p>  
 {% endif %}  
</div>  
  
<script>  
 document.addEventListener('DOMContentLoaded', function () {  
 flatpickr("#set-goal-date", {  
 enableTime: false,  
 dateFormat: "F j",  
 onChange: function(selectedDates, dateStr) {  
 // AJAX call to save goal date  
 fetch('/set\_goal\_date', {  
 method: 'POST',  
 headers: {  
 'Content-Type': 'application/json',  
 },  
 body: JSON.stringify({goal\_date: dateStr})  
 })  
 .then(response => response.json())  
 .then(data => {  
 document.getElementById('date-set').textContent = dateStr;  
 document.getElementById('days-remaining').textContent = data.days\_remaining >= 0 ? data.days\_remaining : "Past Due";  
 });  
 }  
 });  
 });  
</script>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
home.html  
{% extends "base.html" %}  
{% block title %}Home - DPAT{% endblock %}  
{% block content %}  
<div class="main-content" style="padding: 3rem; border-radius: 10px; max-width: 900px; margin: 2rem auto;">  
 <!-- Logo Section -->  
 <div class="logo-container" style="text-align: center; margin-bottom: 3rem;">  
 <img src="{{ url\_for('static', filename='images/dpat\_logo.png') }}" alt="DPAT Logo" style="max-width: 400px; height: auto; margin: 0 auto;">  
 </div>  
  
 <!-- Welcome Section -->  
 <div class="welcome-section" style="text-align: center; margin-bottom: 3rem;">  
 <h1 class="welcome-text" style="font-size: 2.5rem; font-weight: 700; margin-bottom: 1rem;">  
 Welcome to the Data Privacy Analysis Tool  
 </h1>  
 <p style="font-size: 1.3rem; max-width: 800px; margin: 0 auto; line-height: 1.6;">  
 DPAT helps organizations ensure compliance with EU data privacy regulations, including GDPR, through comprehensive assessments, checklists, and resources.  
 </p>  
 </div>  
  
 <!-- User Status Section -->  
 <div class="user-status" style="text-align: center; margin-bottom: 3rem;">  
 {% if not current\_user.is\_authenticated %}  
 <p style="font-size: 1.2rem; margin-bottom: 1.5rem;">  
 Please sign in to access tools for your organization.  
 </p>  
 <a href="{{ url\_for('sign\_in') }}" class="action-button" style="display: inline-block; padding: 0.75rem 2rem; border-radius: 5px; text-decoration: none; font-size: 1.1rem; transition: background-color 0.3s;">  
 Sign In  
 </a>  
 {% else %}  
 <p style="font-size: 1.2rem; margin-bottom: 1.5rem;">  
 Welcome, {{ current\_user.email }}. You are now logged in.  
 </p>  
 <a href="{{ url\_for('dashboard') }}" class="action-button" style="display: inline-block; padding: 0.75rem 2rem; border-radius: 5px; text-decoration: none; font-size: 1.1rem; transition: background-color 0.3s;">  
 Go to Dashboard  
 </a>  
 {% endif %}  
 </div>  
  
 <!-- Disclaimer Section -->  
 <div class="disclaimer-section" style="text-align: center; padding-top: 2rem;">  
 <p class="disclaimer" style="font-size: 1rem; line-height: 1.5;">  
 The DPAT is designed to help companies meet and maintain compliance with EU data privacy regulations<br>  
 We are not responsible for implementing those changes  
 </p>  
</div>  
</div>  
  
  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
library.html  
{% extends "base.html" %}  
  
{% block content %}  
<div class="main-content">  
 <div class="section">  
 <h2>DPAT Compliance Library</h2>  
 <p class="intro-text">  
 Below is the General Data Protection Regulation (GDPR) document, provided as an interactive PDF. Use the navigation controls to browse through the document.  
 </p>  
  
 <!-- PDF Embed Container -->  
 <div class="pdf-container">  
 <iframe src="{{ url\_for('static', filename='pdf/DPAT Library.pdf') }}#toolbar=1&navpanes=0&scrollbar=1"  
 class="pdf-viewer"  
 title="DPAT Compliance Library - GDPR Document">  
 <!-- Fallback for browsers that don't support iframes or PDF embedding -->  
 <p>Your browser does not support embedded PDFs.  
 <a href="{{ url\_for('static', filename='pdf/DPAT Library.pdf') }}" target="\_blank">Download the PDF here</a>.  
 </p>  
 </iframe>  
 </div>  
 </a>  
 </div>  
</div>  
  
<!-- JavaScript to Ensure PDF Loads Properly -->  
<script>  
 document.addEventListener('DOMContentLoaded', function() {  
 const iframe = document.querySelector('.pdf-viewer');  
 iframe.onload = function() {  
 console.log('PDF loaded successfully');  
 };  
 iframe.onerror = function() {  
 console.error('Error loading PDF');  
 };  
 });  
</script>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
org\_manager.html  
{% extends "base.html" %}  
{% block title %}Organization Manager - DPAT{% endblock %}  
{% block content %}  
<div class="main-content">  
 {% if current\_user.role == 'admin' %}  
 {% with messages = get\_flashed\_messages() %}  
 {% if messages %}  
 <meta http-equiv="refresh" content="2;url={{ url\_for('org\_manager') }}">  
 {% endif %}  
 {% endwith %}  
 <h1>Organization Manager</h1>  
 <div class="org-manager-container">  
 <div class="admin-manager">  
 <h2>Admin Manager</h2>  
 <p>Users: {{ organization\_name | default('Sacred Heart University') }}</p>  
 <table>  
 <thead>  
 <tr>  
 <th>Name</th>  
 <th>Role</th>  
 <th>Remove</th>  
 </tr>  
 </thead>  
 <tbody>  
 {% for user in users %}  
 <tr>  
 <td>{{ user.email }}</td>  
 <td>  
 <form method="POST" action="{{ url\_for('update\_role') }}">  
 <input type="hidden" name="email" value="{{ user.email }}">  
 <select name="role" onchange="this.form.submit()">  
 <option value="user" {% if user.role == 'user' %}selected{% endif %}>User</option>  
 <option value="admin" {% if user.role == 'admin' %}selected{% endif %}>Admin</option>  
 </select>  
 </form>  
 </td>  
 <td><input type="checkbox" name="remove\_user" value="{{ user.id }}"></td>  
 </tr>  
 {% endfor %}  
 </tbody>  
 </table>  
 <button onclick="removeUsers()" class="action-button">Remove</button>  
</div>  
 <div class="create-user-box">  
 <h2>Create User</h2>  
 <form method="POST" action="{{ url\_for('org\_manager') }}">  
 <div class="form-group">  
 <label for="first\_name">First Name</label>  
 <input type="text" id="first\_name" name="first\_name" required>  
 </div>  
 <div class="form-group">  
 <label for="last\_name">Last Name</label>  
 <input type="text" id="last\_name" name="last\_name" required>  
 </div>  
 <div class="form-group">  
 <label for="email">Email</label>  
 <input type="email" id="email" name="email" required>  
 </div>  
 <div class="form-group">  
 <label for="password">Password</label>  
 <input type="password" id="password" name="password" required>  
 </div>  
 <div class="form-group">  
 <label for="privileges">Privileges</label>  
 <select id="privileges" name="privileges" required>  
 <option value="user">User</option>  
 <option value="admin">Admin</option>  
 </select>  
 </div>  
 <button type="submit">Create</button>  
 </form>  
 </div>  
 </div>  
 <p class="disclaimer">This page is accessible only to admin users.</p>  
 {% else %}  
 <h1>Access Denied</h1>  
 <p>This page is restricted to admin users only. Please contact an administrator.</p>  
 {% endif %}  
</div>  
  
<script>  
 function removeUsers() {  
 const checkboxes = document.querySelectorAll('input[name="remove\_user"]:checked');  
 const userIds = Array.from(checkboxes).map(cb => cb.value);  
 if (userIds.length > 0) {  
 if (confirm(`Are you sure you want to remove ${userIds.length} user(s)?`)) {  
 window.location.href = `{{ url\_for('org\_manager') }}?remove=${userIds.join(',')}`;  
 }  
 } else {  
 alert('Please select at least one user to remove.');  
 }  
 }  
</script>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

results\_admin.html  
{% extends "base.html" %}  
{% block title %}Admin Results - DPAT{% endblock %}  
{% block content %}  
<div class="main-content">  
 {% if current\_user.role == 'admin' %}  
 <h1>User Results</h1>  
 <div class="org-manager-container">  
 <div class="admin-manager">  
 <h2>Users: {{ organization\_name | default('Sacred Heart University') }}</h2>  
 <table>  
 <thead>  
 <tr>  
 <th>Number</th>  
 <th>Name</th>  
 <th>Role</th>  
 <th>Score</th>  
 </tr>  
 </thead>  
 <tbody>  
 {% for user in users %}  
 <tr>  
 <td>{{ user.id }}</td>  
 <td>{{ user.email }}</td>  
 <td>{{ user.role }}</td>  
 <td>{{ user.assessment\_scores[-1].score if user.assessment\_scores else 'N/A' }}%</td>  
 </tr>  
 {% endfor %}  
 </tbody>  
 </table>  
 </div>  
 <div class="compliance-score">  
 <h2>Average Score</h2>  
 <div class="score-box">{{ avg\_score }}</div>  
 </div>  
 </div>  
 <p class="disclaimer">User Assessment Score - only accessible to Admin - displays user’s assessment score and average scores of all users.</p>  
 {% else %}  
 <h1>Access Denied</h1>  
 <p>This page is restricted to admin users only. Please contact an administrator.</p>  
 {% endif %}  
</div>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

results\_user.html  
{% extends "base.html" %}  
{% block title %}User Results - DPAT{% endblock %}  
{% block content %}  
<div class="main-content">  
 <h1>Your Assessment Results</h1>  
 <p>Your score: {{ score }}%</p>  
 <a href="{{ url\_for('assessment') }}" class="results-button">Retake Assessment</a>  
</div>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
risks\_bp.html  
{% extends "base.html" %}  
{% block title %}Breach Informant Graphical Analysis - DPAT{% endblock %}  
{% block content %}  
<div class="main-content">  
 <h1>Breach Informant Graphical Analysis</h1>  
 <p class="intro-text">This page provides a visual analysis of the consequences and financial impacts of major data breaches since 2010, helping organizations understand the risks and potential costs associated with data breaches.</p>  
  
 <!-- Graphical Analysis -->  
 <div class="graph-container">  
 <h3 class="graph-title">Figure 1 – Consequence Analysis</h3>  
 <img src="{{ url\_for('static', filename='images/data\_breach\_consequence\_analysis.png') }}" alt="Data Breach Consequence Analysis" class="graph-image">  
 <p class="graph-caption">This chart illustrates the various consequences faced by companies after a data breach, such as resignations, criminal convictions, financial penalties, security upgrades, legal fees, shutdowns, reputational damage, regulatory scrutiny, and loss of customer trust.</p>  
 </div>  
  
 <div class="graph-container">  
 <h3 class="graph-title">Figure 2 – Consequence Frequency Analysis</h3>  
 <img src="{{ url\_for('static', filename='images/data\_breach\_consequence\_frequency\_analysis.png') }}" alt="Data Breach Consequence Frequency Analysis" class="graph-image">  
 <p class="graph-caption">This histogram shows the frequency of each consequence across the analyzed breaches, highlighting that loss of customer trust, regulatory scrutiny, and reputational damage are the most common outcomes.</p>  
 </div>  
  
 <div class="graph-container">  
 <h3 class="graph-title">Figure 3 – Financial Analysis</h3>  
 <img src="{{ url\_for('static', filename='images/data\_breach\_financial\_analysis.png') }}" alt="Data Breach Financial Analysis" class="graph-image">  
 <p class="graph-caption">This bar chart displays the financial penalties (in millions USD) incurred by each company due to data breaches, with Equifax facing the highest penalty at over 2000 million USD.</p>  
 </div>  
</div>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
sign\_in.html  
{% extends "base.html" %}  
{% block title %}Sign In - Data Privacy and Analysis Tool{% endblock %}  
{% block content %}  
<div class="main-content">  
 <div class="sign-in-box">  
 <h1>Sign In</h1>  
 <p>Data Privacy and Analysis Tool</p>  
 <form action="{{ url\_for('sign\_in') }}" method="POST">  
 <div class="form-group">  
 <label for="username">Organization Email:</label>  
 <input type="email" id="username" name="username" required>  
 </div>  
 <div class="form-group">  
 <label for="password">Password:</label>  
 <input type="password" id="password" name="password" required>  
 </div>  
 {% with messages = get\_flashed\_messages(with\_categories=true) %}  
 {% if messages %}  
 {% for category, message in messages %}  
 <div class="error-message">  
 {{ message }}  
 </div>  
 {% endfor %}  
 {% endif %}  
 {% endwith %}  
 <div class="form-actions">  
 <button type="submit">Log-In</button>  
 <a href="{{ url\_for('forgot\_password') }}" class="forgot-password">Forgot Password?</a>  
 </div>  
 </form>  
 </div>  
</div>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
sys\_manager.html  
  
{% extends "base.html" %}  
{% block title %}System Manager - DPAT{% endblock %}  
{% block content %}  
<div class="main-content">  
 <h1>System Manager</h1>  
 {% with messages = get\_flashed\_messages() %}  
 {% if messages %}  
 <meta http-equiv="refresh" content="2;url={{ url\_for('sys\_manager') }}">  
 {% endif %}  
 {% endwith %}  
 <div class="sys-manager-container">  
 <div class="admin-manager">  
 <h2>Organizations</h2>  
 <table>  
 <thead>  
 <tr>  
 <th>ID</th>  
 <th>Name</th>  
 <th>Admin</th>  
 <th>Remove</th>  
 </tr>  
 </thead>  
 <tbody>  
 {% for org in organizations %}  
 <tr>  
 <td>{{ org.id }}</td>  
 <td>{{ org.name }}</td>  
 <td>{{ org.admin.email if org.admin else 'N/A' }}</td>  
 <td><input type="checkbox" name="remove\_org" value="{{ org.id }}"></td>  
 </tr>  
 {% endfor %}  
 </tbody>  
 </table>  
 <button onclick="removeOrgs()" class="action-button">Remove Selected</button>  
 </div>  
 <div class="create-org-box">  
 <h2>Create Organization</h2>  
 <form method="POST" action="{{ url\_for('sys\_manager') }}">  
 <div class="form-group">  
 <label for="org\_name">Organization Name</label>  
 <input type="text" id="org\_name" name="org\_name" required>  
 </div>  
 <div class="form-group">  
 <label for="admin\_name">Admin Name</label>  
 <input type="text" id="admin\_name" name="admin\_name" required>  
 </div>  
 <div class="form-group">  
 <label for="admin\_username">Admin Username (Email)</label>  
 <input type="email" id="admin\_username" name="admin\_username" required>  
 </div>  
 <div class="form-group">  
 <label for="admin\_password">Admin Password</label>  
 <input type="password" id="admin\_password" name="admin\_password" required>  
 </div>  
 <button type="submit">Create</button>  
 </form>  
 </div>  
 </div>  
 {% with messages = get\_flashed\_messages(with\_categories=true) %}  
 {% if messages %}  
 {% for category, message in messages %}  
 <p class="flash-{{ category }}">{{ message }}</p>  
 {% endfor %}  
 {% endif %}  
 {% endwith %}  
</div>  
  
<script>  
 function removeOrgs() {  
 const checkboxes = document.querySelectorAll('input[name="remove\_org"]:checked');  
 const orgIds = Array.from(checkboxes).map(cb => cb.value);  
 if (orgIds.length > 0) {  
 if (confirm(`Are you sure you want to remove ${orgIds.length} organization(s)?`)) {  
 window.location.href = `{{ url\_for('sys\_manager') }}?remove=${orgIds.join(',')}`;  
 }  
 } else {  
 alert('Please select at least one organization to remove.');  
 }  
 }  
</script>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
  
  
to\_do\_list.html  
  
{% extends "base.html" %}  
{% block title %}To-Do List - DPAT{% endblock %}  
{% block content %}  
<div class="main-content">  
 {% with messages = get\_flashed\_messages() %}  
 {% if messages %}  
 <!-- Display only the first message -->  
 <div class="flash-messages" id="flash-messages">  
 <p>{{ messages[0] }}</p>  
 </div>  
 {% endif %}  
 {% endwith %}  
 <h1>To-Do List</h1>  
 {% if to\_do\_items %}  
 <p>Complete the following tasks to improve your compliance score:</p>  
 <table class="to-do-table">  
 <thead>  
 <tr>  
 <th>Task</th>  
 <th>Action</th>  
 </tr>  
 </thead>  
 <tbody>  
 {% for item in to\_do\_items %}  
 <tr>  
 <td>{{ item.description }}</td>  
 <td>  
 <form method="POST" action="{{ url\_for('remove\_todo', todo\_id=item.id) }}">  
 <button type="submit" class="action-button">Remove</button>  
 </form>  
 </td>  
 </tr>  
 {% endfor %}  
 </tbody>  
 </table>  
 {% else %}  
 <p>Congratulations! You have no outstanding tasks to improve your compliance score.</p>  
 {% endif %}  
 <a href="{{ url\_for('checklist') }}" class="results-button">Back to Checklist</a>  
</div>  
  
<script>  
 // Fade out flash messages after 5 seconds  
 document.addEventListener('DOMContentLoaded', function () {  
 const flashMessages = document.getElementById('flash-messages');  
 if (flashMessages) {  
 setTimeout(() => {  
 flashMessages.style.opacity = '0';  
 setTimeout(() => {  
 flashMessages.style.display = 'none';  
 }, 1000); // Wait for the fade-out transition to complete (1s)  
 }, 5000); // 5 seconds delay before starting the fade-out  
 }  
 });  
</script>  
{% endblock %}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

App.py  
from flask import Flask, render\_template, request, redirect, url\_for, flash, session, make\_response, jsonify  
from flask\_login import LoginManager, UserMixin, login\_user, logout\_user, login\_required, current\_user  
from flask\_sqlalchemy import SQLAlchemy  
from werkzeug.security import generate\_password\_hash, check\_password\_hash  
from datetime import datetime  
import os  
  
app = Flask(\_\_name\_\_)  
app.secret\_key = 'your-secret-key'  
  
# SQLite configuration with absolute path  
app.config['SQLALCHEMY\_DATABASE\_URI'] = f'sqlite:///{os.path.join(os.path.dirname(\_\_file\_\_), "dpat.db")}'  
app.config['SQLALCHEMY\_TRACK\_MODIFICATIONS'] = False  
print(f"Database URI: {app.config['SQLALCHEMY\_DATABASE\_URI']}")  
db = SQLAlchemy(app)  
  
# Flask-Login setup  
login\_manager = LoginManager()  
login\_manager.init\_app(app)  
login\_manager.login\_view = 'sign\_in'  
  
  
# User model  
class User(UserMixin, db.Model):  
 id = db.Column(db.Integer, primary\_key=True)  
 email = db.Column(db.String(120), unique=True, nullable=False)  
 password = db.Column(db.String(128), nullable=False) # Hashed password  
 role = db.Column(db.String(20), nullable=False, default='user')  
 first\_name = db.Column(db.String(50))  
 last\_name = db.Column(db.String(50))  
 organization\_id = db.Column(db.Integer, db.ForeignKey('organization.id'))  
  
 def get\_id(self):  
 return str(self.id)  
  
  
# Organization model  
class Organization(db.Model):  
 id = db.Column(db.Integer, primary\_key=True)  
 name = db.Column(db.String(100), unique=True, nullable=False)  
 admin\_id = db.Column(db.Integer, db.ForeignKey('user.id'))  
 goal\_date = db.Column(db.DateTime) # Existing column for goal date  
 compliance\_score = db.Column(db.Float, default=0.0) # New column for compliance score  
 admin = db.relationship('User', backref='organization\_admin', uselist=False, foreign\_keys=[admin\_id])  
 users = db.relationship('User', backref='organization', foreign\_keys='User.organization\_id')  
  
  
# Assessment score model  
class AssessmentScore(db.Model):  
 id = db.Column(db.Integer, primary\_key=True)  
 user\_id = db.Column(db.Integer, db.ForeignKey('user.id'), nullable=False)  
 score = db.Column(db.Integer, nullable=False)  
 date\_taken = db.Column(db.DateTime, default=db.func.current\_timestamp())  
 user = db.relationship('User', backref='assessment\_scores')  
  
  
# To-Do Item model  
class ToDoItem(db.Model):  
 id = db.Column(db.Integer, primary\_key=True)  
 organization\_id = db.Column(db.Integer, db.ForeignKey('organization.id'), nullable=False)  
 description = db.Column(db.String(200), nullable=False)  
 completed = db.Column(db.Boolean, default=False)  
 organization = db.relationship('Organization', backref='todo\_items')  
  
class ChecklistItem(db.Model):  
 id = db.Column(db.Integer, primary\_key=True)  
 key = db.Column(db.String(50), unique=True, nullable=False) # e.g., 'lawful\_basis\_identified'  
 description = db.Column(db.String(200), nullable=False) # e.g., 'Identify and document lawful basis for data processing'  
@login\_manager.user\_loader  
def load\_user(user\_id):  
 return User.query.get(int(user\_id))  
  
  
# Initialize database and add sysadmin user if not exists  
def init\_db():  
 with app.app\_context():  
 db.create\_all()  
 # Check if sysadmin exists, add if not  
 if not User.query.filter\_by(email='sysadmin@dpat.org').first():  
 sysadmin = User(  
 email='sysadmin@dpat.org',  
 password=generate\_password\_hash('sysadminpass'),  
 role='sysadmin'  
 )  
 db.session.add(sysadmin)  
 db.session.commit()  
 print("Sysadmin user created!")  
  
  
# Routes  
@app.route('/')  
def home():  
 if current\_user.is\_authenticated and current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
 return render\_template('home.html')  
  
  
@app.route('/sign\_in', methods=['GET', 'POST'])  
def sign\_in():  
 if request.method == 'POST':  
 email = request.form.get('username')  
 password = request.form.get('password')  
 user = User.query.filter\_by(email=email).first()  
 if user and check\_password\_hash(user.password, password):  
 login\_user(user)  
 if email == 'sysadmin@dpat.org':  
 return redirect(url\_for('sys\_manager'))  
 return redirect(url\_for('home'))  
 else:  
 flash('Login credentials failed.')  
 return render\_template('sign\_in.html')  
  
  
@app.route('/logout')  
@login\_required  
def logout():  
 logout\_user()  
 return redirect(url\_for('home'))  
  
  
@app.route('/dashboard')  
@login\_required  
def dashboard():  
 if current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
  
 # Fetch organization data  
 org = Organization.query.filter\_by(id=current\_user.organization\_id).first()  
 compliance\_score = org.compliance\_score if org else 0.0  
 goal\_date = org.goal\_date.strftime('%B %d') if org and org.goal\_date else None  
 days\_remaining = None  
 if org and org.goal\_date:  
 today = datetime.now()  
 diff\_time = org.goal\_date - today  
 days\_remaining = diff\_time.days  
  
 # Pass a flag to indicate if the user is an admin  
 is\_admin = current\_user.role == 'admin'  
  
 return render\_template('dashboard.html',  
 avg\_score=f"{compliance\_score:.1f}",  
 goal\_date=goal\_date,  
 days\_remaining=days\_remaining,  
 is\_admin=is\_admin)  
  
  
@app.route('/set\_goal\_date', methods=['POST'])  
@login\_required  
def set\_goal\_date():  
 if current\_user.role != 'admin':  
 return jsonify({'error': 'Unauthorized'}), 403  
  
 data = request.get\_json()  
 goal\_date\_str = data.get('goal\_date')  
 goal\_date = datetime.strptime(goal\_date\_str, '%B %d')  
 # Set year to current year  
 goal\_date = goal\_date.replace(year=datetime.now().year)  
  
 org = Organization.query.filter\_by(id=current\_user.organization\_id).first()  
 if org:  
 org.goal\_date = goal\_date  
 db.session.commit()  
  
 today = datetime.now()  
 diff\_time = goal\_date - today  
 days\_remaining = diff\_time.days  
  
 return jsonify({'days\_remaining': days\_remaining})  
 return jsonify({'error': 'Organization not found'}), 404  
  
  
@app.route('/assessment', methods=['GET', 'POST'])  
@login\_required  
def assessment():  
 if current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
 if request.method == 'POST':  
 # Scoring logic for 20 questions  
 score = 0  
 total\_questions = 20  
 correct\_answers = {  
 'q1': 'b', 'q2': 'b', 'q3': 'b', 'q4': 'b', 'q5': 'd', 'q6': 'b',  
 'q7': 'a', 'q8': 'c', 'q9': 'b', 'q10': 'b',  
 'q11': ['a', 'c'], 'q12': ['a', 'b', 'c'], 'q13': ['a', 'b', 'd'],  
 'q14': ['a', 'c', 'd'], 'q15': ['a', 'c'],  
 'q16': ['a', 'b', 'c'], 'q17': ['a', 'b', 'c'],  
 'q18': ['a', 'b', 'c'], 'q19': ['a', 'c'], 'q20': ['a', 'b', 'd']  
 }  
 for q in range(1, 11): # Radio button questions  
 answer = request.form.get(f'q{q}')  
 if answer == correct\_answers[f'q{q}']:  
 score += 5  
 for q in range(11, 21): # Checkbox questions  
 answers = request.form.getlist(f'q{q}')  
 if sorted(answers) == sorted(correct\_answers[f'q{q}']):  
 score += 5  
  
 new\_score = AssessmentScore(user\_id=current\_user.id, score=score, date\_taken=datetime.now())  
 db.session.add(new\_score)  
 db.session.commit()  
 flash('Assessment submitted successfully!', 'success')  
 return redirect(url\_for('results\_user', score=score))  
 return render\_template('assessment.html')  
  
  
@app.route('/results\_user')  
@login\_required  
def results\_user():  
 if current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
 score = request.args.get('score', default=0, type=int)  
 return render\_template('results\_user.html', score=score)  
  
  
@app.route('/results\_admin')  
@login\_required  
def results\_admin():  
 if current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
 elif current\_user.role != 'admin':  
 flash('Access denied. Only admins can view admin results.')  
 return redirect(url\_for('dashboard'))  
  
 users\_data = User.query.filter\_by(organization\_id=current\_user.organization\_id).all()  
 scores = AssessmentScore.query.join(User).filter(User.organization\_id == current\_user.organization\_id).all()  
 avg\_score = sum(score.score for score in scores) / len(scores) if scores else 0  
 return render\_template('results\_admin.html', avg\_score=f"{avg\_score:.1f}%", users=users\_data)  
  
  
@app.route('/library')  
@login\_required  
def library():  
 if current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
 return render\_template('library.html')  
  
  
@app.route('/breach\_info')  
@login\_required  
def breach\_info():  
 if current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
 return render\_template('breach\_info.html')  
  
  
@app.route('/risks\_bp')  
@login\_required  
def risks\_bp():  
 if current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
 return render\_template('risks\_bp.html')  
  
  
@app.route('/org\_manager', methods=['GET', 'POST'])  
@login\_required  
def org\_manager():  
 if current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
 elif current\_user.role != 'admin':  
 flash('Access denied. Only admins can manage organizations.')  
 return redirect(url\_for('dashboard'))  
  
 # Restrict access to non-admin users  
 if current\_user.role != 'admin':  
 flash('Access denied. Only admins can manage organizations.')  
 return redirect(url\_for('dashboard'))  
  
 # Fetch the current admin's organization  
 organization = Organization.query.filter\_by(id=current\_user.organization\_id).first()  
 if not organization:  
 flash('No organization found for this admin. Please contact the system administrator.')  
 return redirect(url\_for('dashboard'))  
  
 # Set the organization name for display  
 organization\_name = organization.name  
  
 # Fetch users for the current admin's organization only  
 users\_data = User.query.filter\_by(organization\_id=current\_user.organization\_id).all()  
  
 # Handle POST request for creating a new user  
 if request.method == 'POST':  
 # Extract form data  
 first\_name = request.form.get('first\_name')  
 last\_name = request.form.get('last\_name')  
 email = request.form.get('email')  
 password = request.form.get('password')  
 privileges = request.form.get('privileges')  
  
 # Validate form data  
 if not email or not password or not privileges:  
 flash('User creation failed. All fields (email, password, privileges) are required.')  
 elif User.query.filter\_by(email=email).first():  
 flash('User creation failed. Email already exists.')  
 else:  
 try:  
 # Create new user with the current admin's organization\_id  
 new\_user = User(  
 email=email,  
 password=generate\_password\_hash(password),  
 role=privileges,  
 first\_name=first\_name,  
 last\_name=last\_name,  
 organization\_id=current\_user.organization\_id  
 )  
 db.session.add(new\_user)  
 db.session.commit()  
 flash(f'User {email} created successfully!', 'success')  
 # Refresh users\_data after adding a new user  
 users\_data = User.query.filter\_by(organization\_id=current\_user.organization\_id).all()  
 except Exception as e:  
 db.session.rollback()  
 flash(f'Error creating user: {str(e)}', 'error')  
  
 # Handle user removal via GET request with 'remove' parameter  
 remove\_indices = request.args.get('remove')  
 if remove\_indices:  
 try:  
 remove\_ids = [int(idx) for idx in remove\_indices.split(',')]  
 # Ensure users to remove belong to the current admin's organization  
 users\_to\_remove = User.query.filter(  
 User.id.in\_(remove\_ids),  
 User.email != current\_user.email, # Prevent self-deletion  
 User.organization\_id == current\_user.organization\_id  
 ).all()  
 if not users\_to\_remove:  
 flash('No valid users selected for removal.', 'warning')  
 else:  
 for user in users\_to\_remove:  
 db.session.delete(user)  
 db.session.commit()  
 flash(f'Removed {len(users\_to\_remove)} user(s).', 'success')  
 # Refresh users\_data after removal  
 users\_data = User.query.filter\_by(organization\_id=current\_user.organization\_id).all()  
 except ValueError:  
 flash('Invalid user IDs provided for removal.', 'error')  
 except Exception as e:  
 db.session.rollback()  
 flash(f'Error removing users: {str(e)}', 'error')  
  
 # Render the org\_manager template with the filtered users and organization name  
 return render\_template(  
 'org\_manager.html',  
 users=users\_data,  
 organization\_name=organization\_name  
 )  
  
  
@app.route('/update\_role', methods=['POST'])  
@login\_required  
def update\_role():  
 if current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
 elif current\_user.role != 'admin':  
 flash('Access denied. Only admins can update roles.')  
 return redirect(url\_for('org\_manager'))  
  
 email = request.form.get('email')  
 new\_role = request.form.get('role')  
 user = User.query.filter\_by(email=email).first()  
 if user:  
 user.role = new\_role  
 db.session.commit()  
 flash(f"Updated role for {email} to {new\_role}.")  
 else:  
 flash("User not found.")  
 return redirect(url\_for('org\_manager'))  
  
  
@app.route('/sys\_manager', methods=['GET', 'POST'])  
@login\_required  
def sys\_manager():  
 if current\_user.email != 'sysadmin@dpat.org':  
 flash('Access denied. Only the System Admin can access this page.')  
 return redirect(url\_for('dashboard' if current\_user.role != 'admin' else 'org\_manager'))  
  
 if request.method == 'POST':  
 org\_name = request.form.get('org\_name')  
 admin\_name = request.form.get('admin\_name')  
 admin\_username = request.form.get('admin\_username')  
 admin\_password = request.form.get('admin\_password')  
  
 if org\_name and admin\_name and admin\_username and admin\_password:  
 if not User.query.filter\_by(email=admin\_username).first():  
 # Create the new admin user  
 new\_admin = User(  
 email=admin\_username,  
 password=generate\_password\_hash(admin\_password),  
 role='admin',  
 first\_name=admin\_name.split()[0],  
 last\_name=admin\_name.split()[-1] if len(admin\_name.split()) > 1 else ''  
 )  
 db.session.add(new\_admin)  
 db.session.flush() # Flush to get the new\_admin.id  
  
 # Create the new organization and link it to the admin  
 new\_org = Organization(name=org\_name, admin\_id=new\_admin.id)  
 db.session.add(new\_org)  
 db.session.flush() # Flush to get the new\_org.id  
  
 # Set the organization\_id for the new admin user  
 new\_admin.organization\_id = new\_org.id  
  
 # Commit all changes  
 db.session.commit()  
 flash(f'Organization {org\_name} created successfully!')  
 else:  
 flash('Admin username already exists.')  
 else:  
 flash('Organization creation failed. All fields are required.')  
  
 remove\_ids = request.args.get('remove')  
 if remove\_ids:  
 remove\_ids = [int(id) for id in remove\_ids.split(',')]  
 orgs\_to\_remove = Organization.query.filter(Organization.id.in\_(remove\_ids)).all()  
 for org in orgs\_to\_remove:  
 admin = User.query.get(org.admin\_id)  
 if admin:  
 db.session.delete(admin)  
 db.session.delete(org)  
 db.session.commit()  
 flash(f'Removed {len(orgs\_to\_remove)} organization(s).')  
  
 organizations = Organization.query.all()  
 return render\_template('sys\_manager.html', organizations=organizations)  
  
  
@app.route('/checklist', methods=['GET', 'POST'])  
@login\_required  
def checklist():  
 if current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
 if request.method == 'POST':  
 checklist\_items = request.form.getlist('checklist\_items')  
 all\_items = {  
 'lawful\_basis\_identified': 'Identify and document lawful basis for data processing',  
 'lawful\_basis\_demonstrated': 'Demonstrate lawful basis for all processing activities',  
 'data\_minimization\_necessary': 'Collect only necessary personal data',  
 'data\_minimization\_review': 'Regularly review data to avoid excess retention',  
 'data\_accuracy\_process': 'Ensure data accuracy with processes',  
 'data\_accuracy\_correction': 'Allow data subjects to correct inaccurate data',  
 'transparency\_notices': 'Provide clear privacy notices',  
 'transparency\_details': 'Include details in privacy notices',  
 'consent\_freely\_given': 'Ensure consent is freely given and unambiguous',  
 'consent\_management': 'Implement consent management processes',  
 'consent\_withdrawal': 'Provide easy consent withdrawal',  
 'subject\_rights\_procedures': 'Have procedures for data subject rights',  
 'subject\_rights\_response': 'Respond to requests within one month',  
 'subject\_rights\_verification': 'Verify identity for rights requests',  
 'retention\_policy': 'Document data retention policy',  
 'retention\_disposal': 'Securely dispose of unneeded data',  
 'security\_measures': 'Implement data security measures',  
 'security\_training': 'Train employees on security practices',  
 'breach\_response\_plan': 'Have a data breach response plan',  
 'breach\_notification': 'Notify authorities of breaches within 72 hours',  
 'breach\_subject\_notification': 'Notify data subjects of breaches',  
 'third\_party\_contracts': 'Have GDPR-compliant contracts with third parties',  
 'third\_party\_audits': 'Audit third-party processors',  
 'dpia\_high\_risk': 'Conduct DPIAs for high-risk activities',  
 'dpia\_documented': 'Document DPIAs with necessity assessment',  
 'dpo\_designated': 'Designate a Data Protection Officer',  
 'processing\_records': 'Maintain data processing records',  
 'internal\_audits': 'Conduct regular internal audits',  
 'data\_transfer\_safeguards': 'Use safeguards for data transfers outside EEA',  
 'data\_transfer\_assessment': 'Assess recipient country privacy standards',  
 'employee\_training': 'Train employees on GDPR principles',  
 'ongoing\_training': 'Provide ongoing GDPR training',  
 'monitoring\_processes': 'Monitor GDPR compliance internally',  
 'gdpr\_review': 'Review GDPR practices regularly'  
 }  
  
 # Calculate compliance score  
 total\_items = len(all\_items)  
 completed\_items = len(checklist\_items)  
 compliance\_score = (completed\_items / total\_items) \* 100 if total\_items > 0 else 0.0  
  
 # Update the organization's compliance score  
 org = Organization.query.filter\_by(id=current\_user.organization\_id).first()  
 if org:  
 org.compliance\_score = compliance\_score  
 db.session.commit()  
  
 # Delete existing todo items for this organization  
 ToDoItem.query.filter\_by(organization\_id=current\_user.organization\_id).delete()  
  
 # Add new todo items  
 for item\_key, description in all\_items.items():  
 if item\_key not in checklist\_items:  
 todo\_item = ToDoItem(  
 organization\_id=current\_user.organization\_id,  
 description=description  
 )  
 db.session.add(todo\_item)  
  
 db.session.commit()  
 flash('Checklist saved successfully!', 'success')  
 return redirect(url\_for('to\_do\_list'))  
 return render\_template('checklist.html')  
  
  
@app.route('/to\_do\_list')  
@login\_required  
def to\_do\_list():  
 if current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
 todo\_items = ToDoItem.query.filter\_by(organization\_id=current\_user.organization\_id).all()  
 response = make\_response(render\_template('to\_do\_list.html', to\_do\_items=todo\_items))  
 session.pop('\_flashes', None)  
 return response  
  
@app.route('/remove\_todo/<int:todo\_id>', methods=['POST'])  
@login\_required  
def remove\_todo(todo\_id):  
 if current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
  
 # Fetch the to-do item  
 todo = ToDoItem.query.get\_or\_404(todo\_id)  
 if todo.organization\_id != current\_user.organization\_id:  
 flash('Unauthorized access to todo item.')  
 return redirect(url\_for('to\_do\_list'))  
  
 # Remove the to-do item  
 db.session.delete(todo)  
 db.session.commit()  
  
 # Recalculate compliance score  
 all\_items = {  
 'lawful\_basis\_identified': 'Identify and document lawful basis for data processing',  
 'lawful\_basis\_demonstrated': 'Demonstrate lawful basis for all processing activities',  
 'data\_minimization\_necessary': 'Collect only necessary personal data',  
 'data\_minimization\_review': 'Regularly review data to avoid excess retention',  
 'data\_accuracy\_process': 'Ensure data accuracy with processes',  
 'data\_accuracy\_correction': 'Allow data subjects to correct inaccurate data',  
 'transparency\_notices': 'Provide clear privacy notices',  
 'transparency\_details': 'Include details in privacy notices',  
 'consent\_freely\_given': 'Ensure consent is freely given and unambiguous',  
 'consent\_management': 'Implement consent management processes',  
 'consent\_withdrawal': 'Provide easy consent withdrawal',  
 'subject\_rights\_procedures': 'Have procedures for data subject rights',  
 'subject\_rights\_response': 'Respond to requests within one month',  
 'subject\_rights\_verification': 'Verify identity for rights requests',  
 'retention\_policy': 'Document data retention policy',  
 'retention\_disposal': 'Securely dispose of unneeded data',  
 'security\_measures': 'Implement data security measures',  
 'security\_training': 'Train employees on security practices',  
 'breach\_response\_plan': 'Have a data breach response plan',  
 'breach\_notification': 'Notify authorities of breaches within 72 hours',  
 'breach\_subject\_notification': 'Notify data subjects of breaches',  
 'third\_party\_contracts': 'Have GDPR-compliant contracts with third parties',  
 'third\_party\_audits': 'Audit third-party processors',  
 'dpia\_high\_risk': 'Conduct DPIAs for high-risk activities',  
 'dpia\_documented': 'Document DPIAs with necessity assessment',  
 'dpo\_designated': 'Designate a Data Protection Officer',  
 'processing\_records': 'Maintain data processing records',  
 'internal\_audits': 'Conduct regular internal audits',  
 'data\_transfer\_safeguards': 'Use safeguards for data transfers outside EEA',  
 'data\_transfer\_assessment': 'Assess recipient country privacy standards',  
 'employee\_training': 'Train employees on GDPR principles',  
 'ongoing\_training': 'Provide ongoing GDPR training',  
 'monitoring\_processes': 'Monitor GDPR compliance internally',  
 'gdpr\_review': 'Review GDPR practices regularly'  
 }  
  
 # Count remaining to-do items  
 remaining\_items = ToDoItem.query.filter\_by(organization\_id=current\_user.organization\_id).count()  
 total\_items = len(all\_items)  
 completed\_items = total\_items - remaining\_items  
 compliance\_score = (completed\_items / total\_items) \* 100 if total\_items > 0 else 0.0  
  
 # Update the organization's compliance score  
 org = Organization.query.filter\_by(id=current\_user.organization\_id).first()  
 if org:  
 org.compliance\_score = compliance\_score  
 db.session.commit()  
  
 flash('Task removed successfully!', 'success')  
 return redirect(url\_for('to\_do\_list'))  
@app.route('/complete\_todo/<int:todo\_id>', methods=['POST'])  
@login\_required  
def complete\_todo(todo\_id):  
 todo = ToDoItem.query.get\_or\_404(todo\_id)  
 if todo.organization\_id != current\_user.organization\_id:  
 flash('Unauthorized access to todo item.')  
 return redirect(url\_for('to\_do\_list'))  
 todo.completed = True  
 db.session.commit()  
 flash('Task marked as completed!')  
 return redirect(url\_for('to\_do\_list'))  
  
  
@app.route('/forgot\_password')  
def forgot\_password():  
 flash('Forgot password functionality is not yet implemented.')  
 return redirect(url\_for('sign\_in'))  
  
  
@app.route('/consequences\_bp')  
@login\_required  
def consequences\_bp():  
 if current\_user.email == 'sysadmin@dpat.org':  
 flash('Access denied. System Admin can only access System Manager.')  
 return redirect(url\_for('sys\_manager'))  
 return render\_template('consequences\_bp.html')  
  
  
if \_\_name\_\_ == '\_\_main\_\_':  
 init\_db() # Initialize database before running  
 app.run(debug=True)

-------------------------------------------------

Database.py  
import sqlite3  
  
  
# Initialize the database connection  
def init\_db():  
 conn = sqlite3.connect("database.db")  
 cursor = conn.cursor()  
  
 # Create Users table  
 cursor.execute('''  
 CREATE TABLE IF NOT EXISTS users (  
 id INTEGER PRIMARY KEY AUTOINCREMENT,  
 name TEXT NOT NULL,  
 username TEXT UNIQUE NOT NULL,  
 password TEXT NOT NULL,  
 role TEXT CHECK(role IN ('user', 'admin', 'sysadmin')) NOT NULL  
 )  
 ''')  
  
 # Create Organizations table  
 cursor.execute('''  
 CREATE TABLE IF NOT EXISTS organizations (  
 id INTEGER PRIMARY KEY AUTOINCREMENT,  
 name TEXT UNIQUE NOT NULL,  
 admin\_username TEXT UNIQUE NOT NULL,  
 admin\_password TEXT NOT NULL  
 )  
 ''')  
  
 # Create Assessment Scores table  
 cursor.execute('''  
 CREATE TABLE IF NOT EXISTS assessment\_scores (  
 id INTEGER PRIMARY KEY AUTOINCREMENT,  
 user\_id INTEGER NOT NULL,  
 score INTEGER NOT NULL,  
 FOREIGN KEY(user\_id) REFERENCES users(id)  
 )  
 ''')  
  
 conn.commit()  
 conn.close()  
  
  
# Function to add a user  
def add\_user(name, username, password, role):  
 conn = sqlite3.connect("database.db")  
 cursor = conn.cursor()  
 try:  
 cursor.execute("INSERT INTO users (name, username, password, role) VALUES (?, ?, ?, ?)",  
 (name, username, password, role))  
 conn.commit()  
 except sqlite3.IntegrityError:  
 print("Error: Username already exists!")  
 conn.close()  
  
  
# Function to add an organization  
def add\_organization(name, admin\_username, admin\_password):  
 conn = sqlite3.connect("database.db")  
 cursor = conn.cursor()  
 try:  
 cursor.execute("INSERT INTO organizations (name, admin\_username, admin\_password) VALUES (?, ?, ?)",  
 (name, admin\_username, admin\_password))  
 conn.commit()  
 except sqlite3.IntegrityError:  
 print("Error: Organization name or admin username already exists!")  
 conn.close()  
  
  
# Function to store assessment scores  
def add\_assessment\_score(user\_id, score):  
 conn = sqlite3.connect("database.db")  
 cursor = conn.cursor()  
 cursor.execute("INSERT INTO assessment\_scores (user\_id, score) VALUES (?, ?)", (user\_id, score))  
 conn.commit()  
 conn.close()  
  
  
# Function to get user scores  
def get\_user\_scores():  
 conn = sqlite3.connect("database.db")  
 cursor = conn.cursor()  
 cursor.execute(  
 "SELECT users.name, assessment\_scores.score FROM users INNER JOIN assessment\_scores ON users.id = assessment\_scores.user\_id")  
 results = cursor.fetchall()  
 conn.close()  
 return results  
  
  
# Run the database initialization  
if \_\_name\_\_ == "\_\_main\_\_":  
 init\_db()  
 print("Database initialized successfully!")

from app import db, app, User, Organization  
from werkzeug.security import generate\_password\_hash  
from datetime import datetime  
  
def populate\_db():  
 with app.app\_context():  
 # Drop and recreate the database (optional if already done)  
 db.drop\_all()  
 db.create\_all()  
  
 # Create sysadmin user  
 sysadmin = User(  
 email='sysadmin@dpat.org',  
 password=generate\_password\_hash('sysadminpass'),  
 role='sysadmin',  
 first\_name='System',  
 last\_name='Admin'  
 )  
 db.session.add(sysadmin)  
 db.session.commit() # Commit sysadmin to get an ID  
  
 # Create Sacred Heart University organization  
 shu\_org = Organization(  
 name='Sacred Heart University',  
 admin\_id=None # Temporarily None, will update after admin creation  
 )  
 db.session.add(shu\_org)  
 db.session.commit() # Commit organization to get an ID  
  
 # Create admin user for SHU  
 shu\_admin = User(  
 email='admin@shu.edu',  
 password=generate\_password\_hash('shuadminpass'),  
 role='admin',  
 first\_name='SHU',  
 last\_name='Admin',  
 organization\_id=shu\_org.id  
 )  
 db.session.add(shu\_admin)  
 db.session.commit() # Commit admin to get an ID  
  
 # Update organization with admin ID  
 shu\_org.admin\_id = shu\_admin.id  
 db.session.commit()  
  
 # Create regular user for SHU  
 shu\_user = User(  
 email='user@shu.edu',  
 password=generate\_password\_hash('shuuserpass'),  
 role='user',  
 first\_name='SHU',  
 last\_name='User',  
 organization\_id=shu\_org.id  
 )  
 db.session.add(shu\_user)  
 db.session.commit()  
  
 print("Database populated with sysadmin, SHU organization, admin, and user!")  
  
if \_\_name\_\_ == '\_\_main\_\_':  
 populate\_db()